SIC-POVMS AND ORDERS OF REAL QUADRATIC FIELDS

GENE S. KOPP AND JEFFREY C. LAGARIAS

Abstract. This paper concerns SIC-POVMs and their relationship to class field theory. SIC-POVMs are generalized quantum measurements (POVMs) described by d^2 equiangular complex lines through the origin in $\mathbb{C}^d$. Weyl–Heisenberg covariant SICs are those SIC-POVMs described by the orbit a single vector under a finite Weyl–Heisenberg group $\mathrm{WH}(d)$.

We relate known data on the structure and classification of Weyl–Heisenberg covariant SICs in low dimensions to arithmetic data attached to certain orders of real quadratic fields. For $4 \le d \le 90$, we show the number of known geometric equivalence classes of Weyl–Heisenberg covariant SICs in dimension d equals the cardinality of the ideal class monoid of (not necessarily invertible) ideal classes in the real quadratic order $\mathcal{O}_\Delta$ of discriminant $\Delta = (d+1)(d-3)$; we conjecture the equality extends to all $d \ge 4$. We prove that this conjecture implies the existence of more than one geometric equivalence class of Weyl–Heisenberg covariant SICs for every $d > 22$. We conjecture that Galois multiplets of SICs may be put in one-to-one correspondence with the over-orders $\mathcal{O}'$ of $\mathcal{O}_\Delta$ in such a way that the number of geometric classes in the multiplet equals the ring class number of $\mathcal{O}'$. We test that conjecture against known data on exact SICs in low dimensions.

We refine the "class field hypothesis" of Appleby, Flammia, McConnell, and Yard [9] to predict the exact class field over $\mathbb{Q}(\sqrt{(d+1)(d-3)})$ generated by the ratios of vector entries for the equiangular lines defining a Weyl–Heisenberg SIC. The refined conjectures use a recently developed class field theory for orders of number fields [34]. The refined class fields assigned to over-orders $\mathcal{O}'$ have a natural partial order under inclusion; the inclusions of these class fields fail to be strict in some cases. We characterize such cases and give a table of them for $d < 500$.

1. Introduction

SIC-POVMs are generalized quantum measurements (POVMs) described by d^2 equiangular complex lines through the origin in $\mathbb{C}^d$. Sets of d^2 equiangular complex lines in $\mathbb{C}^d$ are extremal objects in combinatorial design theory; they give *equiangular tight frames* [46, Ch. 12–14]. The name *SIC-POVM* (abbreviated 'SIC') was introduced in a 2004 paper of Renes, Blume-Kohout, Scott, and Caves [38], whose study was motivated by quantum state tomography, the problem of reconstructing a quantum state from a series of measurements performed on identical states. Scott showed that SICs are optimal measurement ensembles for quantum tomography [39]; see also [25]. SICs have found further applications to quantum information processing [13, 17, 44, 45], quantum foundations [24], compressed sensing for radar [29], and classical phase retrieval [21]. At present SICs have been constructed for finitely many dimensions d, and conjecturally they exist for all d.

The objects of this paper are to extend the range of number-theoretic conjectures about the existence and structure of SICs proposed by Appleby, Flammia, McConnell, and Yard [8, 9] and to test the refined conjectures against empirical data. We also draw consequences of the refined conjectures for counting and classifying equivalence classes of SICs. The conjectures of [9] relate Weyl–Heisenberg SICs in $\mathbb{C}^d$ (defined in Section 2) for $d \ge 4$ to class field theory over real quadratic fields. The ratios of entries of each of the d^2 vectors in the currently known SICs lie in a number field that is an abelian extension of $K = \mathbb{Q}(\sqrt{\Delta_d})$ with $\Delta_d = (d+1)(d-3)$. Class field theory

Date: December 27, 2024.

2020 *Mathematics Subject Classification.* 11R37 (primary), 11R29, 11R65, 81P15, 81P18, 81R05, 42C15.

Key words and phrases. SIC-POVM, complex equiangular lines, equiangular tight frame (ETF), real quadratic field, non-maximal order, ideal class group, explicit class field theory.

classifies the abelian extensions of a given number field K in terms of ray class groups, which encode the arithmetic of ideals of the ring $\mathcal{O}_K$ of algebraic integers of K.

The number fields associated to individual SICs in dimension d may vary with the SIC, and the subclass of SICs to which the most precise conjecture of [9] applies consists of those giving rise to the minimal number field that occurs for a fixed d. Appleby, Flammia, McConnell, and Yard conjecture that this minimal field is a specific ray class field of $\mathbb{Q}(\sqrt{\Delta_d})$; see Conjecture 1.1. The corresponding SICs comprise the *minimal multiplet*, as defined in Section 2. It is one of several *Galois multiplets*, which are finite sets of geometric equivalence classes of SICs making up a single orbit of a Galois group action.

The current paper formulates a refinement of these conjectures that accounts for all the remaining Galois multiplets of Weyl–Heisenberg SICs, those having larger associated number fields. For $d \geq 4$ the refined conjecture asserts that the multiplets can be indexed bijectively by the the orders $\mathcal{O}'$ of the real quadratic number field $K_d = \mathbb{Q}(\sqrt{\Delta_d})$ intermediate between the order $\mathcal{O} = \mathbb{Z}[\varepsilon_d]$ with $\varepsilon_d = \frac{1}{2}(d-1+\sqrt{\Delta_d})$ and the maximal order $\mathcal{O}_{K_d}$ of all algebraic integers in K_d. Here an *order* $\mathcal{O}$ of K_d is a subring of K_d which contains 1 and is of finite index in $\mathcal{O}_K$.

In addition, the number field associated to the $\mathcal{O}'$-multiplet is conjectured to be a certain ray class field associated to the order $\mathcal{O}'$. The notion of ray class fields associated to orders is an extension of the usual class field theory (which is the special case of the maximal order), variants of which were developed (independently) by Campagna and Pengo [12] and the authors [34]. Inclusions of orders induce reverse inclusion of the corresponding ray class fields, so the minimal multiplet corresponds to the maximal order.

1.1. **SICs.** A set S of complex lines through the origin in $\mathbb{C}^d$, written $S = \{\mathbb{C}\mathbf{v}_1, \ldots, \mathbb{C}\mathbf{v}_n\} \subset \mathbb{P}^{d-1}(\mathbb{C})$ with $\mathbf{v}_j$ unit vectors, is *equiangular* if all the pairwise Hermitian inner products $\langle \mathbf{v}_i, \mathbf{v}_j \rangle$ for $i \neq j$ have the same absolute value $|\langle \mathbf{v}_i, \mathbf{v}_j \rangle| = \alpha \geq 0$. In 1975, Delsarte, Goethals, and Seidel [18] proved an upper bound of $n \leq d^2$ on the size of any set of complex equiangular lines in $\mathbb{C}^d$. They showed that if the bound $n = d^2$ is attained, then necessarily $\alpha = \frac{1}{\sqrt{d+1}}$.

A *symmetric informationally complete positive operator-valued measure* or *SIC-POVM* (henceforth *SIC*) is a set of normalized projections onto a (maximal) set of d^2 complex equiangular lines in $\mathbb{C}^d$. For d^2 equiangular lines $\{\mathbb{C}\mathbf{v}_1, \ldots, \mathbb{C}\mathbf{v}_{d^2}\}$ represented by unit column vectors $\mathbf{v}_j \in \mathbb{C}^d$, the associated SIC is the set of normalized rank one Hermitian projection operators $\mathbf{\Pi}(S) := \left\{\frac{1}{d}\Pi_1, \ldots, \frac{1}{d}\Pi_{d^2}\right\}$ where $\Pi_j = \mathbf{v}_j \mathbf{v}_j^\dagger$. (Vectors $\mathbf{v}$ are column vectors, $\mathbf{v}^\dagger$ is the conjugate transpose of $\mathbf{v}$, and the Hermitian inner product is $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = \mathbf{v}_i^\dagger \mathbf{v}_j$, following the quantum mechanics convention established by Dirac [19, Sec. 1.6]. Here, $\mathbf{v}_i^\dagger \mathbf{v}_i = 1$.) The SIC condition is equivalent to the following d^4 identities on the traces of products of the projections:

$$\mathrm{Tr}(\Pi_i \Pi_j) = \begin{cases} 1 & \text{if } i = j, \\ \frac{1}{d+1} & \text{if } i \neq j, \end{cases} \qquad \text{for } 1 \leq i, j \leq d^2.$$

We will use the term "SIC" interchangeably to mean either a "set of d^2 (scaled) Hermitian projection matrices $\mathbf{\Pi}(S)$ forming a SIC-POVM" or a "set of d^2 complex equiangular lines S in $\mathbb{C}^d$." When more specificity is needed, we term the latter a *line-SIC*.

Most work on SICs follows Zauner's 1999 PhD thesis [48,49] on quantum designs. A few sporadic examples (such as the Hoggar lines in dimension 8 [30, 31]) were known prior to Zauner's work. Zauner conjectured, based on his numerical investigations, that SICs exist in every dimension d, and moreover, that a SIC in $\mathbb{C}^d$ could be found as the orbit of a single vector under the Weyl–Heisenberg group [48, 49]; the latter objects are called *Weyl–Heisenberg covariant SICs* (or just *Weyl–Heisenberg SICs*) and are defined and discussed in Section 2. A generating vector $\mathbf{v} \in \mathbb{C}^d$ of such an orbit is called a *fiducial vector*. Weyl–Heisenberg SICs are the main topic of this paper. (An extensive treatment of the history of SICs is given by Fuchs, Hoang, and Stacy [23].)

Over the past 25 years, a large data set has been computed about SICs in particular dimensions—sometimes approximately and sometime exactly—resulting in extensive datasets [22, 40, 41]. SICs have been rigorously constructed in a finite set of dimensions, including Weyl–Heisenberg SICs in all dimensions $1 \leq d \leq 53$ and the Hoggar lines for $d = 8$. Beyond these exact constructions, numerical computations in dimensions including every $d \leq 90$ suggest there are only finitely many (equivalence classes of) Weyl–Heisenberg SICs in each dimension $d \neq 3$. It is known that $d = 3$ has infinitely many equivalence classes of Weyl–Heisenberg SICs, and we will not treat $d = 3$ here.

The current numerical data is believed to account for all Weyl–Heisenberg SICs of dimension $d \leq 90$. There is a geometric action moving these SICs around by the normalizer of the Weyl–Heisenberg group inside the extended unitary group (which is a finite group whose order varies erratically with d, while the Weyl–Heisenberg group itself has order d^3 or $2d^3$, the latter occurring for even d.) In addition, since the (normalized) generating vectors of Weyl–Heisenberg SICs can be (empirically) given by algebraic numbers, there is a Galois action, which sometimes moves SICs to new SICs and sometimes moves them to non-SICs.

The process of understanding this data has led to formulation of a series of interlocking hypotheses. The two most basic conjectures, which are both unsolved, are:

(1) the existence of Weyl–Heisenberg SICs in all dimensions (conjectured by Zauner);
(2) the finiteness of the set of Weyl–Heisenberg line-SICs in every fixed dimension $d \neq 3$.

The finiteness assertion has been a "folklore" conjecture since about 2004. It was observed empirically under heuristics up to dimension $d = 7$ by Renes, Blume-Kohout, Scott, and Caves [38, Tab. I and Sec. V], up to dimension $d = 50$ by Scott and Grassl (who state they are confident their list is complete for $d \leq 50$ in [41, Sec. 4]), and up to $d = 90$ by Fuchs, Hoang, and Stacy [23, Sec. 6] using data of Scott [40]. It was explicitly formulated as a conjecture in the first author's PhD thesis [32, Conj. V.12]. A closely related conjecture was formulated by Waldron [46, Sec. 14.27].

The finiteness assertion would imply fiducial vectors of Weyl–Heisenberg SICs can be chosen to have all entries algebraic numbers. Further study of these algebraic numbers in existing examples has led to surprising discoveries.

1.2. **Connection of SICs to algebraic number theory and class fields.** Recent work has connected SICs to explicit class field theory over real quadratic number fields. Appleby, Yadsan-Appleby, and Zauner [4] discovered in 2013 that in all known examples, the algebraic number field $\mathbb{E}$ generated by the entries of the projections $\mathbf{\Pi}(S)$ contains the quadratic field $K_d = \mathbb{Q}(\sqrt{(d+1)(d-3)})$, and Galois automorphisms often map SICs to new SICs. Moreover, they observed in all known examples (for $d \neq 3$) that $\mathbb{E}$ is an *abelian* extension of K_d.

In 2016, Appleby, Flammia, McConnell, and Yard [8, 9] made explicit predictions relating the number fields generated by Weyl–Heisenberg SICs to ray class fields. Based on extensive data given in [9, Prop. 1], they formulated the following conjecture [9, Conj. 2].

Conjecture 1.1 (Appleby, Flammia, McConnell and Yard). *Let $d \geq 4$, $\Delta_d = (d+1)(d-3)$, and $K_d = \mathbb{Q}(\sqrt{\Delta_d})$.*

(1) *At least one Weyl–Heisenberg line-SIC S exists in dimension d having SIC field $F^{\mathrm{vec}}(S)$ equal to $H_{d'\infty_1\infty_2}$, the ray class field of K_d having ray class modulus $d'\infty_1\infty_2$, where $d' = d$ if d is odd, and $d' = 2d$ if d is even.*
(2) *Every Weyl–Heisenberg line-SIC S in dimension d has SIC field $F^{\mathrm{vec}}(S)$ that is a finite Galois extension of $\mathbb{Q}$ containing $H_{d'\infty_1\infty_2}$.*

The technical definition of the SIC field $F^{\mathrm{vec}}(S)$ appearing in Conjecture 1.1 is given in Section 3.1. Ray class fields are discussed in Section 6.1.

Appleby, Flammia, McConnell, and Yard verified assertion (1) of Conjecture 1.1 for

$$d \in \{4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 24, 28, 30, 35, 39, 48\}.$$

They verified assertion (2) of the conjecture for all known Weyl–Heisenberg SICs in these dimensions. They also verified that the fields $F^{\mathrm{vec}}(S)$ are all abelian over K_d in the known cases. (The list of SICs used is believed to be complete in these dimensions.)

Subsequently, in 2018, the first author [33] proposed an explicit, conjectural construction of a SIC in prime dimensions $d \equiv 2 \pmod 3$ for $d \geq 5$ in terms of Stark units and verified it in the cases $d \in \{5, 11, 17, 23\}$. (He suggested a connection to Stark units in every dimension). Recently Appleby, Bengtsson, Grassl, Harrison, and McConnell [5] gave a (different, related) conjectural construction in prime dimensions of the form $d = p = n^2+3$, and Bengtsson, Grassl, and McConnell [10] extended the latter to dimensions $d = 4p = n^2 + 3$ with p prime.

The origin of the discriminant $\Delta_d = (d+1)(d-3)$ appearing in the conjecture is not completely understood. The appearance of the factor $d+1$ dividing Δ_d seems related to the fact that the inner products of distinct unit vectors in a SIC are of absolute value $\frac{1}{\sqrt{d+1}}$. The appearance of $d-3$ accounts for $d = 3$ being special, in that $\Delta_3 = 0$. The values $d = 1, 2$ have $\Delta_d < 0$, so $K_d = \mathbb{Q}(\sqrt{\Delta_d})$ is an imaginary quadratic field, while for $d \geq 4$, Δ_d specifies a (nontrivial) real quadratic field. The occurrence of a small unit $\varepsilon_d = \frac{1}{2}(d - 1 + \sqrt{\Delta_d})$ (as compared in size to Δ_d, which need not be a fundamental discriminant) is certainly relevant. The first author previously noted that, on skipping repeated fields (e.g., $K_8 = K_4$), the sequence $K_4, K_5, K_6, K_7, K_9, K_{10}, \ldots$ gives precisely the ordering of all real quadratic fields by increasing size of the smallest nontrivial totally positive unit (necessarily equal to ε_d); see [33, p. 13819].

1.3. **Main results.** In this paper, we refine Conjecture 1.1 to conjectures that specify the number fields associated to all the Weyl–Heisenberg SICs in each dimension $d \geq 4$, and which also count the number of geometric equivalence classes of such SICs associated to each such field.

More precisely, we connect both SICs and their associated fields to certain orders of the real quadratic number field $K_d = \mathbb{Q}(\sqrt{\Delta_d})$, with $\Delta_d = (d+1)(d-3)$. Write $\Delta_d = f^2\Delta_0$, where Δ_0 is the fundamental discriminant K_d, and $f \geq 1$. The orders that arise are exactly those $\mathcal{O}'$ satisfying $\mathbb{Z}[\varepsilon_d] \subseteq \mathcal{O}' \subseteq \mathcal{O}_K$ for $\varepsilon_d = \frac{1}{2}(d - 1 + \sqrt{\Delta_d})$. These orders, arranged by set inclusion, form a distributive lattice, isomorphic to that of the positive divisors of f under divisibility.

We organize Weyl–Heisenberg SICs into equivalence classes. For such a line-SIC S,

(1) the *geometric equivalence class* $[S]$ is the orbit of S under the action of the *projective extended Clifford group* $\mathrm{PEC}(d)$ (by Definition 2.9), and
(2) the *Galois multiplet* $[[S]]$ is the set of geometric equivalence classes that are permuted with each other under a certain Galois action (by Definition 4.9).

In Sections 3 and 4, we define several fields attached to a line-SIC $S = \{\mathbb{C}\mathbf{v}_k : 1 \leq k \leq d^2\}$. These fields are finitely generated extensions of the rational numbers $\mathbb{Q}$.

(1) The *ratio SIC field* $F^{\mathrm{vec}}(S)$ (called the "SIC field" in [9]) is the field generated by all the ratios $\frac{v_{ki}}{v_{kj}}$ of distinct entries ($i \neq j$, $v_{kj} \neq 0$) of the vectors $\mathbf{v}_k$ with $\mathbf{v}_k \in S$.
(2) The *projection SIC field* $F^{\mathrm{proj}}(S)$ is the field generated by the matrix entries of the Hermitian projection operators $\Pi_i = \mathbf{v}_i\mathbf{v}_i^\dagger$ of the d^2 unit vectors $\{\mathbf{v}_i : 1 \leq i \leq d^2\}$ defining S.
(3) The *extended projection SIC field* $F^{\mathrm{eproj}}(S) = F^{\mathrm{proj}}(S)(\xi_d)$ is obtained by adjoining the root of unity $\xi_d = -e^{\frac{\pi i}{d}}$.
(4) For algebraic SICs (ones with $F^{\mathrm{vec}}(S)$ a finite extension of $\mathbb{Q}$), the *Galois projection SIC field* $F^{\mathrm{Gproj}}(S)$ is the normal closure of $F^{\mathrm{eproj}}(S)$.

We have the following field inclusions, with the last being valid only for algebraic SICs:

$$F^{\mathrm{vec}}(S) \subseteq F^{\mathrm{proj}}(S) \subseteq F^{\mathrm{eproj}}(S) \subseteq F^{\mathrm{Gproj}}(S)\,.$$

The field $F^{\mathrm{Gproj}}(S)$ is an invariant of the Galois multiplet $[[S]]$ of an algebraic SIC S. In Lemma 4.8, we show that Conjecture 1.1 implies the equalities

$$F^{\mathrm{vec}}(S) = F^{\mathrm{proj}}(S) = F^{\mathrm{eproj}}(S) = F^{\mathrm{Gproj}}(S)\,,$$

whence $F^{\mathrm{vec}}(S)$ is a finite Galois extension of $\mathbb{Q}$.

The refinements of Conjecture 1.1 formulated in this paper assert that Weyl–Heisenberg SICs in dimension $d \neq 3$ occur in Galois multiplets indexed by the intermediate orders $\mathcal{O}'$ of K_d that lie between $\mathcal{O}_{\Delta_d} = \mathbb{Z}[\varepsilon_d]$ and $\mathcal{O}_{K_d}$. Each intermediate order is in turn labeled by its *conductor* f', a positive integer such that $\mathrm{disc}(\mathcal{O}') = (f')^2\Delta_0$ where $\Delta_0 = \mathrm{disc}(\mathcal{O}_{K_d})$. Quadratic orders are uniquely specified by their discriminants, so we may write $\mathcal{O}' = \mathcal{O}_{(f')^2\Delta_0}$. The conductors appearing are the positive divisors f' of the conductor f of $\mathcal{O}$.

Conjecture 1.2 (Order-to-Multiplet Conjecture)**.** *Fix a positive integer $d \neq 3$, let $\Delta = \Delta_d = (d+1)(d-3)$, and write $\Delta = f^2\Delta_0$ for $\Delta_0 = \mathrm{disc}(\mathcal{O}_{K_d})$ and some positive integer f. Then there is a bijection $\mathcal{M}$ between intermediate orders $\mathcal{O}' = \mathcal{O}_{(f')^2\Delta_0}$, labeled by their conductors f', and Galois multiplets,*

$$\{f' \text{ a positive divisor of } f\} \xrightarrow{\mathcal{M}} \{[[S]] : S \text{ a Weyl–Heisenberg line-SIC in } \mathbb{C}^d\},$$

having the following properties.

1. *The number of geometric equivalence classes $[S]$ in the multiplet $\mathcal{M}(f') = [[S]]$ is the class number $h_{(f')^2\Delta_0} := \left|\mathrm{Cl}(\mathcal{O}_{(f')^2\Delta_0})\right|$ of the the order $\mathcal{O}'$ of discriminant $(f')^2\Delta_0$.*
2. *If $f_1|f_2$ and $f_2|f$, and $[S_1] \in \mathcal{M}(f_1)$, and $[S_2] \in \mathcal{M}(f_2)$, then $F^{\mathrm{vec}}(S_1) \subseteq F^{\mathrm{vec}}(S_2)$.*

The special case $f' = 1$ corresponds to Conjecture 1.1, where the order $\mathcal{O}'$ is the maximal order. Appleby, Flammia, McConnell, and Yard [8] call the associated Galois multiplet $[[S]]$ the *minimal multiplet*, as it has the smallest associated field $F^{\mathrm{vec}}(S)$ under inclusion. The field inclusions asserted in Conjecture 1.1(2) imply the truth of Conjecture 1.2(2) in the special case $f_1 = 1$.

The following conjecture is an extension of both Conjecture 1.1 and Conjecture 1.2, which uses the notion of ray class fields of an order $\mathcal{O}'$ introduced in [34] and reviewed in Section 6.1.

Conjecture 1.3 (Ray Class Fields of Orders Conjecture)**.** *Let $d \geq 4$. Then the map $\mathcal{M}$ in Conjecture 1.2 may be chosen so that, for any Weyl–Heisenberg line-SIC S in dimension d with associated order $\mathcal{O}'$ having discriminant $(f')^2\Delta_0$ (that is, with $\mathcal{M}(f') = [[S]]$), one has*

$$F^{\mathrm{vec}}(S) = F^{\mathrm{proj}}(S) = H^{\mathcal{O}'}_{d'\mathcal{O}', \{\infty_1, \infty_2\}},$$

where $H^{\mathcal{O}'}_{d'\mathcal{O}', \{\infty_1, \infty_2\}}$ is the ray class field having level datum $(\mathcal{O}'; d'\mathcal{O}', \{\infty_1, \infty_2\})$, $d' = 2d$ if d is even, and $d' = d$ if d is odd.

The paper describes numerical checks of predictions of these conjectures against numerical data for SICs obtained in the datasets [22, 23, 40, 41]. The numerical data include both exact Weyl–Heisenberg SICs given by algebraic fiducial vectors and numerical SICs given as rational vectors approximately satisfying the fiducial vector SIC relations (to many decimal places). The notion of *geometric equivalence class* makes sense for numerical SICs, because they have well-defined $\mathrm{PEC}(d)$-orbits; however, the notion of *Galois multiplet* is not well-defined for them. In consequence we cannot test Conjecture 1.2 using numerical SICs, since its statement involves Galois multiplets. Instead, we extract a numerical prediction implied by Conjecture 1.2 that is testable.

