

# GENERATING RAY CLASS FIELDS OF REAL QUADRATIC FIELDS VIA COMPLEX EQUIANGULAR LINES

MARCUS APPLEBY, STEVEN FLAMMIA, GARY MCCONNELL, AND JON YARD

ABSTRACT. Let  $K$  be a real quadratic field. For certain  $K$  with sufficiently small discriminant we produce explicit unit generators for specific ray class fields of  $K$  using a numerical method that arose in the study of complete sets of equiangular lines in  $\mathbb{C}^d$  (known in quantum information as symmetric informationally complete measurements or SICs). The construction in low dimensions suggests a general recipe for producing unit generators in infinite towers of ray class fields above arbitrary  $K$  and we summarise this in a conjecture. Such explicit generators are notoriously difficult to find, so this recipe may be of some interest.

In a forthcoming paper we shall publish promising results of numerical comparisons between the logarithms of these canonical units and the values of  $L$ -functions associated to the extensions, following the programme laid out in the Stark Conjectures.

Let  $D$  be a square-free integer  $\geq 2$ . Throughout this paper  $K = \mathbb{Q}(\sqrt{D})$  will denote the corresponding real quadratic field with ring of integers  $\mathbb{Z}_K$ . Let  $d \geq 4$  be an integer for which  $D$  is the square-free part of  $(d-1)^2 - 4 = (d+1)(d-3)$ . By Lemma 2 below there are infinitely many such  $d$  for any given  $D$ . Conversely every  $d \geq 4$  corresponds to a non-trivial value of  $D$ .

Set  $d' = 2d$  if  $d$  is even and  $d' = d$  if  $d$  is odd. We abbreviate the ideal  $d'\mathbb{Z}_K$  to  $d'$ . This will be the finite part of the modulus for all of the ray class fields discussed in this paper. Let the infinite primes of  $K$  be denoted by  $\infty_1, \infty_2$ . Write  $\mathfrak{R} = \mathfrak{R}_{1,2}$  for the ray class field of  $K$  modulo  $d'$  with ramification allowed at both infinite primes; similarly we write  $\mathfrak{R}_0, \mathfrak{R}_1$  and  $\mathfrak{R}_2$  when ramification is allowed respectively at no infinite primes, at  $\infty_1$  and at  $\infty_2$ .

Let  $\mathbb{C}^d$  be a  $d$ -dimensional complex vector space equipped with the standard hermitian inner product  $(\cdot, \cdot)$ . The span  $\mathbb{C}\mathbf{v}$  of  $\mathbf{v} \in \mathbb{C}^d$  is a (complex) line. The hermitian angle between two lines  $\mathbb{C}\mathbf{v}, \mathbb{C}\mathbf{w}$  is  $\cos^{-1}\left(\frac{|(\mathbf{v}, \mathbf{w})|}{\|\mathbf{v}\|\|\mathbf{w}\|}\right)$ . A set of  $n$  lines is said to be equiangular if any two distinct lines in the set subtend the same hermitian angle. It can be shown [8] that for any set of  $n$  lines  $n \leq d^2$ , and if  $n = d^2$  we say the set is *complete*. We call a complete set of equiangular lines a SIC following the terminology established in quantum information [17].

Explicit constructions of SICs have been found in dimensions  $d = 1, \dots, 20; 24; 28; 35; 48$ . Numerical evidence suggests that they exist for all  $d \leq 121$ , and they are conjectured to exist in every finite dimension [17, 20, 21, 25]. This paper is exclusively concerned with SICs that are also orbits of the  $d$ -dimensional Heisenberg group. We define this group action in §2.1. For every Heisenberg SIC there is a *distinguished basis* that is unique up to an overall multiplicative factor, as defined in §2.1.

Let  $E$  be a Heisenberg SIC. For each line  $\mathbb{C}\mathbf{v} \in E$ , let  $v_j$  be the components of  $\mathbf{v}$  relative to any distinguished basis, and let  $S_{\mathbf{v}} = \{\frac{v_j}{v_k} : j, k = 0, 1, \dots, d-1; v_k \neq 0\}$ . Define  $S(E) = \bigcup_{\mathbf{v} \in E} S_{\mathbf{v}}$ , and define  $\mathbb{Q}(E) = \mathbb{Q}(S(E))$ . Notice that the field  $\mathbb{Q}(E)$  is independent of both the choice of spanning vectors and the choice of distinguished basis. Consider the following set of 21 dimensions:

$$(1) \quad d = 4, \dots, 20; 24; 28; 35; 48.$$

Then we have the following result and subsequent natural conjecture:

**Proposition 1.** *For every  $d$  in (1) there exists a Heisenberg SIC  $E$  such that  $\mathbb{Q}(E) = \mathfrak{R}$ .*

**Conjecture 1.** *The statement of Proposition 1 holds for every dimension  $d \geq 4$ .*

These statements are a substantial strengthening of results and conjectures in [2]. We remark that for some of the dimensions in (1) there exist SICs for which  $\mathbb{Q}(E) \neq \mathfrak{R}$ , but for every such set which has been calculated  $\mathbb{Q}(E)$  is an extension of  $\mathfrak{R}$  which is Galois over  $\mathbb{Q}$ .