This numerical prediction counts the total number of geometric equivalence classes of Weyl–Heisenberg SICs in dimension d and is formulated as Conjecture 5.4. It says that the total number of geometric equivalence classes of Weyl–Heisenberg SICs in dimension $d \geq 4$ is $|\mathrm{Clm}(\mathcal{O}_{\Delta_d})|$, the cardinality of the *class monoid of the order* $\mathcal{O}_{\Delta_d}$, as defined in Section 5.1.

We formulate this prediction as Conjecture 5.4, and we test it in Proposition 5.7 using both exact and numerical SICs. These tests are summarized by Table 5.1 and Table 5.2 for all dimensions $4 \leq d \leq 90$. Conjecture 5.4 gives agreement in all these dimensions, assuming that the list of exact plus numerical SICs is complete. (The number $|\mathrm{Clm}(\mathcal{O}_{\Delta_d})|$ is equal to a sum of the ring class numbers $h_{(f')^2\Delta_0}$ appearing in Conjecture 1.2; see Theorem 5.3.)

The existence of the bijection $\mathcal{M}$ asserted in Conjecture 1.2 implies a numerical prediction concerning the number of Galois multiplets, predicting that it equals the number of quadratic orders between $\mathcal{O}_{\Delta_d}$ and $\mathcal{O}_{K_d}$, which is the number of over-orders of $\mathcal{O}_{\Delta_d}$ in $K = \mathbb{Q}(\sqrt{\Delta_d})$. This numerical prediction is formulated as Conjecture 5.8 and tested in Proposition 5.9 against certain dimensions d in which all known SICs are exact SICs. Supporting data is given in Table 5.1.

In Section 6, we provide further tests of Conjecture 1.2(2) and Conjecture 1.3. We first summarize results on ray class fields of orders required to understand the conjectures. In Proposition 6.6, we numerically test the equality of degrees over $\mathbb{Q}$ of the ray class fields of orders in Conjecture 1.3 to those of the fields $F^{\mathrm{vec}}(S)$. Tests are performed for exact SICs in dimensions $4 \le d \le 15$ and $d = 35$, and a supporting table of fields is given in Table 6.1.

We display for $d = 35$ in Example 5.10 and Example 6.7 a (unique) bijective map $\mathcal{M}$ of orders to Galois multiplets that fulfills both conditions (1) and (2) of Conjecture 1.2. In Section 8 we show that Conjecture 1.3 strongly restricts the map $\mathcal{M}$ and, according to results proved elsewhere [36], determines it uniquely for a fraction $\frac{47}{48}$ of dimensions d. We show in Theorem 8.2 that the set of d for which there exist two distinct orders $\mathcal{O}', \mathcal{O}''$ with identical $H^{\mathcal{O}'}_{d'\mathcal{O}',\{\infty_1,\infty_2\}}$ in Conjecture 1.3 is the set of d for which the squarefree part of $(d+1)(d-3)$ is 1 (mod 8). Then Proposition 8.3 computes the asymptotic density of this set to be $\frac{1}{48}$. We present Table 8.1, which lists all cases of equality of such orders occurring for $d \le 500$. These equality cases include all cases of observed equality of SIC fields $d \in \{47, 67, 259\}$ by Grassl [26].

1.4. Notation.

- Boldface roman upper case letters represent continuous groups, e.g., $\mathbf{EU}(d)$.
- Boldface roman lower case letters $\mathbf{v} = (v_0, v_1, \cdots v_{d-1})^T$ represent column vectors in $\mathbb{C}^d$. For a complex vector, $\mathbf{w}^\dagger := \overline{\mathbf{w}}^T$, and similarly for matrices.
- Upper case roman letters represent $d \times d$ complex matrices (e.g., X, Z); they also appear in names of finite matrix groups (e.g., $\mathrm{WH}(d)$) and sets (e.g., $\mathrm{WHSIC}(d)$).
- Matrices and vectors have rows and columns numbered from 0 to $d-1$. We follow the text of Waldron [46], which identifies indices with $\mathbb{Z}/d\mathbb{Z}$.
- Greek letters generally represent algebraic numbers (e.g., $\xi_d = -e^{\frac{\pi i}{d}}$ and $\zeta_d = e^{\frac{2\pi i}{d}}$).
- However, the letter σ is exclusively used for Galois automorphisms, with σ_c denoting complex conjugation. Galois group actions are treated either as acting on scalars or as acting entrywise on vectors or matrices.
- The notation S is used for a (d-dimensional) line-SIC; it is a set of d^2 complex lines.
- The notation $[S]$ is used for a geometric equivalence class of SICs. (However, $[\mathbf{v}]$ denotes the complex line $\mathbb{C}\mathbf{v}$, when $\mathbf{v}$ is a vector.)
- We use the convention that d' means $d' = d$ if d is odd and $d' = 2d$ if d is even. The number $\xi_d = -e^{\frac{\pi i}{d}}$ is a d'-th root of unity.
- We write $\Delta_d = (d+1)(d-3)$ for the (often non-fundamental) discriminant associated to dimension d, $K_d = \mathbb{Q}(\sqrt{\Delta_d})$ for the associated field, and $\varepsilon_d = \frac{1}{2}(d - 1 + \sqrt{\Delta_d})$ for the associated unit.

2. Weyl–Heisenberg SICs

In this section, we define and give background on Weyl–Heisenberg (covariant) SICs, which satisfy a particular group symmetry property.

2.1. Weyl–Heisenberg SICs.

Specifically, Weyl–Heisenberg line-SICs will be defined as the orbit of a single line under the action of the Weyl–Heisenberg group, a finite subgroup of the group of $d \times d$ unitary matrices.

Definition 2.1. The *Weyl–Heisenberg group* is $\mathrm{WH}(d) = \{\xi^r X^p Z^q : p, q, r \in \mathbb{Z}\}$, where $\xi = -e^{\frac{\pi i}{d}}$, $\zeta = \xi^2 = e^{\frac{2\pi i}{d}}$, and

$$X = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \zeta & 0 & \cdots & 0 \\ 0 & 0 & \zeta^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \zeta^{d-1} \end{pmatrix},$$

The *projective Weyl–Heisenberg group* $\mathrm{PWH}(d)$ is defined to be $\mathrm{WH}(d)$ modulo its scalar matrix subgroup $Z(\mathrm{WH}(d)) = \{\xi^j I : j \geq 0\}$, where I is the $d \times d$ identity matrix, X is called the *cyclic shift matrix*, and Z is called the *modulation matrix* [46, Sec. 14.5].

It is easily checked that $ZX = \zeta XZ$. It follows that $\mathrm{WH}(d)$ is a group. Its order is d^3 if d is odd and $2d^3$ if d is even, noting that ξ is a d-th root of unity for odd d and a $2d$-th root of unity for even d. The center $\mathrm{Z}(\mathrm{WH}(d)) = \langle \xi I \rangle$ of $\mathrm{WH}(d)$ is given by scalar matrices, and the quotient group $\mathrm{PWH}(d) \cong \mathrm{WH}(d)/\mathrm{Z}(\mathrm{WH}(d)) \cong (\mathbb{Z}/d\mathbb{Z})^2$.

Definition 2.2. For $\mathbf{w} \in \mathbb{C}^d$, its *Weyl–Heisenberg orbit* is

$$\mathrm{orb}_{\mathrm{WH}}(\mathbf{w}) := \{H\mathbf{w} : H \in \mathrm{WH}(d)\}.$$

Its associated set of complex lines, denoted $\mathrm{WHL}(\mathbf{w})$, is

$$\mathrm{WHL}(\mathbf{w}) := \{[\mathbf{w}] : \mathbf{w} \in \mathrm{orb}_{\mathrm{WH}}(\mathbf{w})\} = \{[H\mathbf{w}] : H \in \mathrm{PWH}(d)\}.$$

For any $\mathbf{w}$, $\mathrm{WHL}(\mathbf{w})$ has cardinality at most d^2, and for generic $\mathbf{w}$, exactly d^2.

Definition 2.3. A *Weyl–Heisenberg covariant SIC* (or simply a *Weyl–Heisenberg SIC*) is any $S(\mathbf{v}) := \mathrm{WHL}(\mathbf{v})$ for which $\mathbf{\Pi}(S)$ is a d-dimensional SIC. We denote the set of all Weyl–Heisenberg SICs in dimension d as $\mathrm{WHSIC}(d)$.

We call a generating vector $\mathbf{v}$ of a Weyl–Heisenberg SIC a *fiducial vector*. Such a vector is well-defined up to multiplication by a complex scalar $z \in \mathbb{C}^\times$. Each SIC has a choice of d^2 fiducial vectors, up to scalars.

Conjecture 2.4 (Strong Zauner Conjecture)**.** *For each dimension $d \geq 1$, there exists at least one Weyl–Heisenberg SIC.*

This conjecture is currently known by explicit constructions to hold for finitely many dimensions d, including $1 \leq d \leq 53$ and a extensive number of higher dimensions.

Conjecture 2.5 (Weyl–Heisenberg Boundedness Conjecture)**.** *For each dimension $d \geq 1$, except $d = 3$, there are finitely many Weyl–Heisenberg SICs.*

There are a few small dimensions where this conjecture has been proved rigorously, including $d \in \{1, 2, 4, 5, 6\}$. The cases $d = 1, 2$ may be done by hand; the cases $d = 4, 5, 6$ have been handled by computer using Gröbner bases [27, unpublished]. In higher dimensions, up to at least $d = 50$, it is supported by non-rigorous evidence given by numerical optimization routines repeatedly returning the same SICs [40,41]; see Table 5.1. In dimension 3, there is a one-parameter family of inequivalent Weyl–Heisenberg SICs.

A closely related conjecture is stated in Waldron [46, Sec. 14.27] as follows: *The algebraic variety of SIC fiducials is zero dimensional (and* nonempty*), except for $d = 3$, where it is one dimensional.* Resolving Conjecture 2.5 or Waldron's conjecture in general (and specifically even for $n = 7$) is an interesting open problem in optimization and real algebraic geometry.

2.2. **Geometric equivalence classes of Weyl–Heisenberg SICs.** There are two types of geometric operators acting on $\mathbb{C}^d$ that send SICs to SICs. Firstly, if U is a unitary matrix in $\mathbf{U}(d) = \{U \in \mathbf{GL}(\mathbb{C}^d) : UU^\dagger = 1\}$, and $S = \{\mathbb{C}\mathbf{v}_1, \ldots, \mathbb{C}\mathbf{v}_{d^2}\}$ is a SIC, then so is $US = \{\mathbb{C}U\mathbf{v}_1, \ldots, \mathbb{C}U\mathbf{v}_{d^2}\}$. (This is a *unitary equivalence*.) Secondly, if C_d is the complex conjugation operator acting pointwise on $\mathbb{C}^d$, so that $C_d\mathbf{v} := \overline{\mathbf{v}}$, then C_d also preserves the SIC property, as does any "antiunitary" operator of the form C_dU. These operators may be collected together to form the extended unitary group.

Definition 2.6. The *extended unitary group* is $\mathbf{EU}(d) := \mathbf{U}(d) \sqcup C_d\mathbf{U}(d)$. The *projective extended unitary group* $\mathbf{PEU}(d) := \mathbf{EU}(d)/\{zI : z \in \mathbb{C}, |z| = 1\}$.

All known SICs are group covariant, meaning that they are the orbit of a vector under the action of a finite subgroup of the unitary group.

Definition 2.7. A SIC S is *group covariant* for a subgroup G of $\mathbf{U}(d)$ if there exists a vector $v \in \mathbb{C}^d$, called a *fiducial vector*, such that $S = \{\mathbb{C}Av : A \in G\}$.

If $\mathbf{v}$ is a fiducial vector for a Weyl–Heisenberg covariant SIC and $U \in \mathbf{EU}(d)$, then the vector $U\mathbf{v}$ will be a fiducial vector for a SIC covariant for the group $G' = U\,\mathrm{WH}(d)U^{-1}$. All currently known SICs are unitary-equivalent to a Weyl–Heisenberg group $\mathrm{WH}(d)$ covariant SIC, with a single exception, the Hoggar lines in $\mathbb{C}^8$ [30, 31]. The Hoggar lines are group covariant for the tensor product $\mathrm{WH}(2) \otimes \mathrm{WH}(2) \otimes \mathrm{WH}(2)$. (The group $\mathrm{WH}(2) \otimes \mathrm{WH}(2) \otimes \mathrm{WH}(2)$ may itself be thought of as a generalized (Weyl)–Heisenberg group.)

The extended unitaries $U \in \mathbf{EU}(d)$ that preserve the Weyl–Heisenberg covariance property are precisely those for which $U\,\mathrm{WH}(d)U^{-1} = \mathrm{WH}(d)$, that is, elements of the extended Clifford group, defined as follows.

Definition 2.8. We define several closely related groups.

(1) The *Clifford group* $\mathrm{C}(d)$ is the normalizer of $\mathrm{WH}(d)$ in $\mathbf{U}(d)$.
(2) The *projective Clifford group* $\mathrm{PC}(d)$ is the quotient group of $\mathrm{C}(d)$ modulo its scalar matrix subgroup.
(3) The *extended Clifford group* $\mathrm{EC}(d)$ is the normalizer of $\mathrm{WH}(d)$ in $\mathbf{EU}(d)$.
(4) The *projective extended Clifford group* $\mathrm{PEC}(d)$ is the quotient of the extended Clifford group $\mathrm{EC}(d)$ modulo its scalar matrix subgroup.

The Clifford group $\mathrm{C}(d)$ is infinite because it contains a copy of $\mathbf{U}(1)$ as scalar matrices zI with $|z| = 1$; thus, $\mathrm{EC}(d)$ is infinite. The groups $\mathrm{PC}(d)$ and $\mathrm{PEC}(d)$ are finite groups. (The extended Clifford $\mathrm{EC}(d)$ group is studied in connection with SICs by Appleby [1].)

Definition 2.9. The set of *geometric equivalence classes of Weyl–Heisenberg SICs* is the set of equivalence classes of $\mathrm{WHSIC}(d)$ under the equivalence relation $[S(\mathbf{v})] \sim [S(U\mathbf{v})]$ whenever $U \in \mathrm{PEC}(d)$ (equivalently, whenever $U \in \mathrm{EC}(d)$.) This set of equivalence classes is denoted $\mathrm{WHSIC}(d)/\,\mathrm{PEC}(d)$. (It is not a group.) We denote the geometric equivalence class of a Weyl–Heisenberg SIC S by $[S]$.

3. Fields generated by SICs

In this section, we define several number fields attached to arbitrary SICs. Many of these fields have been studied before, often within the context of assuming various conjectures about SICs. Here, we focus on relationships between "SIC fields" that can be proven rigorously, either in general (Section 3.1) or in the case of Weyl–Heisenberg SICs (Section 3.2).

In Section 4, we will focus on SICs expressible in terms of algebraic numbers and discuss some conditional results about fields generated by SICs in that setting.

3.1. **Fields generated by general SICs.** The fields we study here are each associated to an individual SIC S and depend only on data computed from the orthogonal projections $\{\Pi_i : 1 \le i \le d^2\}$ defining the SIC.

Definition 3.1. Let $\mathbf{\Pi}(S) = \{\frac{1}{d}\Pi_1, \dots, \frac{1}{d}\Pi_{d^2}\}$ be an arbitrary SIC in dimension d, with each $\Pi_i = \mathbf{v}_i\mathbf{v}_i^\dagger$ for a *unit vector* $\mathbf{v}_i$. (Thus each $\mathbf{v}_i$ is unique up to multiplication by a unit scalar.)

(1) The *ratio SIC field* $F^{\mathrm{vec}}(S)$ is the field extension of $\mathbb{Q}$ generated by all the ratios v_{ij}/v_{ik} (for $v_{ik} \neq 0$) of the entries of the d^2 fiducial vectors $\mathbf{v}_i$ of S.
(2) The *triple product SIC field* $F^{\mathrm{trip}}(S)$ is the field extension of $\mathbb{Q}$ generated by all the *triple products* $\mathrm{Tr}(\Pi_i\Pi_j\Pi_k)$ (also called 3-*vertex Bargmann invariants* [46, Sec. 8.2]).
(3) The *unitary invariant SIC field* $F^{\mathrm{inv}}(S)$ is the field extension of $\mathbb{Q}$ generated by all the *unitary invariants* $\mathrm{Tr}(\Pi_{i_1}\Pi_{i_2}\cdots\Pi_{i_n})$ for $n \in \mathbb{N}$ (also called *n-vertex Bargmann invariants* [46, Sec. 8.2]).
(4) The *projection SIC field* $F^{\mathrm{proj}}(S)$ is the field extension of $\mathbb{Q}$ generated by all the entries of the d^2 Hermitian projection matrices Π_j.
(5) The *extended projection SIC field* $F^{\mathrm{eproj}}(S) := F^{\mathrm{proj}}(S)(\xi_d)$, adjoining $\xi_d = -e^{\frac{\pi i}{d}}$.

A priori, these fields could be transcendental extensions of $\mathbb{Q}$, as happens in dimension $d = 3$.

Remark 3.2. These fields have previously been studied with various names and notations.

(1) The field $F^{\mathrm{vec}}(S)$ is the *SIC field* $\mathbb{Q}[S]$ attached to a general SIC S by Appleby, Flammia, McConnell, and Yard [9, p. 212 bottom], as used in Thm. 1 and Conj. 2 of that paper. By definition, this field is independent of scaling factors in the $\mathbf{v}_i$. It is determined by $\mathbf{\Pi}(S)$, because the ratios
$$\frac{v_{ij}}{v_{ik}} = \frac{v_{ij}\overline{v}_{ik}}{v_{ik}\overline{v}_{ik}} = \frac{(\Pi_i)_{jk}}{(\Pi_i)_{kk}}.$$
We may rescale each of the d^2 vectors in S to give $S = \{\mathbb{C}\mathbf{w}_i : 1 \le i \le d^2\}$ so that all entries of each $\mathbf{w}_i$ belong to $F^{\mathrm{vec}}(S)$. A given $\mathbf{v}_i = \left(v_{i0}, v_{i1}, \cdots, v_{i(d-1)}\right)^T$ has at least one nonzero entry, say v_{ik}, and we may set $\mathbf{w}_i = \frac{1}{v_{ik}}\mathbf{v}_i$, whence $w_{ij} = v_{ij}/v_{ik} \in F^{\mathrm{vec}}(S)$. The vectors $\mathbf{w}_i$ obtained this way may not be unit vectors.
It is stated as [9, Prop. 3] that, for a Weyl–Heisenberg SIC, the ratio SIC field is the same for any SIC $S' \in [S]$. The presented proof outline [9, Sec. 7.1] appears to assume some conjectural equivalences and characterizations of other related fields.
(2) Concerning the triple product SIC field $F^{\mathrm{trip}}(S)$, the fact that a SIC is determined up to unitary equivalence by its triple products was proved in 2011 by Appleby, Flammia, and Fuchs [3, Thm. 3]; see also [46, Cor. 8.1]. We show unconditionally that $F^{\mathrm{trip}}(S)$ is an invariant of the geometric $\mathrm{PEC}(d)$-orbit of a Weyl–Heisenberg SIC S; see Proposition 3.4.
(3) The unitary invariant SIC field $F^{\mathrm{inv}}(S)$ is generated by the full set of projective unitary invariants of a general finite set of lines in $\mathbb{C}^d$; see [14] and [46, Ch. 8, Thm. 8.2]. We show in Proposition 3.3 that $F^{\mathrm{trip}}(S) = F^{\mathrm{inv}}(S)$.
(4) The projection SIC field $F^{\mathrm{proj}}(S)$, in the special case that S is a Weyl–Heisenberg SIC, coincides with the field L appearing in [9, Sec. 7], defined as the smallest subfield of $\mathbb{C}$ generated by the entries $v_j\overline{v}_k$ of unit vectors generating $\Pi_{\mathbf{v}}$ taken over all d^2 projectors $\Pi_{\mathbf{v}}$ of a Weyl–Heisenberg SIC.
(5) The extended projection SIC field $F^{\mathrm{eproj}}(S)$ is the *SIC field* $\mathbb{E}$ as defined by Appleby, Flammia, McConnell, and Yard [8, Sec. 4] for any SIC projector S. This definition of the SIC field is also used in [6] and is treated in detail in [46, Sec. 14.20]. Appleby, Flammia, McConnell, and Yard [8] state that the field $\mathbb{E}$ is well-defined on the $\mathrm{PEC}(d)$-orbit $[S]$ of a Weyl–Heisenberg SIC S. We supply a proof in Proposition 3.8.

The next result establishes some inclusion relations among these fields.

Proposition 3.3. *Let S be an arbitrary line-SIC in dimension d. The fields associated to S are related in the following ways.*

(1) $F^{\mathrm{proj}}(S) = F^{\mathrm{vec}}(S)\,\overline{F^{\mathrm{vec}}(S)}$ *(the compositum of $F^{\mathrm{vec}}(S)$ and its complex conjugate field). In particular, $F^{\mathrm{proj}}(S)$ is invariant under complex conjugation.*

(2) $F^{\mathrm{trip}}(S) = F^{\mathrm{inv}}(S) \subseteq F^{\mathrm{proj}}(S)$.

Proof. Write $\mathbf{\Pi}(S) = \{\frac{1}{d}\Pi_1, \ldots, \frac{1}{d}\Pi_{d^2}\}$.

Proof of (1). Write $\Pi_i = \mathbf{v}_i\mathbf{v}_i^\dagger$, where $\mathbf{v}_i$ has entries v_{im} and $|\mathbf{v}_i|^2 = 1$, for $1 \le i \le d^2$. The entries of Π_i are of the form $v_{im}\overline{v}_{in}$ for $0 \le m, n \le d-1$ When both $v_{im} \neq 0$, $v_{in} \neq 0$, these entries can be expressed as

$$v_{im}\overline{v}_{in} = \frac{v_{im}\overline{v}_{in}}{|\mathbf{v}_i|^2} = \frac{1}{\sum_{p=0}^{d-1}(v_{ip}/v_{im})\overline{(v_{ip}/v_{in})}} \in F^{\mathrm{vec}}(S)\,\overline{F^{\mathrm{vec}}(S)},$$

where $0 \le m, n, p \le d-1$. Thus, $F^{\mathrm{proj}}(S) \subseteq F^{\mathrm{vec}}(S)\,\overline{F^{\mathrm{vec}}(S)}$. To show the reverse inclusion, note that for $v_{ik} \neq 0$,

$$v_{im}/v_{in} = \frac{v_{im}\overline{v}_{in}}{v_{im}\overline{v}_{im}} \text{ and } \overline{(v_{im}/v_{in})} = \frac{v_{in}\overline{v}_{im}}{v_{in}\overline{v}_{in}}.$$

Proof of (2). First, the inclusion $F^{\mathrm{inv}}(S) \subseteq F^{\mathrm{proj}}(S)$ of (2) follows because $\mathrm{Tr}(\Pi_{i_1}\Pi_{i_2}\cdots\Pi_{i_n})$ is an integer polynomial in the entries of the various Π_j.