The problem of finding explicit generators for arbitrary class fields of an algebraic number field  $K$  lies at the heart of algebraic number theory. Little is known outside the cases where  $K$  is either  $\mathbb{Q}$  or an imaginary quadratic field [7], or a CM field [22]. The fact that a geometric problem seems to

yield a canonical Galois orbit of generators for certain specific ray class fields is therefore of some interest.

After introducing the necessary geometric and number-theoretic apparatus in the next two sections, we establish some properties of the ray class fields in §4. In §5 and §6 we relate invariants of the geometric objects to arithmetic quantities in the ray class fields and to associated canonical units. The last section is concerned with verifying Proposition 1, and we illustrate these general discoveries in the first appendix by focussing on the particular case of dimension 19. In the final appendix, we survey the history and current state of knowledge regarding complete sets of equiangular lines and the closely related problem of Zauner's conjecture [25].

## 2. SICS AND THEIR CLASSIFICATION

**2.1. Heisenberg groups.** With one exception<sup>1</sup> every known SIC is a Heisenberg SIC, and from now on we use the term SIC to mean a Heisenberg SIC. We now describe and classify these structures.

We first need to deal with the mismatch arising from the fact that lines are projective objects, whereas  $\mathcal{H}(d)$  consists of unitary operators. The field  $\mathbb{Q}(E)$  defined in the Introduction is the minimal field of definition for  $E$  since  $\bigcap_{\mathbf{w} \in \mathbf{C}\mathbf{v}} \mathbb{Q}(w_0, \dots, w_{d-1}) = \mathbb{Q}(S_{\mathbf{v}})$  for every line  $\mathbf{C}\mathbf{v} \in E$ . It would be possible to choose, as line-representative, a spanning vector whose components generate  $\mathbb{Q}(S_{\mathbf{v}})$ . However, there is no natural preferred way of doing this. Instead of a vector it is therefore convenient to represent the line by the rank-1 projection matrix  $\Pi$  with elements

$$(2) \quad \Pi_{jk} = \frac{v_j v_k^*}{(\mathbf{v}, \mathbf{v})},$$

where the elements are chosen in the same distinguished basis used to define  $S_{\mathbf{v}}$ . This establishes a bijective correspondence between lines and rank-1 projectors, so henceforth we identify the lines with their corresponding projectors. Moreover, the fact that for every known case in the dimensions in (1) we have that  $\mathbb{Q}(E)$  is Galois over  $\mathbb{Q}$  means that  $\mathbb{Q}(\{\Pi_{jk} : \Pi \in E\}) = \mathbb{Q}(E)$ . We then define an action of the unitary group  $U(d)$  on the lines by

$$(3) \quad U : \Pi \rightarrow U\Pi U^\dagger$$

where  $U^\dagger$  is the adjoint of  $U$ . Note that the action is projective, in that two unitary operators which are equal modulo the centre of  $U(d)$  give the same transformation.

For all  $n$  let  $\zeta_n = e^{\frac{2\pi i}{n}}$ .

**Definition 1.** *The Heisenberg group  $\mathcal{H}(d)$  in dimension  $d$  is the order  $d^! d^2$  matrix group  $\langle \zeta_{d^!} I, X_d, Z_d \rangle$  where  $I$  is the  $d \times d$  identity matrix and  $X_d, Z_d$  are the  $d \times d$  unitary matrices*

$$(4) \quad X_d = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}, \quad Z_d = \begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & \zeta_d & 0 & 0 & \dots & 0 \\ 0 & 0 & \zeta_d^2 & 0 & \dots & 0 \\ 0 & 0 & 0 & \zeta_d^3 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & \zeta_d^{d-1} \end{pmatrix}.$$

Note that, while  $X_d, Z_d$  are order  $d$ , the matrix  $\zeta_{d^!} I$  is order  $d^!$ . This differs from the definition used by many authors, who take the first generator to be  $\zeta_d I$ . The above definition has the merit that it simplifies some of the formulae in even dimensions.

The group  $\mathcal{H}(d)$  sits inside the short exact sequence

$$1 \longrightarrow \langle \zeta_{d^!} I \rangle \longrightarrow \mathcal{H}(d) \longrightarrow \langle \overline{X}_d \rangle \times \langle \overline{Z}_d \rangle \longrightarrow 1,$$

where the bar denotes the image of the operators under the natural surjection. The class of the extension [15, §1] is given by the commutation rule of the matrices  $X_d, Z_d$ , viz.:  $Z_d X_d = \zeta_d X_d Z_d$ . Concretely the centre of  $\mathcal{H}(d)$  consists of the scalar matrices  $\zeta_{d^!}^r I_d$  for  $0 \leq r \leq (d^! - 1)$ . The two cyclic groups of order  $d$  are the images under projective equivalence of the two cyclic subgroups  $\langle X_d \rangle$  and  $\langle Z_d \rangle$  of  $U(d)$ .

<sup>1</sup>In dimension 8 there is a complete set of equiangular lines which is an orbit of the three-fold tensor product of  $\mathcal{H}(2)$ , in addition to the  $\mathcal{H}(8)$  orbits. Of course we do not know if similarly non- $\mathcal{H}(d)$ -symmetric constructions exist in other dimensions, though for a fascinating insight into this question see [27].

We are now ready to define a (Heisenberg) SIC. Let  $f$  be any irreducible unitary representation of  $\mathcal{H}(d)$  on  $\mathbb{C}^d$ . There exists an orthonormal basis with respect to which the matrix representing  $f(Z_d)$  is diagonal and the one representing  $f(X_d)$  is identical with the matrix  $X_d$ . This basis is unique up to multiplication by an overall unimodular complex number, and is the *distinguished basis* referred to in the Introduction. By a slight abuse of notation we identify the elements of  $\mathcal{H}(d)$  with their images under  $f$ . An  $\mathcal{H}(d)$ -set of lines is any set of lines of the form

$$(5) \quad \{W\Pi W^\dagger : W \in \mathcal{H}(d)\} = \{X_d^{j_1} Z_d^{j_2} \Pi Z_d^{-j_2} X_d^{-j_1} : j_1, j_2 = 0, 1, \dots, d-1\}$$

for some given projector  $\Pi$ . A SIC is an  $\mathcal{H}(d)$ -set which is also equiangular. We refer to  $\Pi$  as a fiducial projector for the set, and to any corresponding spanning vector as a fiducial vector. As for any SIC [17, 25], the hermitian angle between its elements is  $\cos^{-1}\left(\frac{1}{\sqrt{d+1}}\right)$ .

**2.2. Classification.** We now classify the SICs in a given dimension. We do so using the extended Clifford group [1],  $\text{EC}(d)$ , defined to be the normalizer of  $\mathcal{H}(d)$  inside  $\text{EU}(d)$ , where  $\text{EU}(d)$  is the group of all unitary and anti-unitary operators in dimension  $d$  [24, Chap. 26]. Let  $f$  be a given representation of  $\mathcal{H}(d)$ , and suppose that  $\Pi$  is a fiducial projector for a SIC with respect to  $f$ . Then it is easily seen that  $U\Pi U^\dagger$  is also a SIC fiducial projector with respect to  $f$ , for all  $U \in \text{EC}(d)$  (where, by an abuse of notation, we make no distinction between the normalizers of different representations of  $\mathcal{H}(d)$ ). Moreover the two sets generate the same field over  $\mathbb{Q}$ . The SICs with respect to  $f$  thus split into orbits under the action of  $\text{EC}(d)$ . For every known case in dimensions greater than 3 one finds that distinct  $\text{EC}(d)$  orbits are inequivalent with respect to the action of  $\text{EU}(d)$ : i.e. if  $U \in \text{EU}(d)$  is such that  $\Pi$  and  $U\Pi U^\dagger$  are both SIC fiducial projectors with respect to  $f$ , then  $U \in \text{EC}(d)$ . Let  $f_1$  and  $f_2$  be any two representations of  $\mathcal{H}(d)$ . It is easily seen that every SIC fiducial for  $f_1$  is unitarily conjugated to a SIC fiducial for  $f_2$ , even when  $f_1$  and  $f_2$  are inequivalent. Consequently every SIC is unitarily conjugated to a SIC for the representation  $f$ . We refer to the set of SICs obtained by conjugating the elements of an  $\text{EC}(d)$  orbit for  $f$  with arbitrary unitaries as a *full EC}(d) orbit*. The collection of all SICs thus splits into a collection of disjoint full  $\text{EC}(d)$  orbits.

Aside<sup>2</sup> from dimension 3 there are only finitely many full  $\text{EC}(d)$  orbits in every known case. In the classification scheme of [20] the orbits for  $d \neq 3$  are specified by the dimension followed by a letter. For dimensions in the list (1), the orbits that are known to generate  $\mathfrak{R}$  over the rationals are

$$(6) \quad 4a, 5a, 6b, 7b, 8b, 9a, 10a, 11c, 12b, 13ab, 14ab, 15d, 16ab, 17c, 18ab, 19e, 20ab, 24c, 28c, 35j, 48g$$

while orbits for which the field generated is known to contain, but to be strictly larger than  $\mathfrak{R}$  are

$$(7) \quad 7a, 8a, 11ab, 12a, 15abc, 17ab, 19abcd$$

where two or more letters indicates several orbits—for instance  $13ab$  is shorthand for  $13a, 13b$ . See [2, 3] for a detailed analysis of the number fields associated to the orbits in the two lists. Scott and Grassl [20] have, with high probability, identified every orbit for  $d \leq 50$ ; however, many of them are only known numerically. The above two lists contain every orbit for which an exact solution is known. In the first list (6) the number of orbits in each dimension is the same as the class number of  $K$  for that dimension. This might not be an accident, as we discuss in §5.