Second, we show the equality $F^{\mathrm{trip}}(S) = F^{\mathrm{inv}}(S)$. Clearly $F^{\mathrm{trip}}(S) \subseteq F^{\mathrm{inv}}(S)$. To show the reverse inclusion, note that the Π_i form a basis for the space of $d \times d$ complex matrices, and express

$$\Pi_i\Pi_j = \sum_\ell \alpha_{ij}^\ell \Pi_\ell \tag{3.1}$$

for *structure constants* $\alpha_{ij}^\ell \in \mathbb{C}$, having $1 \le i, j, \ell \le d^2$. We have

$$\sum_\ell \alpha_{ij}^\ell = \mathrm{Tr}(\Pi_i\Pi_j) = \frac{\delta_{ij}d+1}{d+1}, \text{ where } \delta_{ij} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$$

Moreover, the triple products are related to the structure constants by

$$\begin{aligned} \mathrm{Tr}(\Pi_i\Pi_j\Pi_k) &= \sum_\ell \alpha_{ij}^\ell \,\mathrm{Tr}(\Pi_k\Pi_\ell) \\ &= \frac{d}{d+1}\alpha_{ij}^k + \frac{1}{d+1}\sum_\ell \alpha_{ij}^\ell \\ &= \frac{d}{d+1}\alpha_{ij}^k + \frac{\delta_{ij}d+1}{(d+1)^2}. \end{aligned}$$

Thus, $\alpha_{ij}^k = \frac{d+1}{d}\,\mathrm{Tr}(\Pi_i\Pi_j\Pi_k) - \frac{d(\delta_{ij}d+1)}{d+1}$, and the field generated over $\mathbb{Q}$ by the structure constants is $F^{\mathrm{trip}}(S)$. Moreover, using (3.1) repeatedly, we can express any product $\Pi_{i_1}\Pi_{i_2}\cdots\Pi_{i_n}$ in the $\{\Pi_\ell\}_\ell$-basis with coefficients that are integer polynomials in the structure constants. Thus, since $\mathrm{Tr}(\Pi_\ell) = 1$, $\mathrm{Tr}(\Pi_{i_1}\Pi_{i_2}\cdots\Pi_{i_n})$ is also an integer polynomial in the structure constants and is thus contained in $F^{\mathrm{trip}}(S)$. □

Proposition 3.4. *Let S be an arbitrary line-SIC in dimension d. Then the triple product field satisfies the invariance property $F^{\mathrm{trip}}(US) = F^{\mathrm{trip}}(S)$ for any $U \in \mathbf{EU}(d)$.*

Proof. Write $S = \{\mathbb{C}\mathbf{v}_i : 1 \le i \le d^2\}$, and set $\mathbf{\Pi}(S) = \{\frac{1}{d}\Pi_1, \ldots, \frac{1}{d}\Pi_{d^2}\}$ with $\Pi_i = \mathbf{v}_i\mathbf{v}_i^\dagger$. Then set $\mathbf{\Pi}(US) = \{\frac{1}{d}\Pi'_1, \ldots, \frac{1}{d}\Pi'_{d^2}\}$. Write $U = CV$, where C is identity or complex conjugation, and $V \in \mathbf{U}(d)$; then either $\Pi'_i = V^{-1}\Pi_i V$, or $\Pi'_i = V^{-1}\Pi_i^\top V$. In the first case, $\mathrm{Tr}(\Pi'_i\Pi'_j\Pi'_k) = \mathrm{Tr}(V^{-1}\Pi_i\Pi_j\Pi_k V) = \mathrm{Tr}(\Pi_i\Pi_j\Pi_k)$. In the second case,

$$\mathrm{Tr}(\Pi'_i\Pi'_j\Pi'_k) = \mathrm{Tr}\Big(V^{-1}\Pi_i^\top\Pi_j^\top\Pi_k^\top V\Big) = \mathrm{Tr}\Big((\Pi_k\Pi_j\Pi_i)^\top\Big) = \mathrm{Tr}(\Pi_k\Pi_j\Pi_i).$$

So $F^{\mathrm{trip}}(US) = F^{\mathrm{trip}}(S)$ in both cases. □

We derive some unconditional implications when these fields give Galois extensions of $\mathbb{Q}$.

Lemma 3.5. *Let S be an arbitrary line-SIC in dimension d.*

(1) *If $F^{\mathrm{vec}}(S)$ is invariant under complex conjugation σ_c, then $F^{\mathrm{vec}}(S) = F^{\mathrm{proj}}(S)$. Thus, if $F^{\mathrm{vec}}(S)$ is a Galois extension of $\mathbb{Q}$, then $F^{\mathrm{proj}}(S)$ is a Galois extension of $\mathbb{Q}$.*
(2) *If $F^{\mathrm{proj}}(S)$ is a Galois extension of $\mathbb{Q}$, then $F^{\mathrm{eproj}}(S)$ is a Galois extension of $\mathbb{Q}$.*

Proof. The implication $F^{\mathrm{vec}}(S) = F^{\mathrm{proj}}(S)$ follows from Proposition 3.3(1). Moreover, if $K = F^{\mathrm{proj}}(S)$ is Galois over $\mathbb{Q}$, then $F^{\mathrm{eproj}}(S)$ is the compositum KL, with $L = \mathbb{Q}(e^{\frac{\pi i}{d}})$ an abelian extension of $\mathbb{Q}$, so the compositum is a Galois extension of $\mathbb{Q}$. □

3.2. **Fields generated by Weyl–Heisenberg SICs.** We now derive some properties of the fields $F^{\mathrm{vec}}(S)$, $F^{\mathrm{trip}}(S)$, $F^{\mathrm{proj}}(S)$, and $F^{\mathrm{eproj}}(()\,S)$ in the special case of Weyl–Heisenberg SICs.

Proposition 3.6. *Let S be a Weyl–Heisenberg line-SIC $S = S([\mathbf{v}])$ of dimension $d \geq 2$. Then:*

(1) *The field $F^{\mathrm{trip}}(S)$ contains the d-th root of unity $\zeta_d = e^{\frac{2\pi i}{d}}$.*
(2) *The field $F^{\mathrm{proj}}(S) \subseteq L(S) = F^{\mathrm{trip}}(S)(\sqrt[d]{\beta_1}, \sqrt[d]{\beta_2})$, for some $\beta_1, \beta_2 \in F^{\mathrm{trip}}(S)$. $L(S)$ is an abelian extension of $F^{\mathrm{trip}}(S)$ whose degree divides d^2, hence $[F^{\mathrm{proj}}(S) : F^{\mathrm{trip}}(S)]$ divides d^2.*
(3) *The index $[F^{\mathrm{eproj}}(S) : F^{\mathrm{proj}}(S)] \in \{1, 2\}$. It is 1 whenever d is odd.*

Proof. Let $\mathbf{v} = (v_0, v_1, \ldots, v_{d-1})^\top$ be a fiducial vector for S, and let $\Pi = \mathbf{v}\mathbf{v}^\dagger$. For X, Z as in Definition 2.1, let $D_{\mathbf{p}} = X^{p_1}Z^{p_2}$. Then, for $0 \leq p_1 < d$ and $0 \leq p_2 < d$, the vectors $\mathbf{v}_{\mathbf{p}} = X^{p_1}Z^{p_2}\mathbf{v}$ form a set of generating set of vectors of the SIC, all having $\|\mathbf{v}_{\mathbf{p}}\|^2 = \|\mathbf{v}\|^2$. Here $\mathbf{p} = (p_1, p_2) \in (\mathbb{Z}/p\mathbb{Z})^2$, and we also write $\mathbf{v}_i$ with $i = (d-1)p_1 + p_2$ having $1 \leq i \leq d^2$. We note for column vectors $\mathbf{w}_i$ that

$$\begin{aligned}\langle \mathbf{w}_1, \mathbf{w}_2\rangle\langle \mathbf{w}_2, \mathbf{v}_3\rangle\langle \mathbf{w}_3, \mathbf{w}_1\rangle &= \mathrm{Tr}\left(\mathbf{w}_1^\dagger\mathbf{w}_2\mathbf{w}_2^\dagger\mathbf{w}_3\mathbf{w}_3^\dagger\mathbf{w}_1\right)\\ &= \mathrm{Tr}\left(\mathbf{w}_1\mathbf{w}_1^\dagger\mathbf{w}_2\mathbf{w}_2^\dagger\mathbf{w}_3\mathbf{w}_3^\dagger\mathbf{w}_3\right)\\ &= \mathrm{Tr}\left(\Pi_{\mathbf{w}_1}\Pi_{\mathbf{w}_2}\Pi_{\mathbf{w}_3}\right)\end{aligned}$$

is a triple product, and similarly for r-fold cyclic scalar products of $\mathbf{w}_i$.

Proof of (1). The ratio of triple inner products

$$\begin{aligned}\frac{\langle \mathbf{v}, X^{-1}\mathbf{v}\rangle\langle X^{-1}\mathbf{v}, Z\mathbf{v}\rangle\langle Z\mathbf{v}, \mathbf{v}\rangle}{\langle \mathbf{v}, Z^{-1}\mathbf{v}\rangle\langle Z^{-1}\mathbf{v}, X\mathbf{v}\rangle\langle X\mathbf{v}, \mathbf{v}\rangle} &= \frac{\langle X\mathbf{v}, \mathbf{v}\rangle\langle \mathbf{v}, XZ\mathbf{v}\rangle\langle Z\mathbf{v}, \mathbf{v}\rangle}{\langle Z\mathbf{v}, \mathbf{v}\rangle\langle \mathbf{v}, ZX\mathbf{v}\rangle\langle X\mathbf{v}, \mathbf{v}\rangle}\\ &= \frac{\langle \mathbf{v}, XZ\mathbf{v}\rangle}{\langle \mathbf{v}, ZX\mathbf{v}\rangle} = \zeta_d.\end{aligned}$$

Via the SIC relations $|\langle \mathbf{v}_i, \mathbf{v}_j\rangle| = \frac{1}{d+1}\,|\mathbf{v}|^2$, if $i \neq j$, and $\|\mathbf{v}\|^2$ if $i = j$, all factors in these ratios are nonzero. Therefore $\zeta_d \in F^{\mathrm{trip}}(S)$.

Proof of (2). Set $\nu_{\mathbf{p}} = \langle \mathbf{v}, D_{\mathbf{p}}\mathbf{v}\rangle$. Set $\alpha_1 := \nu_{(1,0)} = \langle \mathbf{v}, X\mathbf{v}\rangle$ and $\alpha_2 = \nu_{(0,1)} = \langle \mathbf{v}, Z\mathbf{v}\rangle$. Define the field $L(S) := F^{\mathrm{trip}}(S)\,(\alpha_1, \alpha_2)$. By (1), $\zeta_d \in F^{\mathrm{trip}}(S)$.

To show $F^{\mathrm{proj}}(S) \subseteq L(S)$, it suffices =to show that all entries $(\Pi_i)_{k,\ell} \in L(S)$ for $1 \leq i \leq d^2$ and $0 \leq k, \ell < d$. Set $\mathbf{e}_1 = (1, 0)$ and $\mathbf{e}_2 = (0, 1)$. Now for $\mathbf{p} = p_1\mathbf{e}_1 + p_2\mathbf{e}_2$, the product $\nu_{\mathbf{e}_1}^{p_1}\nu_{\mathbf{e}_2}^{p_2}\nu_{-\mathbf{p}}$ is a $(p_1 + p_2 + 1)$-fold product (up to multiplication by a d-th root of unity), and thus by Proposition 3.3(2), $\nu_{\mathbf{e}_1}^{p_1}\nu_{\mathbf{e}_2}^{p_2}\nu_{-\mathbf{p}} \in F^{\mathrm{trip}}(S)\,(\alpha_1, \alpha_2, \zeta_d)$. We conclude that all $\nu_{-\mathbf{p}}$ are in

$F^{\mathrm{trip}}(S)\,(\alpha_1, \alpha_2, \zeta_d)$. The $D_{\mathbf{p}}$ form a basis of the matrix algebra $\mathrm{Mat}_{d\times d}(\mathbb{Q}(e^{\frac{2\pi i}{d}}))$. In particular all the matrices $E_{k,\ell}$ for $0 \le k, \ell \le d-1$ with entry 1 in the (k, ℓ) position and 0 elsewhere are linear combinations of the D_p over the field $\mathbb{Q}(e^{\frac{2\pi i}{d}})$. Thus $(\Pi_1)_{k,\ell} = \langle \mathbf{v}, E_{k,\ell}\mathbf{v}\rangle \in F^{\mathrm{trip}}(S)\,(\alpha_1, \alpha_2) = L(S)$. Now for $i = (d-1)p_1 + p_2$ we have

$$(\Pi_i)_{k,\ell} = \langle X^{p_1} Z^{p_2}\mathbf{v}, E_{k,\ell} X^{p_1} Z^{p_2}\mathbf{v}\rangle = (\Pi_1)_{k,\ell}$$

holding for all $1 \le i \le p^2$, by unitarity. Hence $(\Pi_i)_{k,\ell} \in L(S)$ for all i, k, ℓ. We conclude that $F^{\mathrm{proj}}(S) \subseteq L(S)$.

Finally, the product $\beta_1 = (\alpha_1)^d = \nu_{\mathbf{e}_1}^d = \nu_{\mathbf{e}_1}^d \nu_0$ is also a $(d+1)$-fold cyclic product and thus is in $F^{\mathrm{inv}}(S) = F^{\mathrm{trip}}(S)$, and similarly for $\beta_2 = (\alpha_2)^d = \nu_{\mathbf{e}_2}^d \in F^{\mathrm{trip}}(S)$. Thus $\alpha_1 = \sqrt[d]{\beta_1}$ and $\alpha_2 = \sqrt[d]{\beta_2}$ are both d-th roots of elements of $F^{\mathrm{trip}}(S)$. Since $\zeta_d \in F^{\mathrm{trip}}(S)$ we conclude adjoining these two elements to $F^{\mathrm{trip}}(S)$ gives an abelian extension $L(S)$ of $F^{\mathrm{trip}}(S)$, which is a Kummer extension whose degree divides d^2. The field $L(S)$ contains $F^{\mathrm{proj}}(S)$, and $F^{\mathrm{trip}}(S) \subseteq F^{\mathrm{proj}}(S)$, which implies $[F^{\mathrm{proj}}(S) : F^{\mathrm{trip}}(S)]$ divides d^2.

Proof of (3). By (1), since $F^{\mathrm{trip}}(S) \subseteq F^{\mathrm{proj}}(S)$, we have $\zeta_d \in F^{\mathrm{proj}}(S)$. Now $F^{\mathrm{eproj}}(S) = F^{\mathrm{proj}}(S)\,(e^{\frac{\pi i}{d}})$ is at most a quadratic extension of $F^{\mathrm{proj}}(S)$, since the field index $[\mathbb{Q}(e^{\frac{\pi i}{d}}) : \mathbb{Q}(e^{\frac{2\pi i}{d}})] = 2$ if d is even and is 1 if d is odd. ☐

We now study the field $F^{\mathrm{eproj}}(S)$ on the $\mathrm{PEC}(d)$-orbit of S and show it is a $\mathrm{PEC}(d)$-invariant. We recall a characterization of generators of the Clifford group.

Proposition 3.7. *The Clifford group* $\mathrm{C}(d)$ *is generated by all unitary scalar matrices* zI *with* $|z| = 1$*, together with*

$$X, Z, F, R$$

where X, Z *are Weyl–Heisenberg group generators,* F *is the discrete Fourier transform*

$$F_{j,k} = \frac{1}{\sqrt{d}} e^{\frac{2\pi i jk}{d}} \quad \text{for } 0 \le j, k \le d-1,$$

and R *is a diagonal matrix with diagonal entries*

$$R_{j,j} = \xi_d^{j(j+d)} = (-1)^{jd} e^{\frac{\pi i j^2}{d}} \quad \text{for } 0 \le j \le d-1.$$

Proof. This is [46, Thm. 14.1]. Every group element is a product of finitely many generators, with exactly one use of a unitary scalar matrix zI. ☐

Proposition 3.8. *Let* S *be a Weyl–Heisenberg line-SIC* $S = S([\mathbf{v}])$ *of dimension* d*.*

(1) *For any* $M \in \mathrm{EC}(d)$*,*

$$F^{\mathrm{eproj}}(MS) = F^{\mathrm{eproj}}(S)\,,$$

where MS *denotes the Weyl–Heisenberg line-SIC having fiducial vector* $\mathbf{w} := M\mathbf{v}$*.*

(2) $F^{\mathrm{eproj}}(S)$ *is equal to the compositum of all the* $F^{\mathrm{proj}}(MS)$ *for* $M \in \mathrm{EC}(d)$*.*

Proof. Proof of (1). To show $F^{\mathrm{eproj}}(MS) = F^{\mathrm{eproj}}(S)$, note that scalar matrices zI with $|z| = 1$ act trivially on projections, with $(zI\mathbf{v})(zI\mathbf{v})^\dagger = \mathbf{v}\mathbf{v}^\dagger$. The matrices X, Z, and F all have entries in $\mathbb{Q}(\xi)$ (where $\xi = \xi_d = -e^{\frac{\pi i}{d}}$). The matrix $\sqrt{d}F$ also has entries in $\mathbb{Q}(\xi)$, and $(F\mathbf{v})(F\mathbf{v})^\dagger = \frac{1}{d}(\sqrt{d}F\mathbf{v})(\sqrt{d}F\mathbf{v})^\dagger$. Writing any $M \in EC(d)$ as a finite product of the generators given in Proposition 3.7 shows that $(M\mathbf{v})(M\mathbf{v})^\dagger = M\mathbf{v}\mathbf{v}^\dagger M^\dagger$ has entries in $F^{\mathrm{eproj}}(S)$ (the compositum of $F^{\mathrm{proj}}(S)$ and $\mathbb{Q}(\xi)$). This argument shows $F^{\mathrm{proj}}(MS) \subseteq F^{\mathrm{eproj}}(S)$, so $F^{\mathrm{eproj}}(MS) \subseteq F^{\mathrm{eproj}}(S)$. By considering M^{-1}, we also have $F^{\mathrm{eproj}}(S) = F^{\mathrm{eproj}}\big(M^{-1}MS\big) \subseteq F^{\mathrm{eproj}}(MS)$, so $F^{\mathrm{eproj}}(MS) = F^{\mathrm{eproj}}(S)$.

Proof of (2). To show $F^{\mathrm{eproj}}(S)$ is equal to the compositum of all the $F^{\mathrm{proj}}(MS)$, it suffices to show that $\xi = -e^{-\frac{\pi i}{d}}$ occurs in the compositum of two fields $F^{\mathrm{proj}}(S)$ and $F^{\mathrm{proj}}(RS)$ where R is the element of $\mathrm{C}(d)$ given in Proposition 3.7. Given a fiducial $\mathbf{v}$ generating $S = S([\mathbf{v}])$ having

$v_0v_1 \neq 0$, we consider the fiducial vector $\mathbf{w} = R\mathbf{v}$ of a geometrically equivalent SIC. It has entries $(R\mathbf{v})_j = \xi^{j(j+d)}v_j$ so $R\mathbf{v}_0 = v_0$ and $R\mathbf{v}_1 = \xi v_1$. Therefore $\Pi' = \mathbf{w}\mathbf{w}^\dagger$ has

$$(\Pi')_{1,0} = \xi v_1 \overline{v}_0 \in F^{\mathrm{proj}}(RS)\,,$$

while $v_1\overline{v}_0 \in F^{\mathrm{proj}}(S)$. Now $v_0v_1 \neq 0$ implies we may take their quotient in the compositum field and so get $\xi_d \in F^{\mathrm{proj}}(S)\,F^{\mathrm{proj}}(RS)$, as required. □

4. Algebraic SICs and the Galois action

We now treat the subclass of algebraic SICs, for which the fields defined in Section 3.1 are algebraic number fields. In this paper, $\overline{\mathbb{Q}}$ is defined to be the algebraic closure of $\mathbb{Q}$ inside $\mathbb{C}$, so there is a canonical choice of complex conjugation automorphism $\sigma_c \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $\sigma_c(z) = \overline{z}$. We show that there is a well-defined Galois action on algebraic SICs and that the property of S being an algebraic SIC is preserved by the subgroup of all automorphisms $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ that commute with σ_c when restricted to the Galois closure of $F^{\mathrm{proj}}(S)$.

It is conjectured for dimensions $d \neq 3$ that all Weyl–Heisenberg SICs are algebraic. In Section 4.3, we define a combined geometric and Galois action on all algebraic Weyl–Heisenberg SICs and classify them into multiplets.

4.1. Algebraic SICs.

We consider SICs generated by algebraic vectors.

Definition 4.1. A complex line $\mathbb{C}\mathbf{v}$ generated by a nonzero vector $\mathbf{v} \in \mathbb{C}^d$ is a *projective-algebraic line* if all the ratios $v_i/v_j \in \overline{\mathbb{Q}}$ (for $v_j \neq 0$). (The definition is independent of the choice of $\mathbf{v}$.) A nonzero vector such that $\mathbb{C}\mathbf{v}$ is a projective-algebraic line is called a *projective-algebraic vector*.

An *algebraic vector* is any $\mathbf{v} \in \overline{\mathbb{Q}}^d$. For a projective-algebraic vector $\mathbf{v}$, its $\overline{\mathbb{Q}}$-*equivalence class* is

$$[[\mathbf{v}]]_{\mathrm{alg}} := \left\{\lambda\mathbf{v} : \lambda \in \mathbb{C} \text{ and } \lambda\mathbf{v} \in \overline{\mathbb{Q}}^d\right\}.$$

The next result implies that the algebraic class $[[\mathbf{v}]]_{\mathrm{alg}}$ of an algebraic complex line always includes algebraic unit vectors.

Lemma 4.2. *If $\mathbf{v} \in \mathbb{C}^d$ is a projective-algebraic vector, then there exists $\lambda \in \mathbb{C}^\times$ such that $\mathbf{x} = \lambda\mathbf{v}$ is algebraic and $|\mathbf{x}| = 1$. The $\overline{\mathbb{Q}}$-equivalence class $[[\mathbf{x}]]_{\mathrm{alg}}$ is independent of λ.*

Proof. Let $\mathbf{v}$ have some $v_i \neq 0$ and set $\mu = \frac{1}{v_i}$. Then $\mathbf{w} := \mu\mathbf{v} = \left(\frac{v_0}{v_i}, \frac{v_1}{v_i}, \ldots, \frac{v_{d-1}}{v_i}\right) \in \overline{\mathbb{Q}}^d$ by the projective-algebraicity of $\mathbf{v}$. Now the complex conjugates $\sigma_c\!\left(\frac{v_k}{v_i}\right) = \frac{\overline{v}_k}{\overline{v}_i}$ are algebraic numbers, hence so is $\left|\frac{v_k}{v_i}\right|^2$. Thus, $|\mathbf{w}| = \sqrt{\sum_k \left|\frac{v_k}{v_i}\right|^2}$ is a positive real algebraic number. We set $\lambda = \frac{\mu}{|\mathbf{w}|}$ and obtain the required $\mathbf{x} := \lambda\mathbf{v} = \frac{\mathbf{w}}{|\mathbf{w}|}$, having $|\mathbf{x}| = 1$.

Finally, if λ and λ' give two algebraic $\mathbf{x}, \mathbf{x}'$, necessarily $\lambda'/\lambda \in \overline{\mathbb{Q}}$. □

Definition 4.3. A d-dimensional line-SIC $S = \{\mathbf{v}_i : 1 \leq i \leq d^2\}$ is *algebraic* if each of its d^2 vectors $\mathbf{v}_i$ are projective-algebraic (or equivalently, if $F^{\mathrm{vec}}(S)$ is a finite extension of $\mathbb{Q}$).

Lemma 4.4. *Algebraic line-SICs satisfy the following properties.*

1. *A line-SIC is algebraic if and only if, for unit vectors $\mathbf{v}_i$, all the SIC projection matrices $\{\Pi_{\mathbf{v}_i} : 1 \leq i \leq d^2\}$ have algebraic number entries.*
2. *For an algebraic SIC S, the fields $F^{\mathrm{vec}}(S)$, $F^{\mathrm{trip}}(S)$, $F^{\mathrm{proj}}(S)$ and $F^{\mathrm{eproj}}(S)$ are algebraic number fields, that is, finite algebraic extensions of $\mathbb{Q}$.*
3. *A Weyl–Heisenberg line-SIC with fiducial vector $\mathbf{v}$ is an algebraic SIC if and only if $\mathbf{v}$ is a projective-algebraic vector.*

Proof. Proof of (1). This follows using Lemma 4.2.

Proof of (2). That $F^{\mathrm{vec}}(S)$ is an algebraic number field follows directly from the definition of algebraic. Given a line-SIC specified by d^2 projective algebraic lines $\mathbb{C}\mathbf{v}_i$, using (1) we immediately have $F^{\mathrm{trip}}(S)$ being an algebraic number field. Furthermore, one may rescale all $\mathbf{v}_i$ to be algebraic unit vectors by Lemma 4.2. Now the associated projection matrices $\Pi_{\mathbf{v}} = \mathbf{v}_i\mathbf{v}_i^\dagger$ have all entries in $\overline{\mathbb{Q}}$, so $F^{\mathrm{proj}}(S)$ is an algebraic number field. Finally, $F^{\mathrm{eproj}}(S)$ is a finite extension of $F^{\mathrm{proj}}(S)$.