**2.3. Structure of  $\text{EC}(d)$ .** We now describe the structure of  $\text{EC}(d)$ . Since we are only interested in the projective action  $\Pi \rightarrow U\Pi U^\dagger$ , it is sufficient to consider  $\text{EC}(d)/\langle \zeta_d I \rangle$ , the quotient of  $\text{EC}(d)$  by its centre. It is shown in [1] that there is a natural homomorphism (isomorphism when  $d$  is odd) of a semidirect product  $\text{ESp}_2(\mathbb{Z}/d'\mathbb{Z}) \ltimes (\mathbb{Z}/d\mathbb{Z})^2$  onto  $\text{EC}(d)/\langle \zeta_d I \rangle$ . Here  $\text{ESp}_2(\mathbb{Z}/d'\mathbb{Z})$  is the *extended symplectic group*, consisting of all matrices in  $\text{GL}_2(\mathbb{Z}/d'\mathbb{Z})$  with determinant  $\pm 1$ . It is also convenient to define the *symplectic group*  $\text{Sp}_2(\mathbb{Z}/d'\mathbb{Z})$ , the subgroup consisting of all matrices in  $\text{ESp}_2(\mathbb{Z}/d'\mathbb{Z})$  with determinant  $+1$ . The natural homomorphism restricts to a homomorphism of  $\text{Sp}_2(\mathbb{Z}/d'\mathbb{Z}) \ltimes (\mathbb{Z}/d\mathbb{Z})^2$  onto  $\text{C}(d)/\langle \zeta_d I \rangle$ , where  $\text{C}(d)$  is the group of unitaries in  $\text{EC}(d)$ . The second component in the semidirect product maps onto  $\mathcal{H}(d)/\langle \zeta_d I \rangle$ . To understand the role of the first component define

$$(8) \quad \Delta_j = (-\zeta_{2d})^{j_1 j_2} X_d^{j_1} Z_d^{j_2}.$$

<sup>2</sup>In  $d = 3$  there is an uncountably infinite pencil of inequivalent SICs with (necessarily) transcendental fields of definition apart from special points [2, §10],[27]. For an in-depth look at the case  $d = 3$ , see also [11].

Then, if  $F$  is any element of  $\mathrm{ESp}_2(\mathbb{Z}/d'\mathbb{Z})$ , and if  $U\langle\zeta_{d'}I\rangle$  is the image of  $(F, (0, 0))$  under the canonical homomorphism,

$$(9) \quad U\Delta_{\mathbf{j}}U^\dagger = \Delta_{F\mathbf{j}}$$

The operators  $\Delta_{\mathbf{j}}$  play an important role in §5 and §6, where we link the geometry of the equiangular lines to the arithmetic of the ray class fields. In these sections we will need one more concept. Given a SIC fiducial projector  $\Pi$ , we define its stabilizer group to consist of the elements of  $\mathrm{EC}(d)/\langle\zeta_{d'}I\rangle$  leaving it invariant under the projective action. Every known orbit contains a fiducial such that

- Under the canonical homomorphism the stabilizer group is the image of a subgroup of the form  $\{(F, (0, 0)) : F \in \mathbf{S}_0\}$ , where  $\mathbf{S}_0$  is a subgroup of  $\mathrm{ESp}_2(\mathbb{Z}/d'\mathbb{Z})$ .
- $\mathbf{S}_0$  contains an element of  $\mathrm{Sp}_2(\mathbb{Z}/d'\mathbb{Z})$  which is order 3 and has trace  $-1 \pmod{d}$ .

We refer to such a fiducial as *centred* (in [2] such fiducials were called “simple”). Although it is not part of the definition let us note that  $\mathbf{S}_0$  is in fact always cyclic when  $d \geq 4$ .

### 3. PELL'S EQUATION AND TOWERS OF RAY CLASS FIELDS OVER $K$

We now prove the assertions made in the Introduction about infinite sequences of dimensions  $d_1, d_2, \dots$  all of which give rise to the same value of  $D$ . Conjecturally these give us ‘towers’ of ray class fields lying above each quadratic field  $K$ .

Fix  $D$ ,  $K = \mathbb{Q}(\sqrt{D})$  as above. Fix  $\infty_1$  to be the place associated to the embedding of  $K$  into  $\mathbb{R}$  under which  $\sqrt{D}$  is sent to the positive square root of  $D$ , and then write  $u_f \in \mathbb{Z}_K^\times$  for the fundamental unit of  $K$  which is  $> 1$  under  $\infty_1$ . If the norm of  $u_f$  is  $-1$  then set  $u_D = u_f^2$ ; otherwise set  $u_D = u_f$ . In other words,  $u_D$  is the first positive power of  $u_f$  of norm 1.