Proof of (3). If the fiducial vector $\mathbf{v}$ of a Weyl–Heisenberg line-SIC S is projective-algebraic, then by Lemma 4.2, $\mathbf{v}$ may be rescaled to be an algebraic unit vector $\mathbf{w} = \lambda\mathbf{v}$. The Weyl–Heisenberg group $\mathrm{WH}(d)$ consists of matrices with algebraic entries, hence its action on $\mathbf{w}$ shows that all $\mathbf{w}_i$ for $1 \le i \le d^2$ are algebraic, so S is an algebraic line-SIC. The converse direction is immediate. ☐

4.2. **Galois actions on algebraic SICs.** There is a well-defined action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on algebraic complex lines which maps them to other algebraic complex lines. Given $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $\mathbf{v} \in \overline{\mathbb{Q}}^d$, we send $\mathbf{v}\mathbb{C} \mapsto \sigma(\mathbf{v})\mathbb{C}$. This action is well-defined on algebraic complex lines, since if $\lambda \in \overline{\mathbb{Q}}^\times$, then $\mathbf{v}\mathbb{C} = \lambda\mathbf{v}\mathbb{C}$ while

$$\sigma(\lambda\mathbf{v})\mathbb{C} = \sigma(\lambda)\sigma(\mathbf{v})\mathbb{C} = \sigma(\mathbf{v})\mathbb{C}.$$

Under this Galois action, the image under σ of d^2 algebraic complex lines will be d^2 algebraic complex lines. If these algebraic lines form a line-SIC, then the image set of lines can be either the same SIC, a different SIC, or not a SIC at all.

For a particular SIC, there is a restricted set of Galois automorphisms (which may depend on the line-SIC) that map it to another line-SIC.

Definition 4.5. Let $\sigma_c \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ denote complex conjugation and E an algebraic Galois extension of $\mathbb{Q}$. Let $C(\sigma_c\,|\,E)$ denote the centralizer of σ_c restricted to $\mathrm{Gal}(E/\mathbb{Q})$, that is,

$$C(\sigma_c\,|\,E) := \{\sigma \in \mathrm{Gal}(E/\mathbb{Q}) : \sigma\sigma_c(\alpha) = \sigma_c\sigma(\alpha) \text{ for all } \alpha \in E\}.$$

It is a subgroup of $\mathrm{Gal}(E/\mathbb{Q})$.

For a algebraic line-SIC S, we will show there is a Galois field E (depending on S) for which $C(\sigma_c\,|\,E)$ is such a restricted set. Since neither the field $F^{\mathrm{proj}}(S)$ nor $F^{\mathrm{eproj}}(S)$ is known to always be a Galois extension of $\mathbb{Q}$, we give a name to the Galois closure of $F^{\mathrm{eproj}}(S)$.

Definition 4.6. Given an algebraic line-SIC S, let $F^{\mathrm{Gproj}}(S)$ denote the normal closure of $F^{\mathrm{eproj}}(S)$ over $\mathbb{Q}$, and call it the *Galois-projection SIC field* of S.

The next proposition shows that $C(\sigma_c \mid F^{\mathrm{Gproj}}(S))$ is a group of Galois automorphisms that preserve the property of being an algebraic line-SIC. For $d \ge 2$, the group $C(\sigma_c \mid F^{\mathrm{Gproj}}(S))$ is always nontrivial because it contains complex conjugation, which acts nontrivially because $F^{\mathrm{proj}}(S)$ cannot be contained in $\mathbb{R}$. (A set of real equiangular lines in $\mathbb{R}^d$ has cardinality at most $\frac{d(d+1)}{2} < d^2$.)

Proposition 4.7. *Let S be an algebraic line-SIC. If $\sigma \in C(\sigma_c\,|\,F^{\mathrm{Gproj}}(S))$, then $\sigma(S)$ is also an algebraic line-SIC, and $F^{\mathrm{Gproj}}(\sigma(S)) = F^{\mathrm{Gproj}}(S)$.*

Proof. Write the line-SIC and (projection) SIC as

$$S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{d^2}\},$$
$$\mathbf{\Pi}(S) = \left\{\tfrac{1}{d}\Pi_1, \tfrac{1}{d}\Pi_2, \ldots, \tfrac{1}{d}\Pi_{d^2}\right\},$$

where $\mathbf{v}_i$ are unit vectors. By definition of $F^{\mathrm{proj}}(S)$, the entries of all the Π_i lie in $F^{\mathrm{proj}}(S)$, so they lie in $F^{\mathrm{Gproj}}(S)$. Also, using the commutativity of σ and σ_c,

$$\sigma(\Pi_i) = \sigma(\mathbf{v}_i\sigma_c(\mathbf{v}_i)^\top) = \sigma(\mathbf{v}_i)\sigma(\sigma_c(\mathbf{v}_i)^\top) = \sigma(\mathbf{v}_i)\sigma_c(\sigma(\mathbf{v}_i)^\top)$$

is the Hermitian projection onto $\sigma(\mathbf{v}_i)$, hence

$$\mathbf{\Pi}(\sigma(S)) = \left\{\tfrac{1}{d}\sigma(\Pi_1), \tfrac{1}{d}\sigma(\Pi_2), \ldots, \tfrac{1}{d}\sigma(\Pi_{d^2})\right\}.$$

Moreover,

$$\mathrm{Tr}(\sigma(\Pi_i)\sigma(\Pi_j)) = \sigma(\mathrm{Tr}(\Pi_i\Pi_j)) = \sigma\left(\tfrac{\delta_{ij}d+1}{d+1}\right) = \tfrac{\delta_{ij}d+1}{d+1},$$

certifying that $\mathbf{\Pi}(\sigma(S))$ is a SIC. Finally, $F^{\mathrm{Gproj}}(\sigma(S)) \subseteq F^{\mathrm{Gproj}}(S)$, because the entries of Π_i lie in $F^{\mathrm{Gproj}}(S)$, and $F^{\mathrm{Gproj}}(S)$ is Galois over $\mathbb{Q}$, hence $\sigma(F^{\mathrm{Gproj}}(S) = F^{\mathrm{Gproj}}(S)$. It follows by symmetry that $F^{\mathrm{Gproj}}(S) = F^{\mathrm{Gproj}}\big(\sigma^{-1}(\sigma(S))\big) \subseteq F^{\mathrm{Gproj}}(\sigma(S))$ and thus $F^{\mathrm{Gproj}}(\sigma(S)) = F^{\mathrm{Gproj}}(S)$. □

4.3. **Galois multiplets and super-equivalence classes of Weyl–Heisenberg SICs.** We now assemble PEC(d)-orbits of Weyl–Heisenberg SICs in dimension d into *multiplets* under the Galois action by the subgroup $C(\sigma_c\,|\,F^{\mathrm{Gproj}}(S))$ of $\mathrm{Gal}(F^{\mathrm{Gproj}}(S)\,/\mathbb{Q})$ that commutes with complex conjugation. The coarser equivalence classes obtained under the combined geometric and Galois actions (i.e., unions of the orbits in a multiplet) will be called *Galois super-equivalence classes.*

The conjecture of Appleby, Flammia, McConnell, and Yard [9, Conj. 2] implies that many of the fields we have been studying are equivalent Galois extensions of $\mathbb{Q}$.

Lemma 4.8. *Assume Conjecture 1.1 holds. Then in every dimension $d \geq 4$, for each Weyl–Heisenberg line-SIC S, the field $F^{\mathrm{vec}}(S)$ is a finite Galois extension of $\mathbb{Q}$, and*

$$F^{\mathrm{vec}}(S) = F^{\mathrm{proj}}(S) = F^{\mathrm{eproj}}(S) = F^{\mathrm{Gproj}}(S)\,.$$

Proof. By Conjecture 1.1(2), $F^{\mathrm{vec}}(S)$ is a Galois extension of $\mathbb{Q}$. Consequently, $F^{\mathrm{vec}}(S)$ is preserved by complex conjugation, so $F^{\mathrm{vec}}(S) = F^{\mathrm{proj}}(S)$ holds by Lemma 3.5(1).

Also by Conjecture 1.1(2), $F^{\mathrm{vec}}(S)$ always contains the ray class field $H_{d'\infty_1\infty_2}$ of $\mathbb{Q}(\Delta_d)$. This class field must contain the class field of $\mathbb{Q}$ with conductor $d'\infty$, which is $\mathbb{Q}(\zeta_{d'}) = \mathbb{Q}(\xi_d)$. Therefore, $F^{\mathrm{vec}}(S)$ contains $F^{\mathrm{proj}}(S)\,(\xi_d) = F^{\mathrm{eproj}}(S)$. Since $F^{\mathrm{vec}}(S) \subseteq F^{\mathrm{proj}}(S) \subseteq F^{\mathrm{eproj}}(S)$, equality of those three fields follows. So $F^{\mathrm{eproj}}(S)$ is Galois and hence equal to $F^{\mathrm{Gproj}}(S)$. □

The evidence for a Galois action on Weyl–Heisenberg SICs was extensively detailed by Appleby, Yadsan-Appleby, and Zauner [4] in 2013. The group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the elements of Weyl–Heisenberg group WH(d) coordinatewise on its matrices. Any automorphism $\sigma : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$, sending a matrix $H \mapsto \sigma(H)$, acts as a homomorphism $\sigma(H_1H_2) = \sigma(H_1)\sigma(H_2)$. This Galois action fixes the group WH(d) as a set, with any automorphism permuting its elements, since every Galois conjugate $\sigma(H)$ of a group element H is also an element of WH(d).

By Proposition 3.8(2), $F^{\mathrm{eproj}}(S)$ is an invariant of the PEC(d) orbit of the Weyl–Heisenberg SIC S, hence so is its Galois closure $F^{\mathrm{Gproj}}(S)$. Thus the field $F^{\mathrm{Gproj}}(S)$ is invariant under both the geometric and the Galois actions.

The following definition coincides with "Galois multiplet" as defined in [8].

Definition 4.9. For $d \geq 4$, the *Galois multiplet* of a PEC(d)-equivalence class $[S]$ of Weyl–Heisenberg line-SICs is

$$[[S]] = \{[\sigma(S)] : \sigma \in C(\sigma_c\,|\,F^{\mathrm{Gproj}}(S))\}.$$

We also define an associated equivalence relation $\approx_{GPEC}$, termed *Galois super-equivalence*, by

$$[S_1] \approx_{GPEC} [S_2] \iff [[S_1]] = [[S_2]],$$

and term the union of the elements $[S_i]$ of $[[S]]$ the *Galois super-equivalance class of S.*

We summarize the properties noted above in the following proposition.

Proposition 4.10. *Assume Conjecture 1.1 holds. Then for $d \geq 4$ the set* WHSIC(d) *is partitioned into a finite number of Galois super-equivalence classes under the equivalence relation $\approx_{GPEC}$. Each Galois super-equivalence class is a finite union of (geometric)* PEC(d)*-equivalence classes.*

Galois multiplets in a fixed dimension often have different sizes.

5. Conjectures on counting geometric equivalence classes and Galois multiplets of Weyl–Heisenberg SICs

In this section, we formulate two conjectures relating the number of SICs in dimensions $d \geq 4$ to class numbers of certain real quadratic orders. Both these conjectures are numerically testable, and they are consequences of Conjecture 1.2.

5.1. Class groups and class monoids of orders.

Let K be a number field. An *order* in K is any subring $\mathcal{O}$ including 1 that is finitely additively generated and whose rational span $\mathbb{Q}\mathcal{O} = K$. There is a unique *maximal order* $\mathcal{O}_K$ of K that contains all the others; $\mathcal{O}_K$ coincides with the set of algebraic integers in K. The maximal order is a Dedekind domain, while every non-maximal order is not a Dedekind domain. In particular, a non-maximal order will have non-invertible nonzero ideals. However, the set of *invertible* ideals of a non-maximal order behaves much like set of nonzero ideals in a Dedekind domain.

Recall that a *fractional ideal* of a (commutative) integral domain $\mathcal{O}$ is a finitely generated $\mathcal{O}$-module $\mathfrak{m}$ contained in its quotient field K. A fractional ideal $\mathfrak{a}$ is *invertible* if there exists a fractional ideal $\mathfrak{b}$ with $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. Dedekind domains are characterized by the property that all nonzero fractional ideals are invertible.

The class group of an order, defined in terms of invertible fractional ideals, generalizes the usual notion of the class group of (the maximal order of) a number field.

Definition 5.1. The *class group* (also called the *Picard group* or *ring class group*) of an order $\mathcal{O}$ is

$$\mathrm{Cl}(\mathcal{O}) := \frac{\{\text{invertible fractional ideals of } \mathcal{O}\}}{\{\text{principal fractional ideals of } \mathcal{O}\}}.$$

If one instead considers *all* nonzero ideals, one obtains a monoid (that is, a semigroup with identity) rather than a group.

Definition 5.2. The *class monoid* of an order $\mathcal{O}$ is

$$\mathrm{Clm}(\mathcal{O}) := \frac{\{\text{nonzero fractional ideals of } \mathcal{O}\}}{\{\text{principal fractional ideals of } \mathcal{O}\}}.$$

For a more in-depth discussion of the nuances of orders, see [34] and [37, Ch. I, Sec. 12].

If K is a quadratic field of discriminant Δ_0, it has a unique suborder of discriminant $f^2\Delta_0$ for every positive integer f. This order is given explicitly as

$$\mathcal{O}_\Delta := \mathbb{Z}\left[\frac{\Delta + \sqrt{\Delta}}{2}\right] = \mathbb{Z} + \frac{\Delta + \sqrt{\Delta}}{2}\mathbb{Z} = \mathbb{Z} + f\frac{\Delta_0 + \sqrt{\Delta_0}}{2}\mathbb{Z}.$$

For the SIC problem, we specifically consider the case when $\Delta = \Delta_d = (d+1)(d-3)$ for some integer d. In this case, the class monoid $\mathrm{Clm}(\mathcal{O}_{\Delta_d})$ may be understood through bijections with other sets of number-theoretic interest.

Theorem 5.3. *Suppose $d \in \mathbb{Z} \setminus \{-1, 3\}$, and let $\Delta = (d+1)(d-3)$. Write $\Delta_d = f^2\Delta_0$ for some $f \in \mathbb{N}$ and a fundamental discriminant Δ_0. Then there are explicit, canonical bijections between the sets*

(0) $\mathrm{Clm}(\mathcal{O}_\Delta)$;
(1) *the disjoint union* $\bigsqcup_{f' \mid f} \mathrm{Cl}(\mathcal{O}_{(f')^2\Delta_0})$;
(2) *the set* $\mathcal{Q}(\Delta)/\mathbf{GL}_2(\mathbb{Z})$, *where* $\mathcal{Q}(\Delta)$ *is the set of binary quadratic forms of discriminant* Δ, *and* $A = \left(\begin{smallmatrix} s & t \\ u & v \end{smallmatrix}\right) \in \mathbf{GL}_2(\mathbb{Z})$ *acts on the right by* $Q^A(x,y) = (\det A)Q(sx+ty, ux+vy)$; *and*
(3) *the set* $\mathcal{C}_{d-1} = \{\{R^{-1}AR : R \in \mathbf{GL}_2(\mathbb{Z})\} : A \in \mathbf{SL}_2(\mathbb{Z}), \mathrm{Tr}(A) = d-1\}$ *of* $\mathbf{GL}_2(\mathbb{Z})$*-conjugacy class of elements of* $\mathbf{SL}_2(\mathbb{Z})$ *of trace* $d-1$.

Proof. The bijection between (0) and (1) holds for quadratic orders in general. Specifically, by Halter-Koch [28, Sec. 5.5], one has, as sets, $\mathrm{Clm}(\mathcal{O}_\Delta) = \bigsqcup_{f'|f} \mathrm{Cl}(\mathcal{O}_{(f')^2\Delta_0})$.

The bijection between (0) and (2) also holds for quadratic orders in general (and with appropriate modifications, nondegenerate quadratic rings) and is known as twisted Gauss composition. This is proven as [47, Thm. 1.2]; for an introduction to Gauss composition, see [15, Ch. 5].

We now exhibit a bijection between (2) and (3) which specifically holds only for $\Delta = (d+1)(d-3)$. It is defined by a map $\phi : \mathcal{Q}(\Delta) \to \mathbf{GL}_2(\mathbb{Z})$ that induces the bijection. For a quadratic form $Q(x,y) = ax^2 + bxy + cy^2$ of discriminant $\Delta = (d+1)(d-3)$, define $\phi(Q) := \begin{pmatrix} \frac{1}{2}(b+d-1) & -a \\ c & \frac{1}{2}(-b+d-1) \end{pmatrix}$. Note that

$$\det(\phi(Q)) = \frac{1}{4}(-b^2 + (d-1)^2) + ac = \frac{1}{4}(-\Delta + (d-1)^2) = 1$$

and $\mathrm{Tr}(\phi(Q)) = d-1$. It is straightforward to check that $\phi(Q^R) = R^{-1}\phi(Q)R$ for $R \in \mathbf{GL}_2(\mathbb{Z})$. Thus, ϕ defines a map $\overline{\phi} : \mathcal{Q}(\Delta)/\mathbf{GL}_2(\mathbb{Z}) \to \mathcal{C}_{d-1}$. In the other direction, for $A = \left(\begin{smallmatrix} s & t \\ u & v \end{smallmatrix}\right) \in \mathbf{SL}_2(\mathbb{Z})$, define the quadratic form $(\psi(A))(x,y) := -tx^2 + (s-v)xy + uy^2$. It is straightforward to check that $\mathrm{disc}(\psi(A)) = \Delta$ and $\psi(R^{-1}AR) = \psi(A)^R$, so ψ defines a map $\overline{\psi} : \mathcal{C}_{d-1} \to \mathcal{Q}(\Delta)/\mathbf{GL}_2(\mathbb{Z})$. A direct calculation shows $\overline{\phi} \circ \overline{\psi} = \mathrm{id}$ and $\overline{\psi} \circ \overline{\phi} = \mathrm{id}$. $\square$

5.2. **Statement of the Geometric Count Conjecture.** The following conjecture counts the number of geometric equivalence classes of Weyl–Heisenberg SICs in dimension d. It is implied by Conjecture 1.2.

Conjecture 5.4 (Geometric Count Conjecture)**.** *Fix a positive integer $d \neq 3$, and let $\Delta = (d+1)(d-3)$ and $\mathcal{O}_\Delta$ be the quadratic order of discriminant Δ. Then, the number of geometric equivalence classes $[S]$ of Weyl–Heisenberg covariant SICs is*

$$|\mathrm{WHSIC}(d)/\,\mathrm{PEC}(d)| = |\mathrm{Clm}(\mathcal{O}_\Delta)|\,.$$

By Theorem 5.3, the quantity $|\mathrm{Clm}(\mathcal{O}_\Delta)|$ is equal to

(1) the sum of (ring) class numbers $\sum_{f'|f} h_{(f')^2\Delta_0}$, where $h_{(f')^2\Delta_0} = \left|\mathrm{Cl}(\mathcal{O}_{(f')^2\Delta_0})\right|$;
(2) $|\mathcal{Q}(\Delta)/\mathbf{GL}_2(\mathbb{Z})|$, the number of twisted $\mathbf{GL}_2(\mathbb{Z})$-classes of binary quadratic forms of discriminant Δ;
(3) $|\mathcal{C}_{d-1}|$, the number of $\mathbf{GL}_2(\mathbb{Z})$-conjugacy class of elements of $\mathbf{SL}_2(\mathbb{Z})$ of trace $d-1$.

Conjecture 5.4 immediately gives an upper bound for the total number of Weyl–Heisenberg line-SICs in dimensions $d \geq 4$.

Proposition 5.5. *Conjecture 5.4 implies that the number $|\mathrm{WHSIC}(d)|$ of Weyl–Heisenberg line-SICs in dimensions $d \geq 4$ satisfies*

$$|\mathrm{WHSIC}(d)| \leq \frac{|\mathrm{PEC}(d)|}{d^2}\,|\mathrm{Clm}(\mathcal{O}_{\Delta_d})|\,.$$

Proof. The number of distinct Weyl–Heisenberg line-SICs in a $\mathrm{PEC}(d)$-equivalence class $[S]$ is $\frac{|\mathrm{PEC}(d)|}{|\mathrm{stab}(S)|}$, where $\mathrm{stab}(S)$ is the subgroup of $\mathrm{PEC}(d)$ stabilizing a line-SIC $S \in [S]$. The cardinality $|\mathrm{stab}(S)|$ is independent of the choice of $S \in [S]$. The Weyl–Heisenberg group $\mathrm{WH}(d)$ acts transitively on the set of d^2 complex lines in the $\mathrm{WH}(d)$-orbit of a fiducial vector, so $\mathrm{WH}(d)$ is a subgroup of $\mathrm{stab}(S)$. Thus d^2 divides $|\mathrm{stab}(S)|$. Hence we have $\frac{|\mathrm{PEC}(d)|}{|\mathrm{stab}(S)|} \leq \frac{|\mathrm{PEC}(d)|}{d^2}$. The result now follows from Conjecture 5.4. $\square$

Remark 5.6. Table 5.1 presents, in the column labeled $|\mathrm{WHSIC}(d)|$, empirical data for the number of observed (numerical) SICs for $4 \leq d \leq 50$ from Scott and Grassl [41, Table 1]. That table also observes that all known numerical Weyl–Heisenberg SICs of dimensions $4 \leq d \leq 50$ have an additional stabilizer element of order 3. If this statement were true in general, then we could strengthen Proposition 5.5 to conclude

$$|\mathrm{WHSIC}(d)| \leq \frac{1}{3}\frac{|\mathrm{PEC}(d)|}{d^2}\,|\mathrm{Clm}(\mathcal{O}_{\Delta_d})| \tag{5.1}$$

holds for all $d \geq 4$. Examination of Table 5.1 shows for known numerical SICs that (5.1) holds for $4 \leq d \leq 50$ and that equality in (5.1) holds for

$$d \in \{5, 13, 17, 23, 25, 27, 29, 37, 41, 43, 47, 49\}.$$

5.3. **Verification of cases of the Geometric Count Conjecture.** We have verified that the two sets in the Geometric Count conjecture have the same size for dimensions $4 \leq d \leq 90$, under the assumption that the published lists of Weyl–Heisenberg SICs in these dimensions, given in Scott [40], are complete. (The list builds on earlier work of Scott and Grassl [41].)

Proposition 5.7 (Empirical Proposition 1)**.** *For dimensions d with $\Delta = (d+1)(d-3)$, the total number of* $\mathrm{PEC}(d)$ *equivalence classes* $[S]$ *of numerical SICs equals* $|\mathrm{Clm}(\mathcal{O}_\Delta)|$ *for* $4 \leq d \leq 50$ *in the Scott and Grassl list [41], and for* $51 \leq d \leq 90$ *in the Scott list [40].*

Proof. For $4 \leq d \leq 90$, we computed $|\mathrm{Clm}(\mathcal{O}_\Delta)|$ using Magma [16] by computing the equivalent quantity $|\mathcal{Q}(\Delta)/\mathbf{GL}_2(\mathbb{Z})|$.

Write $\Delta = (d+1)(d-3) = f^2\Delta_0$ for a fundamental discriminant Δ_0. Recall that for any quadratic order

$$\mathrm{Clm}(\mathcal{O}_\Delta) = \bigsqcup_{f'|f} \mathrm{Cl}(\mathcal{O}_{(f')^2\Delta_0}).$$

For each $f' \,|\, f$, we computed the set of reduced primitive binary quadratic forms of discriminant $(f')^2\Delta_0$ using the Magma function `ReducedForms()`, written by David Kohel. This function produces a list of $\mathbf{SL}_2(\mathbb{Z})$-classes of primitive binary quadratic forms in which a twisted $\mathbf{GL}_2(\mathbb{Z})$-class is always represented either by a single form $ax^2 + bxy + cy^2$ with $a > 0$ or a pair of forms $\{ax^2 + bxy + cy^2, -ax^2 + bxy - cy^2\}$. Removing forms with $a < 0$ produced a list containing one representative for each primitive twisted $\mathbf{GL}_2(\mathbb{Z})$-class. Multiplying by f/f' and joining the lists gave a list of representatives of all (not necessarily primitive) classes in $\mathcal{Q}(\Delta)/\mathbf{GL}_2(\mathbb{Z})$. The counts of quantities for the different f' are given are the unordered set of all ring class numbers $h_{(f')^2\Delta_0} = \left|\mathrm{Cl}(\mathcal{O}_{(f')^2\Delta_0})\right|$. They are given in column labeled by $h_{(f')^2\Delta_0}$ in Table 5.1. The total counts of class numbers are , are given in the column labeled by $|\mathrm{Clm}(\mathcal{O}_\Delta)|$.

Numerical Weyl–Heisenberg SICs are systems of d^2 complex lines that are the Weyl–Heisenberg orbit of a single numerical fiducial vector and that appears to have equal angles to 10 decimal places. Numerical SICs are produced as output of an optimization algorithm. Empirical counts for the number of $\mathrm{PEC}(d)$-equivalence classes of numerical SICs were given by Scott and Grassl for $4 \leq d \leq 50$ [41, Tab. 1 and Tab. 2] and by Scott [40, pp. 3–6] for $51 \leq d \leq 90$. The classes in the tables are denoted by dimension and letter, eg., $31a$. Tab. 1 of [41] contains the subset of exact SICs, grouped into Galois multiplets, while Tab. 2 of [41] gives a list of numerical SICs, not grouped into Galois multiplets. In both cases one can count the total number of $\mathrm{PEC}(d)$-equivalence classes.

We also found agreement for all dimensions $51 \leq d \leq 90$ of $|\mathrm{Clm}(\mathcal{O}_{\Delta_d})|$ given in Table 5.2 with the total count of $\mathrm{PEC}(d)$-classes of SICs in each dimension listed in [40, Appendix C]. ☐

d	Δ	Δ_0	f'	$\sigma_0(f)$	$h_{(f')^2\Delta_0}$	$\lvert\mathrm{Clm}(\mathcal{O}_\Delta)\rvert$	d	$\lvert\mathrm{WHSIC}(d)\rvert$	$\frac{\lvert\mathrm{PEC}(d)\rvert}{d^2}$	#
1	-4	-4	1	1	1	1	1	1	1	1
2	-3	-3	1	1	1	1	2	2	12	1
3	0	0	$\mathbb{N}$	∞	1	∞	3	∞	48	∞
4	5	5	1	1	1	1	4	16	96	1
5	12	12	1	1	1	1	5	80	240	1
6	21	21	1	1	1	1	6	96	288	1
7	32	8	1, 2	2	1, 1	2	7	336	672	2
8	45	5	1, 3	2	1, 1	2	8	320	768	2
9	60	60	1	1	2	2	9	864	1296	2
10	77	77	1	1	1	1	10	480	1440	1
11	96	24	1, 2	2	1, 2	3	11	2640	2640	3
12	117	13	1, 3	2	1, 1	2	12	1152	2304	2
13	140	140	1	1	2	2	13	2912	4368	2
14	165	165	1	1	2	2	14	2688	4032	2
15	192	12	1, 2, 4	3	1, 1, 2	4	15	6720	5760	4
16	221	221	1	1	2	2	16	4096	6144	2
17	252	28	1, 3	2	1, 2	3	17	9792	9792	3
18	285	285	1	1	2	2	18	5184	7776	2
19	320	5	1, 2, 4, 8	4	1, 1, 1, 2	5	19	16720	13680	5
20	357	357	1	1	2	2	20	7680	11520	2
21	396	44	1, 3	2	1, 4	5	21	26880	16128	5
22	437	437	1	1	1	1	22	5280	15840	1
23	480	120	1, 2	2	2, 4	6	23	48576	24288	6
24	525	21	1, 5	2	1, 2	3	24	15360	18432	3
25	572	572	1	1	2	2	25	20000	30000	2
26	621	69	1, 3	2	1, 3	4	26	34944	26208	4
27	672	168	1, 2	2	2, 4	6	27	69984	34992	6
28	725	29	1, 5	2	1, 2	3	28	26880	32256	3
29	780	780	1	1	4	4	29	64960	48720	4
30	837	93	1, 3	2	1, 3	4	30	46080	34560	4
31	896	56	1, 2, 4	3	1, 2, 4	7	31	138880	59520	7
32	957	957	1	1	2	2	32	32768	49152	2
34	1020	1020	1	1	4	4	33	84480	63360	4
34	1085	1085	1	1	2	2	34	39168	58752	2
35	1152	8	1, 2, 3, 4, 6, 12	6	1, 1, 1, 1, 2, 4	10	35	235200	80640	10
36	1221	1221	1	1	4	4	36	82944	62208	4
37	1292	1292	1	1	4	4	37	134976	101232	4
38	1365	1365	1	1	4	4	38	109440	82080	4
39	1440	40	1, 2, 3, 6	4	2, 2, 2, 4	10	39	314496	104832	10
40	1517	1517	1	1	2	2	40	61440	92160	2
41	1596	1596	1	1	8	8	41	367360	137360	8
42	1677	1677	1	1	4	4	42	129024	96768	4
43	1760	440	1, 2	2	2, 4	6	43	317856	158928	6
44	1845	205	1, 3	2	2, 4	6	44	253440	126720	6
45	1932	1932	1	1	4	4	45	207360	155520	4
46	2021	2021	1	1	3	3	46	145728	145728	3
47	2112	33	1, 2, 4, 8	4	1, 1, 2, 4	8	47	553472	207552	8
48	2205	5	1, 3, 7, 21	4	1, 1, 1, 4	7	48	276480	147456	7
49	2300	92	1, 5	2	1, 6	7	49	537824	230496	7
50	2397	2397	1	1	2	2	50	120000	180000	2

TABLE 5.1. Comparison for $1 \leq d \leq 50$ of ring class numbers with counts of SICs. The three rightmost columns are from [41, Table 1]. They include empirical data for $|\mathrm{WHSIC}(d)|$, and column # gives empirical data for $|\mathrm{WHSIC}(d)/\,\mathrm{PEC}(d)|$. The left columns give $\Delta = (d+1)(d-3) = f^2\Delta_0$ for a fund. disc. Δ_0, f' runs over divisors of f, $h_{(f')^2\Delta_0} = \left|\mathrm{Cl}(\mathcal{O}_{(f')^2\Delta_0})\right|$, and $\sigma_0(f) = |\{\mathcal{O} : \mathcal{O}_\Delta \subseteq \mathcal{O} \subseteq \mathcal{O}_{\Delta_0}\}|$.

d	Δ	Δ_0	f'	$\widetilde{\#}$	$h_{(f')^2\Delta_0}$	$\lvert\mathrm{Clm}(\mathcal{O}_\Delta)\rvert$	d	Δ	Δ_0	f'	$\widetilde{\#}$	$h_{(f')^2\Delta_0}$	$\lvert\mathrm{Clm}(\mathcal{O}_\Delta)\rvert$
51	2496	156	1, 2, 4	3	2, 4, 8	14	71	4896	136	1, 2, 3, 6	4	2, 4, 4, 8	18
52	2597	53	1, 7	2	1, 3	4	72	5037	5037	1	1	4	4
53	2700	12	1, 3, 5, 15	4	1, 1, 2, 6	10	73	5180	5180	1	1	4	4
54	2805	2805	1	1	4	4	74	5325	213	1, 5	2	1, 6	7
55	2912	728	1, 2	2	2, 4	6	75	5472	152	1, 2, 3, 6	4	1, 2, 4, 8	15
56	3021	3021	1	1	6	6	76	5621	5621	1	1	6	6
57	3132	348	1, 3	1	2, 6	8	77	5772	5772	1	1	8	8
58	3245	3245	1	1	4	4	78	5925	237	1, 5	2	1, 6	7
59	3360	840	1, 2	2	4, 8	12	79	6080	380	1, 2, 4	3	2, 4, 8	14
60	3477	3477	1	1	4	4	80	6237	77	1, 3, 9	3	1, 2, 6	9
61	3596	3596	1	1	6	6	81	6396	6396	1	1	12	12
62	3717	413	1, 3	2	1, 4	5	82	6557	6557	1	1	3	3
63	3840	60	1, 2, 4, 8	4	2, 2, 4, 8	16	83	6721	105	1, 2, 4, 8	4	2, 2, 4, 8	16
64	3965	3965	1	1	4	4	84	6885	85	1, 3, 9	3	2, 2, 6	10
65	4092	4092	1	1	8	8	85	7052	7052	1	1	4	4
66	4221	469	1, 3	2	3, 6	9	86	7221	7221	1	1	10	10
67	4352	17	1, 2, 4, 8, 16	5	1, 1, 1, 2, 4	9	87	7392	1848	1, 2	2	4, 8	12
68	4485	4485	1	1	4	4	88	7565	7565	1	1	4	4
69	4620	4620	1	1	8	8	89	7740	860	1, 3	2	2, 8	10
70	4757	4757	1	1	5	5	90	7917	7917	1	1	4	4

TABLE 5.2. Ring class numbers and ring class monoid numbers for $51 \le d \le 90$. Here $\Delta = (d+1)(d-3) = f^2\Delta_0$ for a fund. disc. Δ_0, f' runs over divisors of f, $h_{(f')^2\Delta_0} = \left|\mathrm{Cl}(\mathcal{O}_{(f')^2\Delta_0})\right|$, and $\widetilde{\#}$ is $|\{\mathcal{O} : \mathcal{O}_\Delta \subseteq \mathcal{O} \subseteq \mathcal{O}_{\Delta_0}\}| = \sigma_0(f)$. (The values $|\mathrm{Clm}(\mathcal{O}_\Delta)|$ agree with empirical data for $|\mathrm{WHSIC}(d)/\mathrm{PEC}(d)|$ of Scott [40]).

5.4. **Statement of the Multiplet Count Conjecture.** We showed in Proposition 4.10 that Conjecture 1.1 implies that there are a finite number of well-defined Galois multiplets of WHSICs in dimensions $d \ge 4$, each consisting of a finite number of geometric equivalence classes; we now refine this prediction to a precise count in every dimension.

Recall that a *fundamental discriminant* of a quadratic field is any (positive or negative) integer Δ_0 with $\Delta_0 \equiv 0, 1 \pmod 4$, $16 \nmid \Delta_0$, and the odd part of Δ_0 squarefree. Equivalently, Δ_0 is a fundamental discriminant if and only if it is the field discriminiant of $\mathbb{Q}(\sqrt{\Delta_0})$.

Conjecture 5.8 (Multiplet Count Conjecture). *Fix a positive integer $d \neq 3$. Let $\Delta = \Delta_d = (d+1)(d-3)$ and $K = \mathbb{Q}(\sqrt{\Delta})$. The number of Galois multiplets of Weyl–Heisenberg SICs in dimension d equals the number of quadratic orders $\mathcal{O}'$ with $\mathcal{O}_\Delta \subseteq \mathcal{O}' \subseteq \mathcal{O}_K$. That is,*

$$|\mathrm{WHSIC}(d)/\approx_{GPEC}| = \left|\{\mathcal{O}' : \mathcal{O}_\Delta \subseteq \mathcal{O}' \subseteq \mathcal{O}_K\}\right|.$$

(Note that, if we write $\Delta = f^2\Delta_0$ for a fundamental discriminant Δ_0, with $f > 0$, then

$$\left|\{\mathcal{O}' : \mathcal{O}_\Delta \subseteq \mathcal{O}' \subseteq \mathcal{O}_K\}\right| = \sigma_0(f),$$

where $\sigma_0(f)$ denotes the number of positive divisors of f.)

The content of Conjecture 5.8 is that the multiplets of Weyl–Heisenberg SICs are in one-to-one correspondence with orders between $\mathcal{O}_\Delta$ and $\mathcal{O}_K$.

An order in a quadratic field is determined uniquely by its discriminant, which can be $(f')^2\Delta_0$ for a fundamental discriminant Δ_0 and a positive integer f'. The order $\mathcal{O}_\Delta = \mathcal{O}_{f^2\Delta_0}$ is contained in $\mathcal{O}' = \mathcal{O}_{(f')^2\Delta_0}$ if and only if $f' \mid f$, so there are $\sigma_0(f)$ of them. The order $\mathcal{O}_{(f')^2\Delta_0}$ contains $\mathcal{O}_{f^2\Delta_0} = \mathcal{O}_\Delta$ if and only if $f' | f$. (These facts do not hold for general number fields.)

5.5. **Verification of cases of the Multiplet Count Conjecture.** We have verified that the two sets in the Multiplet Count Conjecture (Conjecture 5.8) have the same size for dimensions $d \leq 90$ ($d \neq 3$) under the assumption that the published lists of Weyl–Heisenberg SICs in these dimensions are complete.

Proposition 5.9 (Empirical Proposition 2)**.** *The total number of constructed Galois multiplets* $[[S]]$ *of exact SICs for dimensions*

$$d \in \{4, 5, 6, 7, 8, 9, 10, 11, 12, 23, 14, 15, 16, 17, 18, 19, 20, 21, 24, 28, 30, 35, 39, 48\} \tag{5.2}$$

equals the total number of orders

$$s(\mathcal{O}_{\Delta_d}) := \left|\{\mathcal{O}' : \mathcal{O}_\Delta \subseteq \mathcal{O}' \subseteq \mathcal{O}_{\Delta_0}\}\right|,$$

where $\Delta = (d+1)(d-3)$. *Equivalently, writing* $\Delta = f^2\Delta_0$, *where* Δ_0 *is a fundamental discriminant, this number* $s(\mathcal{O}_{\Delta_d}) = \sigma_0(f)$, *the number of positive divisors of* f. *(The function* $\sigma_0(f)$ *is also denoted* $\tau(f)$ *or* $d(f)$ *by some authors.)*

For the dimensions in (5.2), *there is at least one bijective map*

$$\mathcal{M} : \{\mathcal{O}' : \mathcal{O}_\Delta \subseteq \mathcal{O}' \subseteq \mathcal{O}_{\Delta_0}\} \to \{[[S]] : S \text{ a Weyl–Heisenberg line-SIC in } \mathbb{C}^d\}$$

such that the number of geometric equivalence classes $[S] \in \mathcal{M}(\mathcal{O}_{(f')^2\Delta_0})$ *is* $\left|\mathrm{Cl}(\mathcal{O}_{(f')^2\Delta_0})\right|$.

Proof. The result follows from comparison of [6, Tab. 1 and Tab. 2] on known exact SICs with the number theoretic data on $h_{(f')^2\Delta_0}$ from our Table 5.1. Here [6, Tab. 1] gives results of Scott and Grassl [41] for exact multiplets for $4 \leq d \leq 16$, excluding $d = 15$; [6, Tab. 2] gives the remaining exact multiplets in (5.2). Each Galois multiplet contains a number of PEC(d)-orbits, indicated by letters; for example, the multiplet 35*bcdg* consists of four PEC(35)-orbits.

In the dimensions in (5.2), the number of Galois multiplets is found to agree with the data for $s(\mathcal{O}_{\Delta_d}) = \sigma_0(f)$, given in column $\sigma_0(f)$ of Table 5.1.

The existence of a bijective map $\mathcal{M}$ is equivalent to the assertion that the unordered multiset of candinalities $|\{[S] \in [[S]]\}|$ of PEC(d)-orbits of SICs in each Galois multiplet is equal to the unordered multiset of ring class numbers $h_{(f')^2\Delta_0}$ such that $f'|f$. The multiset equality was verified comparing the exact multiplet data of [6] with that in column labeled $h_{(f')^2\Delta_0}$ in Table 5.1. □

The bijective map $\mathcal{M}$ is not uniquely specified using these class number counts alone. However, when augmented by requiring agreement of all inclusion relations between the associated SIC fields $F^{\mathrm{proj}}(S)$, the truth of Conjecture 1.3 in dimension d uniquely determines the map $\mathcal{M}$ determined for the dimensions (5.2). (See Section 8.1; the smallest dimension where $\mathcal{M}$ is not determined by the inclusion relations is $d = 47$.)

Example 5.10. Let $d = 35$. Here $\Delta = 36 \cdot 32 = 2^7 \cdot 3^2$. Here $\Delta_0 = 8$ and $f = 12$. The set of divisors f' of 12 are $\{1, 2, 3, 4, 6, 12\}$.

We exhibit a bijection $\mathcal{M}$ of Conjecture 1.2 from orders to multiplets in Figure 5.1. This bijection satisfies part (1) of Conjecture 1.2 for $d = 35$. This choice of $\mathcal{M}$ also satisfies part (2) of Conjecture 1.2 for $d = 35$, as shown in Example 6.7.

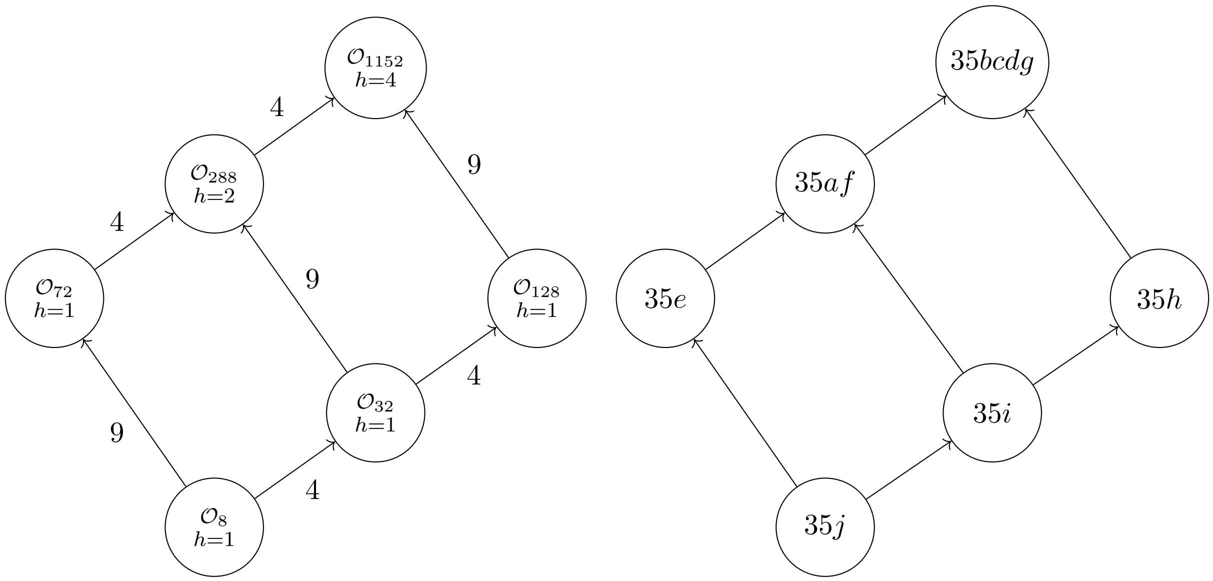

FIGURE 5.1. Left side: For $d = 35$, over-orders of $\mathcal{O}_{1152}$, and their ring class numbers $h = h_{\Delta_0(f')^2} = \left|\mathrm{Cl}(\mathcal{O}_{(f')^2\Delta_0})\right|$, with $\Delta_0 = 8$. The direction on edges indicate (reverse) set inclusions, with edge labels giving relative indices of orders. Thus $\mathcal{O}_{1152} \subset \mathcal{O}_8$ has index 144 in $\mathcal{O}_8$. Right side: For $d = 35$, $\mathcal{M}$-correspondence to Galois multiplets of $d = 35$ SICs, with multiplet letter labels ($35a$ to $35j$) corresponding to PEC(35)-equivalence classes of SICs. Class numbers match the number of orbit letter labels in each multiplet.

6. Conjectures on precise fields of definition of Weyl–Heisenberg SICs

In this section, we study the number-theoretic properties of the ray class fields of orders $\mathcal{O}'$ predicted to be fields of definition of Weyl–Heisenberg SICs by Conjecture 1.3. We give formulas for the degrees of those ray class field over K, by means of studying the associated ray class groups. In Proposition 6.6, we test numerical predictions of relative degrees and field inclusions implied by Conjecture 1.2 and Conjecture 1.3. We also study the relative degrees of field inclusions predicted in Conjecture 1.2(2), noting there exist cases where the map $\mathcal{M}$ is not uniquely determined by the conclusions of Conjecture 1.2 and Conjecture 1.3. Before studying the special ray class fields conjecturally associated to SICs, we summarize some properties of ray class fields of orders in general.

6.1. **Ray class fields of orders.** The fields attached to a Weyl–Heisenberg SIC are believed to be abelian extensions of $K = \mathbb{Q}(\sqrt{\Delta_d})$. Class field theory gives an abstract description of abelian extensions of K, viewed with respect to the ideals of the maximal order $\mathcal{O}_K$. Conjecture 1.2 implies that a Weyl–Heisenberg SIC can unambiguously be assigned an order $\mathcal{O}$ of K with $\mathbb{Z}[\varepsilon_d] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$. There is a long history of work which supplies a notion of class field theory attached to orders of number fields. In particular, the *ring class field* of an order $\mathcal{O}$ has Galois group over K isomorphic to $\mathrm{Cl}(\mathcal{O})$ and generalizes the *Hilbert class field*, which is the maximal unramified extension of K and has class group $\mathrm{Cl}(\mathcal{O}_K)$.

In [34], the authors modify the standard constructions of class field theory to describe a distinguished collection of *ray class fields of orders* $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}$, each specified by a *level datum* $(\mathcal{O}; \mathfrak{m}, \Sigma)$, where $\mathcal{O}$ is a (possibly non-maximal) order of K, $\mathfrak{m}$ an integral $\mathcal{O}$-ideal, and Σ a subset of real places of K. In the case that K is real quadratic, there are two infinite places, so Σ is one of $\emptyset$, $\{\infty_1\}$, $\{\infty_2\}$, or $\{\infty_1, \infty_2\}$. For the datum $(\mathcal{O}; \mathcal{O}, \emptyset)$, the associated field $H^{\mathcal{O}}_{\mathcal{O},\emptyset}$ is the ring class field associated to the order. For the datum $(\mathcal{O}_K; \mathfrak{m}, \Sigma)$, the associated field $H^{\mathcal{O}_K}_{\mathfrak{m},\Sigma}$ is the standard (Takagi) ray class field $H_{\mathfrak{m},\Sigma}$. For a fixed order $\mathcal{O}$, any abelian extension of K as a subfield of some $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}$.

We recall [34, Thm. 1.1]:

Theorem 6.1. *Let K be a number field and $(\mathcal{O}; \mathfrak{m}, \Sigma)$ a level datum for K. There exists a unique abelian Galois extension $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}/K$ with the property that a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ that is coprime to the quotient ideal $(\mathfrak{m} : \mathcal{O}_K)$ splits completely in $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}/K$ if and only if $\mathfrak{p} \cap \mathcal{O} = \pi\mathcal{O}$, a principal prime $\mathcal{O}$-ideal having $\pi \in \mathcal{O}$ with $\pi \equiv 1 \pmod{\mathfrak{m}}$ and $\rho(\pi) > 0$ for $\rho \in \Sigma$.*

To understand Theorem 6.1, recall that for any integral ideal $\mathfrak{m}$ of $\mathcal{O}$, the quotient ideal $(\mathfrak{m} : \mathcal{O}_K)$ is the largest ideal of $\mathcal{O}_K$ contained in $\mathfrak{m}$. An important invariant of an order $\mathcal{O}$ of an algebraic number field K is its (absolute) conductor $\mathfrak{f} = \mathfrak{f}(\mathcal{O}) = (\mathcal{O} : \mathcal{O}_K)$, which is the (set-theoretically) largest integral ideal $\mathfrak{f} \subseteq \mathcal{O}$ of $\mathcal{O}$ that is also an ideal of the maximal order $\mathcal{O}_K$. The conductor ideal $\mathfrak{f}(\mathcal{O})$ encodes information on all the non-invertible ideals in the order $\mathcal{O}$. The quotient ideal $(\mathfrak{m} : \mathcal{O}_K)$ always satisfies the inclusions (as $\mathcal{O}_K$-ideals)

$$\mathfrak{f}(\mathcal{O})\mathfrak{m} \subseteq (\mathfrak{m} : \mathcal{O}_K) \subseteq \mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}\mathcal{O}_K; \tag{6.1}$$

in particular, $(\mathfrak{m} : \mathcal{O}_K) \subseteq \mathfrak{f}(\mathcal{O})$. The three ideals in (6.1) have the same prime divisors: A prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ such that $\mathfrak{p} \supseteq \mathfrak{f}(\mathcal{O})\mathfrak{m} = \mathfrak{f}(\mathcal{O})\mathfrak{m}\mathcal{O}_K$ satisfies either $\mathfrak{p} \supseteq \mathfrak{f}(\mathcal{O})$ or $\mathfrak{p} \supseteq \mathfrak{m}\mathcal{O}_K$, and thus, $\mathfrak{p} \supseteq \mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}\mathcal{O}_K$.