**Lemma 2.** *With  $D$ ,  $u_D$  as above the following are equivalent.*

- $d$  is a positive integer such that the square-free part of  $(d-1)^2 - 4$  is equal to  $D$
- $\frac{d-1}{2}$  is the rational part of  $u_D^r$  for some  $r \in \mathbb{N}$ .

*Proof.* Statement (i) is equivalent to saying there exists  $y \in \mathbb{Z}$  such that  $(\frac{d-1}{2})^2 - D(\frac{y}{2})^2 = 1$ , which in turn is equivalent to  $\frac{d-1}{2} + \frac{y}{2}\sqrt{D}$  being an element of  $K$  of norm 1. But it is also a root of the monic integral polynomial  $X^2 - (d-1)X + 1$ , hence a unit. Therefore [7, §11B] it is a power of  $u_D$ , proving (ii). The converse is just a restatement of the definitions.  $\square$

**Corollary.** *For every square-free value of  $D \geq 2$  there exist infinitely many values of  $d$  such that the square-free part of  $(d-1)^2 - 4 = (d+1)(d-3)$  is equal to  $D$ .*  $\square$

**Definition 2.** *All  $d$  yielding the same value of  $D$  are indexed by the appropriate power of  $u_D$ :*

$$(10) \quad d_r = 1 + u_D^r + u_D^{-r}.$$

In particular,  $d_1$  is the smallest dimension corresponding to  $D$ . We shall generally omit reference to the underlying  $D$  but *the notation  $d_r$  always applies with reference to a specific fixed value of  $D$* . Note that the rational part of  $u_D^r$  is given by  $\frac{u_D^r + u_D^{-r}}{2} = \cosh(r \log u_D)$ . The Chebyshev polynomials of the first kind  $T_n$  tell us how to go from the rational part of  $u_D^r$  to that of  $u_D^{rs}$ :

$$(11) \quad T_s\left(\frac{d_r-1}{2}\right) = T_s(\cosh(r \log u_D)) = \cosh(rs \log u_D) = \frac{d_{rs}-1}{2} = T_r\left(\frac{d_s-1}{2}\right).$$

Let us define a shifted version of the functions  $T_n$  by

$$T_n^*(x) = 1 + 2T_n\left(\frac{x-1}{2}\right),$$

and for convenience extend it to negative  $n$  by defining  $T_{-n}^* = T_n^*$ . Equation (11) may be rephrased in terms of the new functions  $T_n^*$  and rearranged to read:

$$(12) \quad T_r^*(T_s^*(d_1)) = T_r^*(d_s) = d_{rs} = d_{sr} = T_s^*(d_r) = T_s^*(T_r^*(d_1)).$$

It is also easy to show that  $d_1, d_2, d_3, \dots$  is a strictly increasing sequence of positive integers.

**Proposition 3.** *Within each set of dimensions  $\{d_r\}_{r \geq 1}$  corresponding to a fixed  $D$  there are infinitely many distinct infinite sequences  $\{d_{k_1}, d_{k_2}, d_{k_3}, \dots\}$  with the property that  $d_{k_1} \mid d_{k_2} \mid d_{k_3} \dots$*

*Proof.* Fix  $D$ . The defining recursion for the Chebyshev polynomials:

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)$$

yields the following recursion for the shifted version:

$$T_n^*(x) = xT_{n-1}^*(x) - xT_{n-2}^*(x) + T_{n-3}^*(x).$$

If  $x \in \mathbb{Z}$  then all terms are in  $\mathbb{Z}$ , so for the particular case of a positive integer  $d$ :

$$(13) \quad T_n^*(d) \equiv T_{n-3}^*(d) \pmod{d}$$

and in fact for any positive integer  $r$  we have  $d_{nr} \equiv d_{(n-3)r} \pmod{d_r}$ . We now have three cases according to the congruence class of  $n$  modulo 3.

- **C0:**  $n \equiv 0 \pmod{3}$ :  $T_0^*(d_r) = 3$ , implying  $d_{nr} - 3$  is a multiple of  $d_r$ .
- **C1:**  $n \equiv 1 \pmod{3}$ :  $T_1^*(d_r) = d_r$ , implying  $d_{nr}$  is a multiple of  $d_r$ .
- **C2:**  $n \equiv 2 \pmod{3}$ :  $T_2^*(d_r) = d_r(d_r - 2)$ , implying  $d_{nr}$  is a multiple of  $d_r$ .