There is a Galois correspondence between ray class groups of an order and ray class fields of an order. The *ray class group of an order* $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ for level datum $(\mathcal{O}; \mathfrak{m}, \Sigma)$ is defined as a quotient of certain groups of invertible fractional ideals of the order $\mathcal{O}$. The ray class field $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}$ of an order $\mathcal{O}$ is associated to an appropriate $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ in such a way that $\mathrm{Gal}(H^{\mathcal{O}}_{\mathfrak{m},\Sigma}/K) \simeq \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ as abelian groups. Moreover, if $(\mathcal{O}; \mathfrak{m}, \Sigma)$ and $(\mathcal{O}'; \mathfrak{m}', \Sigma')$ are level data satisfying $\mathcal{O} \subseteq \mathcal{O}'$, $\mathfrak{m}\mathcal{O}' \subseteq \mathfrak{m}'$, and $\Sigma \supseteq \Sigma'$, then there is a natural quotient map $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \twoheadrightarrow \mathrm{Cl}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')$ and a corresponding natural field inclusion $H^{\mathcal{O}'}_{\mathfrak{m}',\Sigma'} \subseteq H^{\mathcal{O}}_{\mathfrak{m},\Sigma}$.

We recall [34, Thm. 1.3]:

Theorem 6.2. *For an order $\mathcal{O}$ in a number field K and any level datum $(\mathcal{O}; \mathfrak{m}, \Sigma)$ with associated ray class field $H_0 := H^{\mathcal{O}}_{\mathfrak{m},\Sigma}$, there is an isomorphism $\mathrm{Art}_{\mathcal{O}} : \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \to \mathrm{Gal}(H_0/K)$, uniquely determined by its behavior on prime $\mathcal{O}$-ideals $\mathfrak{p}$ coprime to $\mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}$, having the property that*

$$\mathrm{Art}_{\mathcal{O}}([\mathfrak{p}])(\alpha) \equiv \alpha^q \pmod{\mathfrak{P}}, \tag{6.2}$$

where $\mathfrak{P}$ is any prime of $\mathcal{O}_{H_0}$ lying over $\mathfrak{p}\mathcal{O}_K$, and $q = p^j$ is the number of elements in the finite field $\mathcal{O}/\mathfrak{p}$. For any (not necessarily prime) ideal $\mathfrak{a}$ of $\mathcal{O}$ coprime to $\mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}$,

$$\mathrm{Art}_{\mathcal{O}}([\mathfrak{a}]) = \mathrm{Art}([\mathfrak{a}\mathcal{O}_K])|_{H_0},$$

where $\mathrm{Art} : \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K) \to \mathrm{Gal}(H_1/K)$ is the usual Artin map in class field theory, with $H_1 = H^{\mathcal{O}_K}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}$ being a (Takagi) ray class field for the maximal order $\mathcal{O}_K$, and $H_0 \subseteq H_1$.

In Theorem 6.2, the set of prime ideals coprime to $\mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}$ includes all but finitely many of the prime ideals of $\mathcal{O}$. The Artin map is fully defined by (6.2), which specifies the map on prime ideals of $\mathcal{O}$ coprime to $\mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}$, because it turns out that any ray ideal class in $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ has a representative that is coprime to $\mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}$ (by [34, Lem. 4.12]), and ideals of $\mathcal{O}$ that are coprime to $\mathfrak{f}$ enjoy unique factorization into prime ideals (even though arbitrary nonzero ideals of $\mathcal{O}$ do not). When $\mathcal{O} = \mathcal{O}_K$, (6.2) specializes to the standard definition of the Artin map in the case of a Takagi ray class field.

6.2. **Special ray class fields of real quadratic orders.** We recall the fact that orders of a quadratic field K are completely specified by their discriminants $\Delta' = (f')^2\Delta_0$, where Δ_0 is the field discriminant of K (a fundamental discriminant; see the beginning of Section 5.4) and f' is a positive integer.

Definition 6.3. Fix a positive integer $d \geq 4$, write $\Delta = (d+1)(d-3) = f^2\Delta_0$ with Δ_0 a fundamental discriminant, and let f' be a positive divisor of f. Let $\Delta' = (f')^2\Delta_0$ and $\mathcal{O}' = \mathcal{O}_{\Delta'}$. We introduce two families of ray class fields of the order $\mathcal{O}'$ parametrized by d and f':

$$E_{d,f'} = H^{\mathcal{O}'}_{d\mathcal{O}',\{\infty_1,\infty_2\}} \quad \text{and} \quad \tilde{E}_{d,f'} := H^{\mathcal{O}'}_{d'\mathcal{O}',\{\infty_1,\infty_2\}}.$$

Here $d' = d$ if d is odd and $d' = 2d$ if d is even.

The definitions yield $E_{d,f'} = \tilde{E}_{d,f'}$ when d is odd, and the natural field inclusion $E_{d,f'} \subseteq \tilde{E}_{d',f'}$ when d is even. We have $[\tilde{E}_{d,f'} : E_{d,f'}] = 2$ when d is even, using Theorem 6.5(2) below.

The larger fields $\tilde{E}_{d,f'}$ appear in Conjecture 1.3, which asserts $\tilde{E}_{d,f'} = F^{\mathrm{proj}}(S)$ whenever $\mathcal{M}(\mathcal{O}') = [[S]]$. Conjecture 1.3 is a natural extension of Conjecture 1.1. Conjecture 1.1(1) is equivalent to the statement that $F^{\mathrm{proj}}(S) = \tilde{E}_{d,1}$ for any S in the minimal multiplet. In Appendix A the smaller fields $E_{d,f'}$ are conjecturally associated to $F^{\mathrm{trip}}(S)$ for $[[S]]$, the multiplet associated to $\mathcal{O}'$ by the map $\mathcal{M}$.

We wish to compute the degrees of these fields. The Galois correspondence of ray class field theory for orders (Theorem 6.2) implies that the degree of $\tilde{E}_{d,f'}$ (resp., $E_{d,f'}$) over $K = \mathbb{Q}(\sqrt{\Delta})$ equals the ray class number $\left|\mathrm{Cl}_{d'\mathcal{O}',\{\infty_1,\infty_2\}}(\mathcal{O}')\right|$ (resp., $\left|\mathrm{Cl}_{d\mathcal{O}',\{\infty_1,\infty_2\}}(\mathcal{O}')\right|$). Theorem 6.5 below gives a formula for these ray class numbers, valid for ray class groups of real quadratic orders specifically of the form $\Delta = (d+3)(d-1)$.

To state the formula, we define for the real quadratic field K the *number field totient function* $\varphi_K(n) = \left|(\mathcal{O}_K/n\mathcal{O}_K)^\times\right|$. It is computed by the following formula.

Lemma 6.4. *Let K be a quadratic field of discriminant Δ_0. Then*

$$\varphi_K(n) = n^2 \prod_{p|n} \left(1 - \frac{1}{p}\right)\left(1 - \left(\frac{\Delta_0}{p}\right)\frac{1}{p}\right), \tag{6.3}$$

where the product is over primes dividing n, and $\left(\frac{\Delta_0}{p}\right)$ is the Kronecker symbol.

Proof. The function $\varphi_K(n)$ is multiplicative by the Chinese remainder theorem. It is computed on prime powers by splitting into cases based on the splitting behavior of p in K, which is measured by the Kronecker symbol. A straightforward calculation yields (6.3). ☐

We now give formulas for the cardinality of various ray class groups $\left|\mathrm{Cl}_{d'\mathcal{O}',\Sigma}(\mathcal{O}')\right|$. We recall that for K a real quadratic field, the *regulator* Reg_K of K takes the value $\log\varepsilon$, where $\varepsilon = \varepsilon_K > 1$ is the fundamental unit of $\mathcal{O}_K$.

Theorem 6.5. *Let $d \geq 4$ and let $\Delta = (d+1)(d-3) = f^2\Delta_0$ for some fundamental discriminant Δ_0. Let $K = \mathbb{Q}(\sqrt{\Delta})$. Let $\varepsilon_d = \frac{(d-1)+\sqrt{\Delta}}{2}$, and let $\mathcal{O}'$ be a K-order such that $\mathbb{Z}[\varepsilon_d] \subseteq \mathcal{O}' \subseteq \mathcal{O}_K$, that is, with $\mathrm{disc}(\mathcal{O}') = (f')^2\Delta_0$ for some $f'|f$.*

(1) *Then*

$$\left|\mathrm{Cl}_{d\mathcal{O}',\Sigma}(\mathcal{O}')\right| = \begin{cases} \dfrac{2^{|\Sigma|}h_K \,\mathrm{Reg}_K\, \varphi_K(df')}{9\log(\varepsilon_d)\varphi(f')}, & \text{if } d \equiv 3 \pmod 9 \text{ and } 3|f', \\[2ex] \dfrac{2^{|\Sigma|}h_K \,\mathrm{Reg}_K\, \varphi_K(df')}{6\log(\varepsilon_d)\varphi(f')}, & \text{otherwise.} \end{cases} \tag{6.4}$$

(2) *If d is even, then $\left|\mathrm{Cl}_{2d\mathcal{O}',\Sigma}(\mathcal{O}')\right| = 2\left|\mathrm{Cl}_{d\mathcal{O}',\Sigma}(\mathcal{O}')\right|$.*

Proof. A proof is given in [36], taking $d = n + 1$.

For the reader's convenience, we include a proof in Appendix B. The proof depends on a specific congruence for the units in such orders, stated as Lemma B.1. □

6.3. **Evidence for the Ray Class Fields of Orders Conjecture.** Assuming the truth of Conjecture 1.3, the Galois correspondence of class field theory (Theorem 6.2) requires that the degree of $F^{\mathrm{proj}}(S)$ over $K = \mathbb{Q}(\sqrt{(d+1)(d-3)})$ equal the class number $\left|\mathrm{Cl}_{d\mathcal{O}',\{\infty_1,\infty_2\}}(\mathcal{O}')\right|$. We verify this numerical requirement.

Proposition 6.6 (Empirical Proposition 3)**.** *For each dimension d with $4 \leq d \leq 15$, there exists a bijective map $\mathcal{M}$ from orders to (empirical) constructed Galois multiplets. Taking $\Delta = (d+1)(d-3) = f^2\Delta_0$ and $K = \mathbb{Q}(\sqrt{\Delta})$, the map $\mathcal{M}$ may be chosen to have the property that, for any $f' \,|\, f$ and constructed SIC S such that $[[S]] = \mathcal{M}(\mathcal{O}_{((f')^2\Delta_0)})$, we have*

$$[F^{\mathrm{proj}}(S) : K] = [\tilde{E}_{d,f'} : K].$$

Proof. The numerical equalities are tabulated for $4 \leq d \leq 15$ and for $d = 35$ in Table 6.1 below. By the Galois correspondence of class field theory (Theorem 6.2) the degree of $\tilde{E}_{d,f'}$ over $K = \mathbb{Q}(\sqrt{(d+1)(d-3)})$ equals the class number $\left|\mathrm{Cl}_{d\mathcal{O}',\{\infty_1,\infty_2\}}(\mathcal{O}')\right|$. We computed the relevant class numbers using the right side of (6.4).

The empirical calculations of field degrees $[F^{\mathrm{proj}}(S) : K]$ is based on data for these fields given in [41, Tab. III] and in [6, Tab. A7]. The calculations of field degrees $[F^{\mathrm{proj}}(S) : K]$ for multiplets $[[S]]$ of exact SICs for $d = 15$ and $d = 35$ also appear in [6, Tab. A7]. The field is $\mathbb{E}_1$; the degree for $\mathbb{E}$ given in the table must be divided by 4, because the degree in [6, Tab. A7] is given over $\mathbb{Q}$, and because $\mathbb{E} = \mathbb{E}_1(i)$, an extension of degree 2 since $\mathbb{E}_1$ does not contain i for odd $d \geq 4$. For inclusions of fields for $d = 35$, we made use of additional calculations [2, unpublished], which determined the inclusions between the fields $F^{\mathrm{proj}}(S)$ in the six multiplets $[[S]]$ of exact SICs for $d = 35$, correcting the picture in [6, Fig. 1], by showing the field associated to multiplet $35e$ is contained in the field associated to multiplet $35af$.

The inclusions of fields $\tilde{E}_{d,f'}$ coincide exactly with the reverse ordering of the lattice of divisibility relations of the set $\{f' : f' \geq 1,\ f' \,|\, f\}$. On comparison we find there exists a unique bijection $\mathcal{M}$ for all the dimensions in Table 6.1 compatible with the field inclusions. In Table 6.1 the orbit labels in the "multiplet" column are based on Flammia's online table [22], following [6, 40, 41], specifically using the labels for exact SICs, which differ in some cases from Scott and Grassl's labels for numerical SICs [41]. The correspondence between the columns labeled f' and "multiplet" in Table 6.1 specifies the map $\mathcal{M}$. □

Example 6.7. We illustrate in Figure 6.1 a choice of map $\mathcal{M}$ in the case $d = 35$, matching inclusions of ray class fields of orders with inclusions of SIC fields $F^{\mathrm{vec}}(S(35*))$ where $* \in \{a, b, c, d, e, f, g, h, i, j\}$. We have $\Delta = 36 \cdot 32 = 2^7 \cdot 3^2$, so $\Delta_0 = 2$ and $f = 12$. The set of divisors f' of 12 are $\{1, 2, 3, 4, 6, 12\}$. The SIC fields for the multiplets for $d = 35$ are extracted from [6, Tab. 9]. The illustrated choice of $\mathcal{M}$ satisfies Conjecture 1.2(2), which determines $\mathcal{M}$ uniquely. This choice also satisfies Conjecture 1.2(1); see Example 5.10.

Inclusions of SIC fields on the right side of Figure 6.1 for $d = 35$ were given in [6, Fig. 1]. Our figure for $d = 35$ here incorporates a later correction [2, unpublished]: the ratio SIC field for $35e$ is contained in the ratio SIC field for $35af$.

6.4. **Verification of cases of the Order-to-Multiplet Conjecture.** We consider whether the bijection $\mathcal{M}$ in Conjecture 1.2 can be determined from numerical data. We have performed a test of the conjecture on numerical invariants: We did not check inclusions $F^{\mathrm{proj}}(S_1) \subseteq F^{\mathrm{proj}}(S_2)$ directly, but we did check divisibility of the degrees of the fields $\left[F^{\mathrm{proj}}(S_1) : \mathbb{Q}\right] \,\Big|\, \left[F^{\mathrm{proj}}(S_2) : \mathbb{Q}\right]$.

However, there would be unresolvable ambiguity in any case where there are two distinct multiplets $[[S_1]]$ and $[[S_2]]$ having

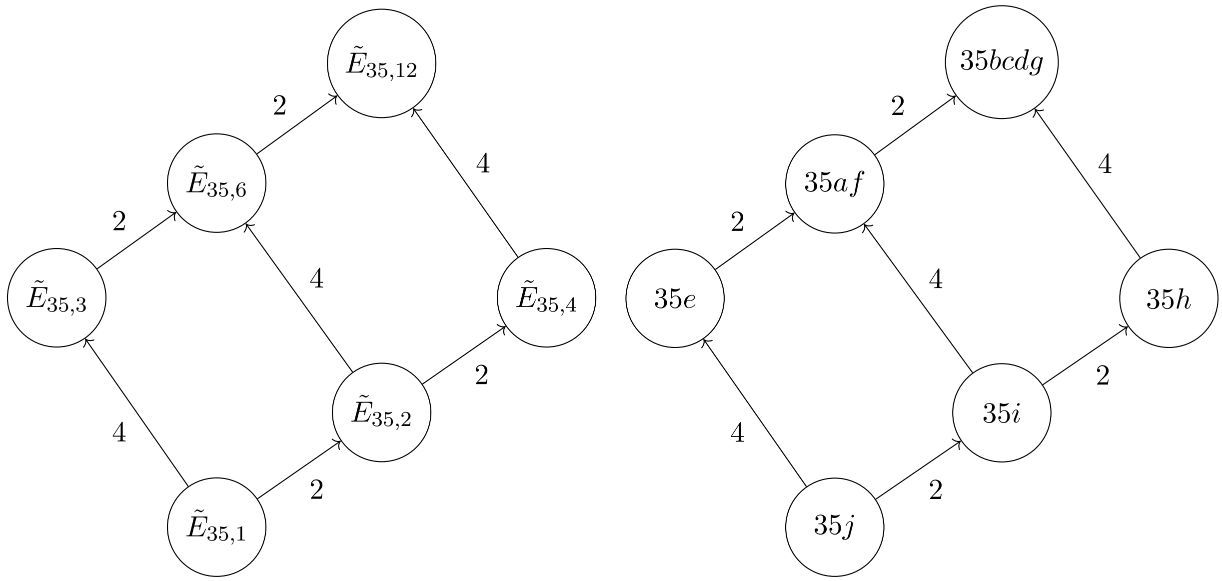

FIGURE 6.1. Left side: For $d = 35$, field inclusions of ray class fields $\tilde{E}_{35,f'}$ $\left(\text{mod } 35\mathcal{O}_{(f')^2\Delta_0}\right)$ of over-orders of $\mathcal{O}_{1152}$, with edge labels giving relative field degrees. $\tilde{E}_{35,1}$ has degree 72 over $\mathbb{Q}(\sqrt{\Delta_0})$, where $\Delta_0 = 8$. Right side: For $d = 35$, SIC multiplets with letter labels ($35a$ to $35j$) specifying PEC(35)-orbits, and edge labels giving relative degrees of associated fields $F^{\text{vec}}(S_{35*})$ for $* \in \{a, b, c, d, e, f, g, h, i, j\}$. $F^{\text{vec}}(S_{35j})$ has degree 72 over $\mathbb{Q}(\sqrt{\Delta_0})$.

(1) identical sizes $|[[S_1]]| = |[[S_2]]|$, and
(2) identical projection fields $F^{\text{proj}}(S_1) = F^{\text{proj}}(S_2)$.

Such an ambiguity can occur. It was discovered experimentally by Markus Grassl [26, unpublished] that two distinct multiplets $[[S_1]] \neq [[S_2]]$ can have the same associated projection SIC field $F^{\text{proj}}(S_1) = F^{\text{proj}}(S_2)$ The identified ambiguous multiplets occurred in dimensions $d \in \{47, 67, 259\}$, where in each case, there is a secondary multiplet having the same projection SIC field as the minimal multiplet (conjecturally corresponding to $\mathcal{O}' = \mathcal{O}_K$ or $f' = 1$). Algebraic SICs have currently not been computed in every dimension up to $d = 259$, but rather, Grassl has computed them is certain dimensions (including $d = 259$) where the projection field has small enough expected degree to permit the calculation.

In Section 8, we report theoretical results (proved elsewhere) classifying when inclusions of the ray class fields $\tilde{E}_{d,f'}$ for fixed d can be equalities; see Table 8.1. The truth of Conjecture 1.3 implies that the map $\mathcal{M}$ is determined uniquely whenever $\text{rad}(\Delta) \not\equiv 1 \pmod 8$, where $\text{rad}(r)$ for a positive integer r denotes the squarefree part of r; see Theorem 8.1. We show the set of such d has natural density $\frac{47}{48}$; see Proposition 8.3. By explicit computation, we determine in Section 8.1 that inclusions of ray class fields of orders that Conjecture 1.3 predicts to equal $F^{\text{proj}}(S)$ for $4 \leq d \leq 500$, do degenerate to the identity map in each of the dimensions $d \in \{47, 67, 259\}$ observed by Grassl, and additionally in dimensions $d \in \{83, 275, 211, 303, 339, 431, 447, 467\}$. (It remains to numerically test these predictions when exact SICs are found in these dimensions.)

d	$\mathcal{O}'$	f'	$h_{\mathcal{O}'}$	$[\tilde{E}_{d,f'} : K]$	multiplet	$[F^{\text{proj}}(S) : K]$
4	$\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$	1	1	8	$4a$	8
5	$\mathbb{Z}[\sqrt{3}]$	1	1	16	$5a$	16
6	$\mathbb{Z}[\frac{1+\sqrt{21}}{2}]$	1	1	24	$6a$	24
7	$\mathbb{Z}[\sqrt{2}]$	1	1	12	$7b$	12
	$\mathbb{Z}[2\sqrt{2}]$	2	1	24	$7a$	24
8	$\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$	1	1	16	$8b$	16
	$\mathbb{Z}[\frac{1+3\sqrt{5}}{2}]$	3	1	64	$8a$	64
9	$\mathbb{Z}[\sqrt{15}]$	1	2	72	$9ab$	72
10	$\mathbb{Z}[\frac{1+\sqrt{77}}{2}]$	1	1	96	$10a$	96
11	$\mathbb{Z}[\sqrt{6}]$	1	1	80	$11c$	80
	$\mathbb{Z}[2\sqrt{6}]$	2	2	160	$11ab$	160
12	$\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$	1	1	32	$12b$	32
	$\mathbb{Z}[\frac{1+3\sqrt{13}}{2}]$	3	1	96	$12a$	96
13	$\mathbb{Z}[\sqrt{35}]$	1	2	192	$13ab$	192
14	$\mathbb{Z}[\frac{1+\sqrt{165}}{2}]$	1	2	288	$14ab$	288
15	$\mathbb{Z}[\sqrt{3}]$	1	1	48	$15d$	48
	$\mathbb{Z}[2\sqrt{3}]$	2	1	96	$15b$	96
	$\mathbb{Z}[4\sqrt{3}]$	4	2	192	$15ac$	192
35	$\mathbb{Z}[\sqrt{2}]$	1	1	72	$35j$	72
	$\mathbb{Z}[2\sqrt{2}]$	2	1	144	$35i$	144
	$\mathbb{Z}[3\sqrt{2}]$	3	1	288	$35c$	288
	$\mathbb{Z}[4\sqrt{2}]$	4	1	288	$35h$	288
	$\mathbb{Z}[6\sqrt{2}]$	6	2	576	$35af$	576
	$\mathbb{Z}[12\sqrt{2}]$	12	4	1152	$35bcdg$	1152

TABLE 6.1. Table of d, orders $\mathcal{O}' = \mathcal{O}_{(f')^2\Delta_0}$ with $\Delta = (d+1)(d-3) = f^2\Delta_0$, class numbers $h_{\mathcal{O}'}$, degrees of fields $\tilde{E}_{d,f'}$, and index of fields $[F^{\text{proj}}(S) : K]$, $K = \mathbb{Q}(\sqrt{\Delta})$.

7. Theorems on sizes of class monoids of real quadratic fields

In this section, we state rigorous results about the behavior of $|\text{Clm}(\mathcal{O})|$ for orders with discriminants $\Delta_d = (d+1)(d-3)$. These results have conditional consequences for SICs via Conjecture 5.4.

Going beyond Zauner's conjecture, one would like to know not only that SICs exist in every dimension d, but also how many there are. The connection between SICs and class numbers gives us a precise prediction for the number of SICs up to equivalence (excluding any SICs that are not Weyl–Heisenberg covariant). In this section, we use known results on the growth of class numbers to derive conditional results on the number of SICs as $d \to \infty$.

The first growth result characterizes those dimensions in which our conjectures predict a unique Weyl–Heisenberg SIC, using a theorem of Byeon, Kim, and Lee [11].

Proposition 7.1. *One has* $|\text{Clm}(\mathcal{O}_{\Delta_d})| > 1$ *for all* $d > 22$. *The values of* $d \neq 3$ *with* $|\text{Clm}(\mathcal{O}_{\Delta_d})| = 1$ *are* $d \in \{1, 2, 4, 5, 6, 10, 22\}$.