It follows that, if  $i_j$  is any increasing sequence of integers coprime to 3 and such that  $i_1 \mid i_2 \mid i_3 \mid \dots$ , then  $d_{i_1} \mid d_{i_2} \mid d_{i_3} \mid \dots$ . To see that there are infinitely many such dimension towers observe that the fact that  $d_r > d_s > 3$  for all  $r > s$  means that if  $m > n$  then  $d_{3^m i_j}$  is not a multiple of  $d_{3^n i_k}$  for all  $j, k$ .  $\square$

**Corollary.** *If Conjecture 1 is true then for every square-free value of  $D \geq 2$  there exist infinitely many infinite ray class field towers above each  $\mathbb{Q}(\sqrt{D})$  whose successive generators may be found by constructing  $\mathcal{H}(d)$ -sets of equiangular lines in  $\mathbb{C}^d$ .*  $\square$

#### 4. PROPERTIES OF THE RAY CLASS FIELDS

In this section we establish some properties of fields of the type considered in this paper. Fix  $D$  and an associated dimension  $d$  and recall that  $d' = d$  if  $d$  is odd and  $d' = 2d$  if  $d$  is even. Write  $\sigma_D \in \text{Gal}(K/\mathbb{Q})$  for the automorphism which sends  $\sqrt{D}$  to  $-\sqrt{D}$  and observe that  $\sigma_D$  interchanges  $\infty_1$  and  $\infty_2$ .

Lift  $\sigma_D$  to an automorphism  $\hat{\sigma}_D \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  and consider the field  $\hat{\sigma}_D(\mathfrak{R})$  as sitting inside a normal closure of  $\mathfrak{R}/\mathbb{Q}$ . Being the image of  $\mathfrak{R}$  means it is also an abelian extension of  $K$  with Galois group equal to  $\hat{\sigma}_D \text{Gal}(\mathfrak{R}/K) \hat{\sigma}_D^{-1}$ . But the finite part of the conductor of  $\mathfrak{R}/K$  is a rational integer, so it is stable under  $\hat{\sigma}_D$ : hence  $\hat{\sigma}_D(\mathfrak{R})$  is an extension of  $K$  with finite conductor  $d'$ , therefore contained in  $\mathfrak{R}$ . Comparison of degrees then shows that it must actually be equal to  $\mathfrak{R}$ .

So  $\mathfrak{R}/\mathbb{Q}$  is a Galois extension. Indeed, the fields  $\mathfrak{R}_1$  and  $\mathfrak{R}_2$  have isomorphic Galois groups over  $K$  which are mapped into one another by the action of  $\hat{\sigma}_D$ , and  $\mathfrak{R}$  is their compositum.

We now show that  $\mathfrak{R}$  contains the  $d'$ -th roots of unity. The extension  $K(\mu_{d'})/K$  is clearly unramified outside primes dividing  $\mathfrak{d}' = d' \infty_1 \infty_2$ .  $\mathfrak{R}$  is the fixed field of the Artin symbols  $((\alpha), \mathfrak{R}/K)$  running over principal ideals generated by those  $\alpha \in \mathbb{Z}_K$  which are multiplicatively congruent to 1 modulo  $\mathfrak{d}'$ , written  $\alpha \equiv 1 \pmod{\times \mathfrak{d}'}$ . To show that  $\mu_{d'}$  is contained in  $\mathfrak{R}$  it therefore suffices to show that these Artin symbols have trivial action upon a primitive  $d'$ -th root of unity  $\zeta_{d'}$ . This action translates via the restriction map [13, X §1 A4] to raising  $\zeta_{d'}$  to the power of the absolute element norm  $\mathbf{N}_{K/\mathbb{Q}}(\alpha)$ . But  $d' \in \mathbb{Z}$  and  $\infty_1, \infty_2$  are switched by the action of  $\sigma_D$ . Therefore

$$\alpha \equiv 1 \pmod{\times \mathfrak{d}'} \implies \alpha^{\sigma_D} \equiv 1 \pmod{\times \mathfrak{d}'} \implies \mathbf{N}_{K/\mathbb{Q}}(\alpha) = \alpha \alpha^{\sigma_D} \equiv 1 \pmod{\times \mathfrak{d}'}$$

So  $K(\mu_{d'}) \subseteq \mathfrak{R}$  as claimed. Since  $d' > 4$  for all dimensions  $d \geq 4$  and  $K$  is real, it follows that  $\mathfrak{R}/K$  is non-trivial and in particular totally complex. Moreover the totally real field  $\mathfrak{R}_0$  is always a proper extension of  $K$ : for  $\zeta_{d'} + \zeta_{d'}^{-1} \in \mathfrak{R}_0$  since  $\gcd(d', D) = 1$  or 3 and so  $d' > 4$  implies that  $\zeta_{d'} + \zeta_{d'}^{-1} \notin K$ . Interestingly,  $\mathfrak{R}_0$  is *abelian* over  $\mathbb{Q}$  in dimensions  $d = 4, 5, 7, 8$ . However this is *never* true of  $\mathfrak{R}$ . Moreover the structure of  $\mathfrak{R}/\mathfrak{R}_0$  is always  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ , as we now show.