Proof. Set $\Delta = \Delta_d = (d+1)(d-3)$ and $s(d) := |\mathrm{Clm}(\mathcal{O}_\Delta)|$; we are trying to determine when $s(d) = 1$. By Theorem 5.3,

$$s(d) = \sum_{f' | f} h_{(f')^2 \Delta_0}.$$

where $\Delta = f^2 \Delta_0$ and Δ_0 is fundamental. If $f > 1$, then $s(d) > 1$.

If $f = 1$, then $\Delta = \Delta_0$ is fundamental. Write $\Delta = (d-1)^2 - 4 = n^2 - 4$, where $n := d - 1$. Byeon, Kim, and Lee solved the class number 1 problem for real quadratic fields with fundamental discriminant of the form $n^2 - 4$, a result previously known as Mollin's conjecture [11, Thm 1.2]; whenever $n > 21$ (so $d > 22$), $s(d) = h_\Delta > 1$. The list of dimensions where $s(d) = 1$ follows from a finite calculation of class numbers. □

Corollary 7.2. *Assuming Conjecture 5.4, there is more than one* $\mathrm{PEC}(d)$*-class of Weyl–Heisenberg SIC in dimension d for all $d > 22$. The dimensions d with a unique* $\mathrm{PEC}(d)$*-class of Weyl–Heisenberg SIC are $d \in \{1, 2, 4, 5, 6, 10, 22\}$.*

Proof. The corollary follows from Proposition 7.1 combined with Conjecture 5.4. □

The second growth result is an asymptotic formula for the size of the ray class monoid of $\mathcal{O}_{\Delta_d}$. The proof uses the Brauer–Siegel theorem, which is an (ineffective) estimate of the growth of the product of the class number and the regulator for maximal orders. The presented result for orders must account for the class numbers of non-maximal orders. The conductor $f = f_{\Delta_d}$ is an extra degree of freedom not present in the Brauer–Siegel theorem.

Theorem 7.3. *As $d \to \infty$, and $\Delta_d = (d+1)(d-3)$, the size of the class monoid of $\mathcal{O}_{\Delta_d}$ obeys the asymptotic formula*

$$\log |\mathrm{Clm}(\mathcal{O}_{\Delta_d})| = \log d + o(\log d).$$

Proof. This is proved in [36], using results from [35]. □

Corollary 7.4. *Assume Conjecture 5.4. Then, as $d \to \infty$,*

$$\log |\mathrm{WHSIC}(d) / \mathrm{PEC}(d)| = \log d + o(\log d).$$

Proof. The corollary follows from Theorem 7.3 combined with the conjecture. □

8. Theorems on strictness or nonstrictness of inclusions of ray class fields of orders

In [36] we prove unconditional results determining exactly when the fields $\tilde{E}_{d,f'}$ introduced in Definition 6.3 can coincide, while fixing d and varying f'.

Theorem 8.1. *The set of $d \geq 4$ such that, for $\Delta = (d+1)(d-3)$ and $\varepsilon_d = \frac{d-1+\sqrt{\Delta}}{2}$, there exist distinct orders $\mathcal{O} \neq \mathcal{O}'$ with*

$$\mathbb{Z}[\varepsilon_d] \subseteq \mathcal{O} \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{\Delta})}, \qquad \mathbb{Z}[\varepsilon_d] \subseteq \mathcal{O}' \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{\Delta})},$$

having $H^{\mathcal{O}}_{d\mathcal{O},\Sigma} = H^{\mathcal{O}'}_{d\mathcal{O}',\Sigma}$ for some Σ (equivalently, all Σ) is exactly the set of all d such that the squarefree part of Δ (called the radical $\mathrm{rad}(d)$*) has* $\mathrm{rad}(\Delta) \equiv 1 \pmod 8$.

The following theorem classifies all pairs where coincidence may occur.

Theorem 8.2. *Let $d \geq 4$. Write $\Delta = (d+1)(d-3) = f^2 \Delta_0$ for Δ_0 a fundamental discriminant, and suppose f', f'' are positive integers satisfying $f' \mid f$, $f'' \mid f$ and $f'' < f'$. The following are equivalent:*

(1) $\tilde{E}_{d,f'} = \tilde{E}_{d,f''}$
(2) $E_{d,f'} = E_{d,f''}$
(3) $\mathrm{rad}(\Delta) \equiv 1 \pmod 8$, *$f' = 2f''$, and f'' is odd.*

(4) $\Delta_0 \equiv 1 \pmod 8$, *$f' = 2f''$, and f'' is odd.*

We also show that the condition $\mathrm{rad}(\Delta) \equiv 1 \pmod 8$ of Theorem 8.1 is satisfied for a set of d having natural density $\frac{1}{48}$.

Proposition 8.3. *We have*

$$\lim_{X\to\infty} \frac{|\{d \in \mathbb{Z} \cap [1, X] : \mathrm{rad}((d+1)(d-3)) \equiv 1 \pmod 8\}|}{X} = \frac{1}{48}.$$

Proof. This is [36, Prop. 9.6]. □

8.1. **Numerical data on degeneration for ray class fields of orders.** We present data on the implications of Theorem 8.2 for $4 \le d \le 500$. In Table 8.1, we use the conditions of Theorem 8.2 to write down all cases of equality of ray class fields of relevant orders $\tilde{E}_{d,f''} = \tilde{E}_{d,f'}$ with $(f'', f') = (f'', 2f'')$. For $d \le 500$, equality of ray class fields $\tilde{E}_{d,f''} = \tilde{E}_{d,f'}$ occurs for

$$d \in \{47, 67, 83, 175, 211, 259, 303, 339, 431, 447, 467\}.$$

For every such d, the conductor pair $(1, 2)$ degenerates (i.e., gives the same field ray class field in the manner of Theorem 8.2), and an additional conductor pair degenerates in three of these dimensions. This data is consistent with, and accounts for, Grassl's data for collapse of SIC field inclusions in dimensions $\{47, 67, 259\}$.

d	$\sqrt{\Delta_0}$	f'', f'	h	$[\tilde{E}_{d,f''} : \mathbb{Q}(\sqrt{\Delta_0})]$	d	$\sqrt{\Delta_0}$	f'', f'	h	$[\tilde{E}_{d,f''} : \mathbb{Q}(\sqrt{\Delta_0})]$
47	33	$1, 2$	1	1472	303	57	$5, 10$	6	244800
67	17	$1, 2$	1	1452	339	1785	$1, 2$	8	408576
83	105	$1, 2$	2	9184	431	321	$1, 2$	3	371520
175	473	$1, 2$	3	43200	431	321	$3, 6$	9	1114560
211	689	$1, 2$	4	117600	447	777	$1, 2$	4	355200
259	65	$1, 2$	2	31104	467	377	$1, 2$	2	290784
303	57	$1, 2$	1	40800	467	377	$3, 6$	8	1163136

TABLE 8.1. Dimensions $d \le 500$ with an equality of ray class fields of orders $\tilde{E}_{d,f''} = \tilde{E}_{d,f'}$. The columns show the fund. disc. Δ_0, each pair of conductors $(f'', f') = (f'', 2f'')$ exhibiting field equality, the order class number $h = h_{(f'')^2\Delta_0} = h_{(f')^2\Delta_0}$, and ray class field extension degree $[\tilde{E}_{d,f''} : \mathbb{Q}(\sqrt{\Delta_0})] = [\tilde{E}_{d,f'} : \mathbb{Q}(\sqrt{\Delta_0})]$.

9. Concluding remarks

We state a conjectures refining Conjecture 1.2 and Conjecture 1.3. We also discuss other number fields attached to SICs that have been studied in the literature.

9.1. **The Ideal-Class-to-SICs Conjecture.** We formulate a final conjecture that refines Conjecture 1.2 and Conjecture 1.3 by insisting on compatibility with the Artin map. We formulate Conjecture 9.1 because its truth would provide a unifying principle explaining the structure of all the other conjectures. In this paper, we present no mechanism to construct a candidate map Ω made in its statement.

To state this conjecture, we decompose

$$\mathrm{Clm}(\mathcal{O}_\Delta) = \bigsqcup_{f'|f} \mathrm{Cl}(\mathcal{O}_{(f')^2\Delta_0})$$

by means of Theorem 5.3.

Conjecture 9.1 (Ideal-Class-to-SIC Conjecture)**.** *Fix a positive integer $d > 3$, let $\Delta = (d+1)(d-3)$, and write $\Delta = f^2\Delta_0$ where Δ_0 is a fundamental discriminant of a quadratic field. Then there is a bijection Ω,*

$$\Omega : \bigsqcup_{f'|f} \mathrm{Cl}(\mathcal{O}_{(f')^2\Delta_0}) \xrightarrow{\Omega} \mathrm{WHSIC}(d)/\,\mathrm{PEC}(d),$$

under which an ideal class $\mathcal{A} \in \mathrm{Cl}(\mathcal{O}')$ with $\mathcal{O}' = \mathcal{O}_{(f')^2\Delta_0}$ maps to a geometric equivalence class $\Omega(\mathcal{A}) = [S_{\mathcal{A}}]$ with associated fields $F^{\mathrm{trip}}(S_{\mathcal{A}}) = E_{d,f'}$ and $F^{\mathrm{proj}}(S_{\mathcal{A}}) = \tilde{E}_{d,f'}$.

Furthermore, Ω can be chosen to be compatible with the Artin map (defined in Theorem 6.2)

$$\mathrm{Art}_{\mathcal{O}'} : \mathrm{Cl}_{d'\mathcal{O}',\{\infty_1,\infty_2\}}(\mathcal{O}') \to \mathrm{Gal}(\tilde{E}_{d,f'}/\mathbb{Q}(\Delta_0)),$$

in the sense that

$$[S_{\bar{\mathcal{A}}\bar{\mathfrak{B}}}] = [(\mathrm{Art}_{\mathcal{O}'}(\mathcal{A}))(S_{\bar{\mathfrak{B}}})] \text{ for any } \mathcal{A}, \mathfrak{B} \in \mathrm{Cl}_{d'\mathcal{O}',\{\infty_1,\infty_2\}}(\mathcal{O}')$$

and their images $\bar{\mathcal{A}}, \bar{\mathfrak{B}} \in \mathrm{Cl}(\mathcal{O}')$ under the natural quotient map.

The required compatibility of Ω with the Artin map implies that there is exactly one Galois multiplet for each order $\mathcal{O}$ between $\mathcal{O}_{\Delta_0}$ and $\mathcal{O}_{\Delta}$.

Conjecture 9.1 would define a map $\mathcal{M}$ of the type given in Conjecture 1.2 by means of the following commutative diagram,

$$\begin{array}{ccc} \bigsqcup_{f'|f} \mathrm{Cl}(\mathcal{O}_{(f')^2\Delta_0}) & \xrightarrow{\Omega} & \mathrm{WHSIC}(d)/\,\mathrm{PEC}(d) \\ \downarrow & & \downarrow \\ \{\text{positive divisors of } f\} & \overset{\mathcal{M}}{\dashrightarrow} & \{[[S]] : S \text{ a line-SIC in } \mathbb{C}^d\} \end{array}$$

where the downward maps send $\mathcal{A} \in \mathrm{Cl}(\mathcal{O}_{(f')^2\Delta_0})$ to f' and $[S]$ to $[[S]]$, respectively.

Conjecture 9.1 is compatible with conjectures of the first author [33] and other authors [5, 10] connecting SICs to the Stark conjectures for real quadratic fields [42, 43], which posit the existence of special algebraic units constructed from partial zeta functions and carrying a Galois action compatible with the Artin map. Work in preparation by Appleby, Flammia, and Kopp [7] will make the classification scheme suggested by Conjecture 9.1 explicit. The explicit classification also yields exact formulas for the stabilizers $\mathrm{stab}(S)$ and thus the size of the set $\mathrm{WHSIC}(d)$ discussed in Remark 5.6.

9.2. **Refined SIC fields.** This paper considered fields that are geometric invariants of a SIC. It can be useful in practice to define SICs using data in smaller subfields that are not geometric invariants. One such subfield is the field generated by the entries of a single fiducial projector Π. That field can be smaller than the full projector field by nearly a factor of d is some special cases, and this is extremely useful for computing exact SICs in some large dimensions that would otherwise be inaccessible to numerical investigation [5, 10]. Another is the field generated by the *SIC overlaps* $\mathrm{Tr}(\Pi D_p)$ (or else the closely related *SIC overlap phases* $\sqrt{d+1}\,\mathrm{Tr}(\Pi D_p)$), where D_p are the *displacement operators*.

The overlap field (and the overlap phase field) both appear to be ray class fields specified by ramification at just one of the infinite places ∞_1, provided one chooses a "strongly centered" fiducial projector; see [8, 20]. That phenomenon relates to the connection to Stark units, which live in a ray class field with ramification at the other infinite place ∞_2 and are (at least in some cases) Galois conjugate to squares of overlap phases.

10. Acknowledgements

Work of the first author was supported by NSF DMS grant #2302514. Work of the second author was supported by NSF DMS grant #1701576.

We are grateful to the developers of Magma and in particular David Kohel, whose software package `reduced_forms` (and whose package `class_number`, on which `reduced_forms` relies) we used to compute class numbers of real quadratic orders.

We thank Markus Grassl for finding numerical examples of degeneration of SIC fields and sharing those examples with us. We thank Marcus Appleby, Steven Flammia, and Gary McConnell for valuable conversations. We also acknowledge the contributions of Steve Donnelly, who independently connected SICs to orders in real quadratic number fields and shared his insights with Marcus Appleby, Steven Flammia, and Markus Grassl through informal discussions.

Appendix A. Conjectures for triple product fields

We formulate conjectures about the triple product fields $F^{\text{trip}}(S)$. Recall that $F^{\text{trip}}(S) \subseteq F^{\text{proj}}(S)$. We have limited empirical evidence for these conjectures.

Recall that $E_{d,f'} = H^{\mathcal{O}'}_{d\mathcal{O}',\{\infty_1,\infty_2\}}$. Note that $E_{d,f'} = \tilde{E}_{d,f'}$ if d is odd, and $E_{d,f'} \subseteq \tilde{E}_{d,f'}$ if d is even.

Conjecture A.1 (Extended Ray Class Fields of Orders Conjecture)**.** *Fix an integer $d \geq 4$ and write $\Delta = (d+1)(d-3) = f^2\Delta_0$ where $\Delta_0 = \operatorname{disc}(\mathbb{Q}(\sqrt{\Delta}))$. Then the bijection $\mathcal{M}$ of Conjecture 1.3 can be chosen to satisfy the properties: If S is a Weyl–Heisenberg SIC with $[S] \in \mathcal{M}(f')$, then*

$$F^{\text{trip}}(S) = E_{d,f'} \qquad \text{and} \qquad F^{\text{vec}}(S) = F^{\text{proj}}(S) = \tilde{E}_{d,f'}.$$

Conjecture A.1 implies part 1 of the following conjecture, which can be tested against data.

Conjecture A.2. *Let $d \geq 4$. Then for a Weyl–Heisenberg SIC S,*

(1) *The index*

$$[F^{\text{proj}}(S) : F^{\text{trip}}(S)] = \begin{cases} 1 & \text{if } d \text{ is odd,} \\ 2 & \text{if } d \text{ is even.} \end{cases}$$

(2) $F^{\text{proj}}(S) = F^{\text{trip}}(S)\,(\xi_d)$.

We have numerically verified part (1) of this conjecture, the index computation, for $4 \leq d \leq 10$. Recall that Proposition 3.6(2) showed unconditionally that $[F^{\text{proj}}(S) : F^{\text{trip}}(S)]$ divides d^2.

Appendix B. Proof of Theorem 6.5

For completeness, this appendix presents results that are to appear elsewhere [36], reformulated using the variable $n = d + 1$.

Let $K = \mathbb{Q}(\sqrt{\Delta})$. Write $\Delta = f^2 D$, $f \geq 1$, where D is squarefree, so $K = \mathbb{Q}(\sqrt{D})$ and

$$\mathcal{O}_K = \left\{ \frac{1}{2}(a + b\sqrt{D}) : (a,b) \in \mathbb{Z}^2,\ a \equiv b \pmod{2},\ a \equiv 0 \pmod{2} \text{ if } D \not\equiv 1 \pmod{4} \right\}.$$

For the datum $(\mathfrak{m}, \Sigma)$ consisting of an ideal $\mathfrak{m}$ of the order $\mathcal{O}$ in K and a set of real places Σ of K, recall the definition of the unit subgroup

$$\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O}) := \left\{ \alpha \in \mathcal{O}^\times : \alpha \equiv 1 \pmod{\mathfrak{m}},\ \sigma(\alpha) > 0 \text{ for } \sigma \in \Sigma \right\}.$$

Theorem 6.5 depends on the following lemma concerning unit groups of orders, which is special to the family $\Delta = (d+1)(d-3)$ of real quadratic orders, with $d \geq 4$.

Lemma B.1. *Let $d \geq 4$, $\Delta = (d+1)(d-3)$, and $\varepsilon_d = \frac{d-1+\sqrt{\Delta}}{2}$. Let Σ be a subset of the real embedding of $\mathbb{Q}(\sqrt{\Delta})$. Fix an order $\mathcal{O}$ satisfying*

$$\mathcal{O}_\Delta := \mathbb{Z}[\varepsilon_d] \subseteq \mathcal{O} \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{\Delta})}.$$

Then,

$$\mathrm{U}_{d\mathcal{O},\Sigma}(\mathcal{O}) = \langle \varepsilon_d^3 \rangle. \tag{B.1}$$

For Lemma B.1, the unit group of interest is $\mathrm{U}_{d\mathcal{O},\Sigma}(\mathcal{O})$. The unit ε_d is totally positive, and

$$\varepsilon_d^3 = \frac{1}{2}\left((d-1)(d^2-2d-2) + d(d-2)f\sqrt{D}\right) \equiv 1 \pmod{d\mathcal{O}_\Delta}.$$

Thus, we have the containment relations

$$\langle \varepsilon_d^3 \rangle \subseteq \mathrm{U}_{d\mathcal{O}_\Delta,\{\infty_1,\infty_2\}} \subseteq \mathrm{U}_{d\mathcal{O},\Sigma}(\mathcal{O}) \subseteq \mathrm{U}_{d\mathcal{O}_K}(\mathcal{O}_K).$$

These relations show it suffices to prove (B.1) for the special case $\mathcal{O} = \mathcal{O}_K$ with $\Sigma = \emptyset$.

The following stronger assertion in the special case, about the minimal unit $\eta \in \mathcal{O}_K$ such that $\eta > 1$ and $\eta = \pm 1 \pmod{d\mathcal{O}_K}$, immediately implies Lemma B.1.

Lemma B.2. *Let $d \geq 4$, $\Delta = (d+1)(d-3)$ and $\varepsilon_d = \frac{1}{2}(d-1+\sqrt{\Delta})$. Let $K = \mathbb{Q}(\sqrt{\Delta})$. Then the smallest unit $\eta > 1$ in $\mathcal{O}_K$ having*

$$\eta = \pm 1 \pmod{d\mathcal{O}_K}.$$

is $\eta = \varepsilon_d^3$.

Proof. Let Δ_0 be the discriminant of the maximal order $\mathcal{O}_K$. Note that $\varepsilon_d > 1$ is a unit of $\mathcal{O}_K$ of positive norm and is a root of $x^2 - (d-1)x + 1 = 0$. If $\varepsilon_d' > 0$ is its Galois conjugate, then $\varepsilon_d' = \frac{1}{\varepsilon_d}$ and $\mathrm{Tr}(\varepsilon_d) = \varepsilon_d + \varepsilon_d' = d-1$, and $\varepsilon_d < d-1$.

Write $\eta = \frac{1}{2}(a + b\sqrt{\Delta_0})$, and denote its Galois conjugate $\eta' = \frac{1}{2}(a - b\sqrt{\Delta_0})$, with $a \equiv b \pmod 2$. A priori η might have negative norm, but we show:

Claim 1. *We have $\mathrm{Nm}(\eta) = \eta\eta' = 1$. Then $\eta' = \frac{1}{\eta}$ and $0 < \eta' < 1$.*

Proof. By hypothesis, $\eta = \pm 1 + d\omega$ for some $\omega \in \mathcal{O}_K$, and taking Galois conjugates yields $\eta' = \pm 1 + d\omega'$. It follows that $\eta\eta' = 1 \pmod{d\mathcal{O}_K}$. Now $\mathrm{Nm}(\eta) = \eta\eta' = \pm 1$ and $1 \not\equiv -1 \pmod{d\mathcal{O}_K}$ since $d \geq 4$, so we conclude $\eta\eta' = 1$. Thus $\eta' > 0$ and $0 < \eta' < 1$, proving the claim.

Claim 2. *For some integer $k \geq 1$, $\eta^k = \varepsilon_d^3$.*

Proof. We have $1 < \eta \leq \varepsilon_d^3$, hence there holds $\eta^{k-1} < \varepsilon_d^3 \leq \eta^k$, for some $k \geq 1$. Then $\omega := \eta^k \varepsilon_d^{-3}$ is a unit, $1 \leq \omega < \eta$, and $\omega \equiv \pm 1 \pmod{d\mathcal{O}_K}$. However, by minimality of $\eta > 1$, we must have $\omega = 1$, proving the claim.

Claim 3. *$\eta^k = \varepsilon_d^3$ for some $k \geq 3$ cannot occur.*

Proof. If $k = 3$, then we have $\eta^3 = \varepsilon_d^3$, and, since $\eta > 1$, we have $\eta = \varepsilon_d$. By hypothesis $\eta \equiv \pm 1 \pmod{d\mathcal{O}_K}$, so we deduce $\varepsilon_d \equiv \pm 1 \pmod{d\mathcal{O}_K}$. We rule out this possibility, arguing by contradiction. So suppose $\varepsilon_d \equiv \pm 1 \pmod{d\mathcal{O}_K}$. We know $\varepsilon_d\varepsilon_d' = \eta\eta' = 1$, which viewed $\pmod{d\mathcal{O}_K}$ implies $\varepsilon_d' \equiv \varepsilon_d \equiv \pm 1 \pmod{d\mathcal{O}_K}$. We conclude that $\varepsilon_d + \varepsilon_d' \equiv \pm 2 \pmod{d\mathcal{O}_K}$. On the other hand

$$\varepsilon_d + \varepsilon_d' = \frac{1}{2}(d-1+\sqrt{\Delta}) + \frac{1}{2}(d-1+\sqrt{\Delta}) = d-1 \equiv -1 \pmod{d\mathcal{O}_K}.$$

Since $\pm 2 \not\equiv -1 \pmod{d\mathcal{O}_K}$ for any $d \geq 4$, we have a contradiction, whence it always holds that $\varepsilon_d \not\equiv \pm 1 \pmod{d\mathcal{O}_K}$.

If $k \geq 4$, then $\eta = (\varepsilon_d)^{3/k} < \varepsilon_d$ (taking the positive k-th root.) We study the trace $\mathrm{Tr}(\eta) = \eta + \eta'$ and note, by Claim 1, $\mathrm{Tr}(\eta) = \eta + \frac{1}{\eta}$.

Now, since $x + \frac{1}{x}$ is an increasing function for $x \geq 1$, and $1 < \eta < e_d$, we have

$$1 < \eta + \eta' = \mathrm{Tr}(\eta) < \varepsilon_d + \varepsilon_d' = \mathrm{Tr}(\varepsilon_d) = d - 1. \tag{B.2}$$

Now $\mathrm{Tr}(\eta) \in \mathbb{Z}$, and

$$\mathrm{Tr}(\eta) \equiv \eta + \eta' \pmod{d\mathcal{O}_K} \equiv \pm 2 \pmod{d\mathcal{O}_K}.$$

Since $d \geq 4$, the bounds (B.2) on $\mathrm{Tr}(\eta)$ give

$$\mathrm{Tr}(\eta) = \begin{cases} 2 & \text{if } \eta \equiv 1 \pmod{d\mathcal{O}_K}, \\ d-2 & \text{if } \eta \equiv -1 \pmod{d\mathcal{O}_K}. \end{cases}$$

We have two cases.

- *Case 1:* Suppose $\mathrm{Tr}(\eta) = 2$. Then $\eta + \eta' = 2$ and $\eta\eta' = 1$, so η is a root of the polynomial $x^2 - 2x + 1 = (x-1)^2$, so $\eta = 1$, contradicting $\eta > 1$.
- *Case 2:* Suppose $\mathrm{Tr}(\eta) = d - 2$. In this case η satisfies $x^2 - (d-2)x + 1 = 0$, hence $\eta = d - 2 - \eta' > d - 3$. For $d \geq 7$, noting that $(d-1)^3 < (d-3)^4$ holds, and recalling $\varepsilon_d < d - 1$, we have

  $$(d-3)^3 < \eta^3 < \varepsilon_d^3 < (d-1)^3 < (d-3)^4 < \eta^4 \leq \eta^k,$$

  so there are no solutions $\eta^k = \varepsilon_d^3$ for $k \geq 4$ in this case.

  For the remaining values $d = 4, 5, 6$, case $d = 4$ is already ruled out in Case 1; $d = 5$ has $\eta = \frac{3+\sqrt{5}}{2}$, while $\varepsilon_5 = 2 + \sqrt{3}$; $d = 6$ has $\eta = 2 + \sqrt{3}$ while $\varepsilon_6 = \frac{5+\sqrt{21}}{2}$, so $\eta^k = \varepsilon_d^3$ has no solution since η and ε_d are in different number fields.

This completes the proof of Claim 3.

It remains to rule out $k = 2$, where ε_d^3 is the square of a unit $\tilde{\eta}$. We first classify all d where such a unit exists.

Claim 4. *The set of all $d \geq 4$ having a unit $\tilde{\eta} \in \mathcal{O}_K$ that satisfies $\tilde{\eta}^2 = \varepsilon_d^3$ is:*

(1) *$d = a^2 - 1$ for any $a \geq 3$. Then, $\tilde{\eta} = \pm\eta\varepsilon_d$, where*

$$\eta = \varepsilon_{a+1} = \frac{a + \sqrt{a^2-4}}{2}$$

has $\mathrm{Nm}(\eta) = +1$. Here $\sqrt{\Delta} = a\sqrt{d-3} = a\sqrt{a^2-4}$.

(2) *$d = a^2 + 3$ for any $a \geq 1$. Then, $\tilde{\eta} = \pm\eta\varepsilon_d$, where $\eta = \frac{a+\sqrt{a^2+4}}{2}$ has $\mathrm{Nm}(\eta) = -1$. Here $\sqrt{\Delta} = a\sqrt{d+1} = a\sqrt{a^2+4}$.*

Proof. To prove the claim, we study existence of the unit $\eta = \tilde{\eta}\varepsilon_d^{-1}$. We suppose $\eta = \frac{1}{2}(a + b\sqrt{\Delta_0})$ and $\eta' = \frac{1}{2}(a - b\sqrt{\Delta_0})$, where $a \equiv b \pmod 2$ and both a and b are even unless $\Delta_0 \equiv 1 \pmod 4$. Now

$$\eta^2 = \frac{1}{4}\left((a^2 + b^2\Delta_0) + 2ab\sqrt{\Delta_0}\right),$$

while $\varepsilon_d = \frac{1}{2}(d - 1 + f\sqrt{\Delta_0})$. To obtain a solution, we must have

$$ab = f;$$

$$a^2 + b^2\Delta_0 = 2(d-1).$$

We have $a \neq 0$ since $f \neq 0$, so the first equation gives $b^2 = \frac{f^2}{a^2}$, and the second equation can be rewritten (since $\Delta = \Delta_0 f^2$) as

$$a^2 + \frac{\Delta}{a^2} = 2(d-1).$$

Introducing the new variable $y = a^2$, we find

$$y^2 - 2(d-1)y + (d+1)(d-3) = (y-(d+1))(y-(d-3)) = 0,$$

which yields two cases. The first is $y = a^2 = d+1$, which gives solutions $d = a^2 - 1$ for $a \geq 3$, to make $d \geq 4$. The second is $y = a^2 - 3$, which gives solutions $d = a^2 + 3$ for $a \geq 1$.

- *Case 1:* Suppose $d = a^2 + 1$ (so $a \geq 3$). Then $\Delta = a^2(a^2-4)$, $\sqrt{\Delta} = a\sqrt{a^2-4}$, and $a^2 - 4 = \Delta_0 b^2$. Now

$$\eta = \varepsilon_{a+1} = \frac{1}{2}(a + \sqrt{a^2-4});$$
$$\varepsilon_d = \eta^2 = \frac{1}{2}(a^2 - 2 + a\sqrt{a^2-4}).$$

Here $\mathrm{Nm}(\eta) = +1$, and the unit $\tilde{\eta} = \eta\varepsilon_d > 1$ has $\mathrm{Nm}(\tilde{\eta}) = 1$.
- *Case 2:* Suppose $d = a^2 - 3$, $(a \geq 1)$. Then $\Delta = a^2(a^2+4)$ and $\sqrt{\Delta} = a\sqrt{a^2+4}$. So

$$\eta = \frac{1}{2}(a + \sqrt{a^2+4});$$
$$\varepsilon_d = \eta^2 = \frac{1}{2}(a^2 + 2 + a\sqrt{a^2+4}).$$

Here $\mathrm{Nm}(\eta) = -1$, and the unit $\tilde{\eta} = \eta\varepsilon_d > 1$ has $\mathrm{Nm}(\tilde{\eta}) = -1$.

This proves Claim 4.

To complete the proof, we rule out the final case $k = 2$.

Claim 5. *$\eta^k = \varepsilon_d^3$ for $k = 2$ does not occur.*

Proof. We must show that all the units $\tilde{\eta}$ described by Claim 4 have

$$\tilde{\eta} \not\equiv \pm 1 \ \left(\mathrm{mod}\,(a^2-1)\mathcal{O}_K\right).$$

The Claim 4 solutions for $d = a^2 + 1$ are ruled out by Claim 1, since $\mathrm{Nm}(\tilde{\eta}) = -1$. To rule out the Claim 4 solutions having $d = a^2 - 1$, note that these solutions $\tilde{\eta}$ with $\tilde{\eta}^2 = \varepsilon_d^3$ are given by $\tilde{\eta} = e_{a+1}e_{a^2-1} = e_{a+1}^3$ with $\varepsilon_{a+1} = \frac{1}{2}(a + \sqrt{a^2-4})$. We have

$$\tilde{\eta} = \frac{1}{2}\left(a(a^2-3) + (a^2-1)\sqrt{a^2-4}\right).$$

Now $\Delta = (d+1)(d-3) = a^2(a^2-4)$; hence, $\Delta = f^2\Delta_0$ has $\Delta_0 | (a^2-4)$ and $K = \mathbb{Q}(\sqrt{a^2-4})$. We assert for $d = a^2 - 1$ that

$$\tilde{\eta} \equiv -a \ \left(\mathrm{mod}\,(a^2-1)\mathcal{O}_K\right).$$

The assertion implies $a \pm 1 \notin d\mathcal{O}_K$ holds for $d = a^2 - 1$, with $d \geq 3$, which implies Claim 5. It is proved in two cases.

- *Case 1.* Suppose a is odd. Then, $\Delta = a^2(a^2-4) \equiv 1 \pmod 4$ and $K = \mathbb{Q}(\sqrt{a^2-4})$, so $(a^2-1)(\frac{1}{2}(1 + \sqrt{d^2-4})) \in d\mathcal{O}_K$. Hence,

$$\begin{aligned}
\tilde{\eta} &= \frac{1}{2}(a(a^2-3) + (a^2-1)\sqrt{a^2-4})) \\
&\equiv \frac{1}{2}a(a^2-3) - \frac{1}{2}(a^2-1) && \left(\mathrm{mod}\,(a^2-1)\mathcal{O}_K\right) \\
&\equiv \frac{a-1}{2}(a^2-1) - a && \left(\mathrm{mod}\,(a^2-1)\mathcal{O}_K\right) \\
&\equiv -a && \left(\mathrm{mod}\,(a^2-1)\mathcal{O}_K\right).
\end{aligned}$$

- *Case 2.* Suppose a is even. Let $a = 2a'$. Then, $\Delta = a^2\Delta_0$ with $\Delta_0 = a^2 - 4 = 4((a')^2 - 1)$, so $K = \mathbb{Q}(\sqrt{(a')^2 - 1})$. Now

$$\begin{aligned}\tilde{\eta} &= \frac{a}{2}(a^2-3) + (a^2-1)\sqrt{(a')^2-1} \\ &\equiv \frac{a}{2}(a^2-1) - a && \left(\operatorname{mod} (a^2-1)\mathcal{O}_K\right) \\ &\equiv -a && \left(\operatorname{mod} (a^2-1)\mathcal{O}_K\right).\end{aligned}$$

We have proved the assertion, hence Claim 5 is proved. Thus Lemma B.2 is proved. ☐

Now we prove Theorem 6.5.

Proof of Theorem 6.5. Let $\tilde{d} = d$ if d is odd and $\tilde{d} \in \{d, 2d\}$ if d is even. By [34, Thm. 5.6], the cardinality of the ray class group is

$$\left|\mathrm{Cl}_{\tilde{d}\mathcal{O}',\Sigma}(\mathcal{O}')\right| = \frac{h_K}{\left[\mathcal{O}_K^\times : \mathrm{U}_{\tilde{d}\mathcal{O}',\Sigma}(\mathcal{O}')\right]} \cdot \frac{2^{|\Sigma|}\left|\left(\mathcal{O}_K\Big/\left(\tilde{d}\mathcal{O}' : \mathcal{O}_K\right)\right)^\times\right|}{\left|\mathrm{U}_{\tilde{d}\mathcal{O}'}\left(\mathcal{O}'\Big/\left(\tilde{d}\mathcal{O}' : \mathcal{O}_K\right)\right)\right|}. \tag{B.3}$$

By Lemma B.1, $\mathrm{U}_{d\mathcal{O}',\Sigma}(\mathcal{O}') = \langle \varepsilon_d^3 \rangle$. On the other hand, when $\tilde{d} = 2d$,

$$e_d^3 = -d + 1 + (d^2 - 2d)\varepsilon_d \equiv -d + 1 \not\equiv 1 \pmod{2d},$$

but $\varepsilon_d^6 \equiv 1 \pmod{2d}$, so $\mathrm{U}_{\tilde{d}\mathcal{O}',\Sigma}(\mathcal{O}') = \langle \varepsilon_d^6 \rangle$. Moreover, $\mathcal{O}_K^\times = \langle -1, \varepsilon_K \rangle$ for some fundamental unit ε_K. Thus,

$$\left[\mathcal{O}_K^\times : \mathrm{U}_{\tilde{d}\mathcal{O}',\Sigma}(\mathcal{O}')\right] = \begin{cases} \left[\langle -1, \varepsilon_K\rangle : \langle \varepsilon_d^3\rangle\right] = \dfrac{2\log(\varepsilon_d^3)}{\log(\varepsilon_K)} = \dfrac{6\log(\varepsilon_d)}{\mathrm{Reg}_K}, & \text{if } \tilde{d} = d, \\ \left[\langle -1, \varepsilon_K\rangle : \langle \varepsilon_d^6\rangle\right] = \dfrac{2\log(\varepsilon_d^6)}{\log(\varepsilon_K)} = \dfrac{12\log(\varepsilon_d)}{\mathrm{Reg}_K}, & \text{if } \tilde{d} = 2d. \end{cases} \tag{B.4}$$

The quotient ideal appearing in (B.3) is $\left(\tilde{d}\mathcal{O}' : \mathcal{O}_K\right) = \tilde{d}\,(\mathcal{O}' : \mathcal{O}_K) = \tilde{d}f'\mathcal{O}_K$. Thus,

$$\left|\left(\mathcal{O}_K\Big/\left(\tilde{d}\mathcal{O}' : \mathcal{O}_K\right)\right)^\times\right| = \left|\left(\mathcal{O}_K\Big/\tilde{d}f'\mathcal{O}_K\right)^\times\right| = \varphi_K(\tilde{d}f'). \tag{B.5}$$

Now we must compute the size of $\mathrm{U}_{\tilde{d}\mathcal{O}'}\left(\mathcal{O}'\Big/\left(\tilde{d}\mathcal{O}' : \mathcal{O}_K\right)\right) = \mathrm{U}_{\tilde{d}\mathcal{O}'}\left(\mathcal{O}'\Big/\tilde{d}f'\mathcal{O}_K\right)$. Write $\mathcal{O}_K = \mathbb{Z} + \omega\mathbb{Z}$ and $\mathcal{O}' = \mathbb{Z} + f'\omega\mathbb{Z}$. Thus, $\mathcal{O}'/\tilde{d}f'\mathcal{O}_K = \frac{\mathbb{Z}+f'\omega\mathbb{Z}}{\tilde{d}f'\mathbb{Z}+\tilde{d}f'\omega\mathbb{Z}}$ and $\tilde{d}\mathcal{O}' = \tilde{d}\mathbb{Z} + \tilde{d}f'\omega\mathbb{Z}$, so the multiplicative group

$$\begin{aligned}\mathrm{U}_{\tilde{d}\mathcal{O}'}\left(\mathcal{O}'\Big/\left(\tilde{d}\mathcal{O}' : \mathcal{O}_K\right)\right) &= \left\{u \in \frac{\mathbb{Z}+f'\omega\mathbb{Z}}{\tilde{d}f'\mathbb{Z}+\tilde{d}f'\omega\mathbb{Z}} : u \equiv 1 \left(\operatorname{mod} \tilde{d}\mathbb{Z} + \tilde{d}f'\omega\mathbb{Z}\right)\right\} \\ &\cong \left\{u \in \mathbb{Z}/\tilde{d}f'\mathbb{Z} : u \equiv 1 \left(\operatorname{mod} \tilde{d}\right)\right\}.\end{aligned}$$

If $\gcd(\tilde{d}, f') = 1$, then this group is isomorphic to $(\mathbb{Z}/f'\mathbb{Z})^\times$ by the Chinese remainder theorem. Its order is then $\varphi(f')$. The only case in which $\gcd(\tilde{d}, f') \neq 1$ is when $d \equiv 3 \pmod 9$ and $3 \mid f'$, in which case $\gcd(\tilde{d}, f') = 3$ and $\tilde{d} = 3d_1$ with $\gcd(d_1, 3f') = 1$. The Chinese remainder theorem gives a ring isomorphism $\pi : \mathbb{Z}/\tilde{d}f'\mathbb{Z} \to \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/3f'\mathbb{Z}$ given by $\pi(u) = (\pi_1(u), \pi_2(u)) = (u \pmod{d_1}, u \pmod{3f'})$. Under this isomorphism, the condition $u \equiv 1 \left(\operatorname{mod} \tilde{d}\right)$ is equivalent to $\pi_1(u) = 1$ and $\pi_2(u) \equiv 1 \pmod 3$; the latter condition is satisfied on an index 2 subgroup of $(\mathbb{Z}/3f'\mathbb{Z})^\times$. Thus, the order of $\mathrm{U}_{\tilde{d}\mathcal{O}'}\left(\mathcal{O}' \big/ \left(\tilde{d}\mathcal{O}' : \mathcal{O}_K\right)\right)$ is $\varphi(3f')/2 = \frac{3}{2}\varphi(f')$. In summary,

$$\left|\mathrm{U}_{\tilde{d}\mathcal{O}'}\left(\mathcal{O}' \big/ \left(\tilde{d}\mathcal{O}' : \mathcal{O}_K\right)\right)\right| = \begin{cases} \frac{3}{2}\varphi(f'), & \text{if } d \equiv 3 \pmod 9 \text{ and } 3|f', \\ \varphi(f'), & \text{otherwise.} \end{cases} \tag{B.6}$$

In the case $\tilde{d} = d$, plugging in (B.4), (B.5), and (B.6) to (B.3) yields (6.4). In the case $\tilde{d} = 2d$ (with d even), we have $\varphi_K(\tilde{d}f') = 4\varphi_K(df')$, and again using plugging in (B.4), (B.5), and (B.6) to (B.3) and comparing to (6.4), we see that $\left|\mathrm{Cl}_{2d\mathcal{O}',\Sigma}(\mathcal{O}')\right| = 2\left|\mathrm{Cl}_{d\mathcal{O}',\Sigma}(\mathcal{O}')\right|$. □

References

[1] D. M. Appleby. Symmetric informationally complete-positive operator valued measures and the extended Clifford group. *J. Math. Phys.*, 46(5):052107, 29, 2005.
[2] D. M. Appleby and S. T. Flammia. Personal communication, 2024.
[3] D. M. Appleby, S. T. Flammia, and C. A. Fuchs. The Lie algebraic significance of symmetric informationally complete measurements. *J. Math. Phys.*, 52(2):022202, 34, 2011.
[4] D. M. Appleby, H. Yadsan-Appleby, and G. Zauner. Galois automorphisms of a symmetric measurement. *Quantum Inf. Comput.*, 13(7-8):672–720, 2013.
[5] M. Appleby, I. Bengtsson, M. Grassl, M. Harrison, and G. McConnell. SIC-POVMs from Stark units: prime dimensions $n^2 + 3$. *J. Math. Phys.*, 63(11):Paper No. 112205, 31, 2022.
[6] M. Appleby, T.-Y. Chien, S. Flammia, and S. Waldron. Constructing exact symmetric informationally complete measurements from numerical solutions. *J. Phys. A*, 51(16):165302, 40, 2018.
[7] M. Appleby, S. Flammia, and G. S. Kopp. A constructive approach to Zauner's conjecture via the Stark conjectures, 2024+. In preparation.
[8] M. Appleby, S. Flammia, G. McConnell, and J. Yard. SICs and algebraic number theory. *Found. Phys.*, 47(8):1042–1059, 2017.
[9] M. Appleby, S. Flammia, G. McConnell, and J. Yard. Generating ray class fields of real quadratic fields via complex equiangular lines. *Acta Arith.*, 192(3):211–233, 2020.
[10] I. Bengtsson, M. Grassl, and G. McConnell. SIC-POVMs from Stark units: Dimensions $n^2 + 3 = 4p$, p prime, 2024. Preprint arXiv:2403.02872.
[11] D. Byeon, M. Kim, and J. Lee. Mollin's conjecture. *Acta Arith.*, 126(2):99–114, 2007.
[12] F. Campagna and R. Pengo. Entanglement in the family of division fields of elliptic curves with complex multiplication. *Pacific J. Math.*, 317(1):21–66, 2022.
[13] B. Chen, T. Li, and S.-M. Fei. General SIC measurement-based entanglement detection. *Quantum Inf. Process.*, 14(6):2281–2290, 2015.
[14] T.-Y. Chien and S. Waldron. A characterization of projective unitary equivalence of finite frames and applications. *SIAM J. Discrete Math.*, 30(2):976–994, 2016.
[15] H. Cohen. *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.
[16] Computational Algebra Group, Sydney. *Magma handbook*, 2015.
[17] H. Dai, S. Fu, and S. Luo. Detecting magic states via characteristic functions. *Internat. J. Theoret. Phys.*, 61(2):Paper No. 35, 18, 2022.
[18] P. Delsarte, J. M. Goethals, and J. J. Seidel. Bounds for systems of lines, and Jacobi polynomials. *Philips Res. Rep.*, 30:91–105, 1975.
[19] P. A. M. Dirac. *The Principles of Quantum Mechanics.* Oxford, at the Clarendon Press, 1947. 3rd ed.
[20] K. Dixon and S. Salamon. Moment maps and Galois orbits in quantum information theory. *SIAM J. Appl. Algebra Geom.*, 4(4):502–531, 2020.
[21] A. Fannjiang and T. Strohmer. The numerics of phase retrieval. *Acta Numer.*, 29:125–228, 2020.
[22] S. Flammia. Exact SIC fiducial vectors. `http://www.physics.usyd.edu.au/~sflammia/SIC/`.
[23] C. A. Fuchs, M. C. Hoang, and B. C. Stacey. The SIC question: History and state of play. *Axioms*, 6(3):21, 2017.
[24] C. A. Fuchs and R. Schack. Quantum-Bayesian coherence. *Rev. Mod. Phys.*, 85:1693–1715, Dec 2013.
[25] M. Grassl. Tomography of quantum states in small dimensions. In *Proceedings of the Workshop on Discrete Tomography and its Applications*, volume 20 of *Electron. Notes Discrete Math.*, pages 151–164. Elsevier Sci. B. V., Amsterdam, 2005.
[26] M. Grassl. Personal communication, 2022.
[27] M. Grassl. Personal communication, 2024.

[28] F. Halter-Koch. *Quadratic Irrationals: An Introduction to Classical Number Theory*. Pure and Applied Mathematics (Boca Raton). CRC Press, Boca Raton, FL, 2013.

[29] M. A. Herman and T. Strohmer. High-resolution radar via compressed sensing. *IEEE Trans. Signal Process.*, 57(6):2275–2284, 2009.

[30] S. G. Hoggar. Two quaternionic 4-polytopes. In *The Geometric Vein*, pages 219–230. Springer, New York-Berlin, 1981.

[31] S. G. Hoggar. 64 lines from a quaternionic polytope. *Geom. Dedicata*, 69(3):287–289, 1998.

[32] G. S. Kopp. *Indefinite Theta Functions and Zeta Functions*. PhD thesis, University of Michigan, Ann Arbor, Michigan, USA, Aug. 2017.

[33] G. S. Kopp. SIC-POVMs and the Stark conjectures. *Int. Math. Res. Not. IMRN*, 2021(18):13812–13838, 2021.

[34] G. S. Kopp and J. C. Lagarias. Ray class groups and ray class fields for orders of number fields, 2022. Preprint arXiv:2212.09177.

[35] G. S. Kopp and J. C. Lagarias. Unit-generated orders of real quadratic fields I. Class number bounds, 2024+. In preparation.

[36] G. S. Kopp and J. C. Lagarias. Unit-generated orders of real quadratic fields II. Class monoids and special ray class fields, 2024+. In preparation.

[37] J. Neukirch. *Algebraic Number Theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher.

[38] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves. Symmetric informationally complete quantum measurements. *J. Math. Phys.*, 45(6):2171–2180, 2004.

[39] A. J. Scott. Tight informationally complete quantum measurements. *J. Phys. A*, 39(43):13507–13530, 2006.

[40] A. J. Scott. SICs: Extending the list of solutions, 2017. Preprint arXiv:1703.03993.

[41] A. J. Scott and M. Grassl. Symmetric informationally complete positive-operator-valued measures: a new computer study. *J. Math. Phys.*, 51(4):042203, 16, 2010.

[42] H. M. Stark. L-functions at $s = 1$. III. Totally real fields and Hilbert's twelfth problem. *Advances in Math.*, 22(1):64–84, 1976.

[43] H. M. Stark. Class fields for real quadratic fields and L-series at 1. In *Algebraic Number Fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 355–375. Academic Press, London-New York, 1977.

[44] A. Szymusiak and W. Słomczyński. Informational power of the Hoggar symmetric informationally complete positive operator-valued measure. *Phys. Rev. A*, 94:012122, Jul 2016.

[45] A. Tavakoli, I. Bengtsson, N. Gisin, and J. M. Renes. Compounds of symmetric informationally complete measurements and their application in quantum key distribution. *Phys. Rev. Res.*, 2:043122, Oct 2020.

[46] S. F. D. Waldron. *An Introduction to Finite Tight Frames*. Applied and Numerical Harmonic Analysis. Birkhäuser/Springer, New York, 2018.

[47] M. M. Wood. Gauss composition over an arbitrary base. *Adv. Math.*, 226(2):1756–1771, 2011.

[48] G. Zauner. *Quantendesigns: Grundzüge einer nichtkommutativen Designtheorie*. PhD thesis, University of Vienna, Vienna, Austria, 1999.

[49] G. Zauner. Quantum designs: Foundations of a noncommutative design theory. *Int. J. Quantum Inf.*, 9(1):445–507, 2011.

Department of Mathematics, Louisiana State University, Baton Rouge, LA, USA
Email address: kopp@math.lsu.edu

Department of Mathematics, University of Michigan, Ann Arbor, MI, USA
Email address: lagarias@umich.edu