**Proposition 4.** *Fix  $D$  and an associated  $d$ . The Galois groups  $\text{Gal}(\mathfrak{R}/\mathfrak{R}_1)$ ,  $\text{Gal}(\mathfrak{R}_1/\mathfrak{R}_0)$ ,  $\text{Gal}(\mathfrak{R}/\mathfrak{R}_2)$  and  $\text{Gal}(\mathfrak{R}_2/\mathfrak{R}_0)$  all have order 2.*

**Corollary.** (i)  $\mathfrak{R}$  is non-abelian over  $\mathbb{Q}$ ; and  $\mathfrak{R}_1$  and  $\mathfrak{R}_2$  are non-Galois over  $\mathbb{Q}$ .

(ii) Let  $k$  be any divisor of  $d'$  which is  $> 2$ . Then  $\mathfrak{R} = \mathfrak{R}_1(\zeta_k) = \mathfrak{R}_2(\zeta_k)$ .

*Proof.* If  $\mathfrak{R}/\mathbb{Q}$  were abelian then the inner automorphism  $\hat{\sigma}_D$  would be trivial. Since  $\mathfrak{R}$  is the compositum of  $\mathfrak{R}_1$  and  $\mathfrak{R}_2 = \mathfrak{R}_1^{\hat{\sigma}_D}$  it would follow that  $\mathfrak{R} = \mathfrak{R}_1 = \mathfrak{R}_2$ . But the Galois group of  $\mathfrak{R}/\mathfrak{R}_1$  is non-trivial by the Proposition, a contradiction, proving (i). For (ii) just combine the facts that  $\mathfrak{R}_1$  is not totally complex and  $K(\mu_{d'}) \subseteq \mathfrak{R}$ .  $\square$

*Proof.* (of Proposition 4). Let  $h_K$  denote the class number of  $\mathbb{Z}_K$ . If  $\mathfrak{m}$  is any modulus of  $K$  we denote by  $U_{\mathfrak{m}}^1$  the subgroup of  $U_K = \mathbb{Z}_K^\times$  consisting of units  $\equiv 1 \pmod{\times \mathfrak{m}}$ . This has finite index  $[U_K : U_{\mathfrak{m}}^1]$  in  $U_K$ . Express  $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$  as a product of its finite and infinite parts respectively and write  $\mathbf{Nm}_0$  for the (absolute) norm of the ideal  $\mathfrak{m}_0$ , or in other words the size of the multiplicative group of the ring  $\mathbb{Z}_K/\mathfrak{m}_0$ . Next, write  $\mathbf{Nm}_\infty$  for the size of the ‘signature’ group  $\{\pm 1\}^{r_{\mathfrak{m}}}$  where  $r_{\mathfrak{m}}$  in turn is the number of real places included in  $\mathfrak{m}_\infty$ . The formula [13, VI §1 thm 1] for the order  $h_{\mathfrak{m}}$  of the ray class group of  $K$  of modulus  $\mathfrak{m}$  is:

$$h_{\mathfrak{m}} = \frac{h_K \mathbf{Nm}_0 \mathbf{Nm}_\infty}{[U_K : U_{\mathfrak{m}}^1]}.$$

Recalling the shorthand  $\mathfrak{d}' = d' \infty_1 \infty_2$ , for our purposes it suffices to show that

$$(14) \quad U_{\mathfrak{d}'}^1 = U_{d' \infty_1}^1 = U_{d' \infty_2}^1 = U_{d'}^1,$$

for then the signature factor  $\mathbf{Nm}_\infty$  will tell the whole story of the growth in the size of the ray class groups as we successively add the real places into the modulus. Let  $u_f$  and  $u_D$  be defined as in section 3. Since  $K$  is a real quadratic field,

$$U_{\mathfrak{d}'}^1 \subseteq U_{d' \infty_1}^1 \subseteq U_{d'}^1 \subseteq \mathbb{Z}_K^\times = u_f^{\mathbb{Z}} \times \{\pm 1\}$$

with each inclusion being of finite index; and similarly with  $U_{d' \infty_2}^1$  replacing  $U_{d' \infty_1}^1$ . Now  $-1 \notin U_{d'}^1$  as  $d' > 2$ . Moreover since  $d'$  is invariant under  $\sigma_D$  it follows that  $U_{d'}^1$  is closed under  $\sigma_D$ . So all units in  $U_{d'}^1$  must have absolute norm  $+1$  and  $U_{d'}^1$  is a rank 1 torsion-free abelian group.

If  $\eta \in U_{d' \infty_1}^1$  then in particular  $\eta > 0$  under  $\infty_1$ ; since it has norm 1 it follows that  $\eta^{\sigma_D} = \eta^{-1}$  must also be positive under  $\infty_1$ . So  $(\eta^{\sigma_D})^{\sigma_D} = \eta$  is positive under  $\infty_1^{\sigma_D} = \infty_2$ , hence totally positive, proving that  $U_{\mathfrak{d}'}^1 = U_{d' \infty_1}^1 = U_{d' \infty_2}^1$ . But (14) is the same as asserting that every power of  $u_f$  which is congruent to 1 modulo  $d'$  is in fact totally positive, which from the foregoing discussion is the same as saying *no unit congruent to 1 modulo  $d'$  can be totally negative* (since we have just eliminated the other two possibilities).

Now by construction  $u_D$  is the first totally positive power of  $u_f$ , so any unit in  $U_{d'}^1$  which is both totally negative and congruent to 1 modulo  $d'$  must be of the form  $-u_D^r$  for some  $r \in \mathbb{Z}$ . Without loss of generality we may suppose that  $r$  is positive and minimally so.

For a moment let us suppose that  $d = d_1$  is the minimal dimension corresponding to this  $D$ , in the sense of (10). So  $u_D^r \equiv -1 \pmod{d_1'}$ , which means that  $u_D^r + u_D^{-r} \equiv -2 \pmod{d_1'}$  and so in particular, reducing modulo  $d_1$ :

$$(15) \quad u_D^r + u_D^{-r} \equiv -2 \pmod{d_1}.$$

On the other hand, in the notation of (10):

$$(16) \quad u_D^r + u_D^{-r} = -1 + d_r,$$

while from (12) and (13) we know that

$$(17) \quad d_r \equiv d_{r-3} \equiv \dots \equiv d_{\bar{r}} \pmod{d_1},$$

where we have denoted by  $\bar{r}$  the residue class of  $r$  modulo 3 and where  $d_0$  is understood to be 3 (see **C0** in the proof of Proposition 3). Combining (15) and (16) we see that we would require  $d_r \equiv -1 \pmod{d_1}$ , which is clearly impossible from (17) and the congruences **C0**, **C1**, **C2** unless  $d_1 = 4$  and  $3 \mid r$ , a case which we may in fact eliminate by direct calculation. This contradiction proves that for the minimal dimensions  $d_1$  the units cannot be totally negative, as required.

Now let  $d_j$  lie higher in some tower above  $d_1$  as per equation (10), so this time our ‘base’ dimension will be denoted  $d_b = T_b^*(d_1)$ . If  $b \equiv \pm 1 \pmod{3}$  then the above argument goes through unchanged: we apply **C1**, **C2** to the reduction step (17) on  $d_b$  as well as  $d_r$ . So we may assume  $3 \mid b$ . Write  $b = 3^t q$  where  $t \geq 1$  and  $\gcd(q, 3) = 1$ . But then  $d_b = T_q^*(d_{3^t}) \equiv 0 \pmod{d_{3^t}}$  by the same arguments. In other words, if  $u_D^r \equiv -1 \pmod{d_b'}$  then  $u_D^r \equiv -1 \pmod{d_{3^t}'}$ .

We take the case  $t = 1$  first. From **C0**, **C1**, **C2** we deduce that  $d_{3c}$  is *odd* for any integer  $c$ , hence in particular by Lemma 5 below the order of  $u_D$  modulo the ideal  $d_3^c \mathbb{Z}_K = d_3 \mathbb{Z}_K$  is 9. Therefore

$$u_D^{2r} \equiv 1 \equiv u_D^9 \pmod{d_3'}$$

But  $r$  is minimal, hence  $2r$  and  $9$  are minimal powers yielding  $1$  modulo  $d_3'$ , a contradiction. The argument is identical for  $t \geq 2$ . This completes the proof, conditional on Lemma 5 below.  $\square$

Finally we prove the technical lemma required in the last step of the proof of Prop. 4.

**Lemma 5.** *The order of  $u_D$  modulo  $d_r'$  is  $3r \frac{d_r'}{d_r}$  (i.e. it is  $3r$  if  $d_r$  is odd and  $6r$  if  $d_r$  is even).*

*Proof.* Notice that even when the norm of a fundamental unit is  $-1$  we still have the same relationship between the dimension  $d_r$  and the minimal polynomial for  $u_D^r$ , viz:

$$(18) \quad X^2 - (d_r - 1)X + 1 = (X - u_D^r)(X - u_D^{-r}),$$

so in particular by multiplying by  $(X - 1)$  it follows that  $u_D^{3r} \equiv 1 \pmod{d_r}$  for all  $r$ .

From **C2** we know that  $d_{2r}$  is divisible by  $d_r' = 2d_r$  when  $d_r$  is even. So

$$(X - u_D^{2r})(X - u_D^{-2r}) = X^2 - (d_{2r} - 1)X + 1 \equiv X^2 + X + 1 \pmod{2d_r}$$

and then by multiplying by  $(X - 1)$  once again it follows that  $u_D^{6r} \equiv 1 \pmod{d_r'}$  when  $d_r$  is even.

It remains to show that this power  $3r \frac{d_r'}{d_r}$  is minimal in each case. We first show that  $3r$  is minimal modulo  $d_r$  for all  $r$ . Let  $q \in \mathbb{N}$  be minimal such that  $u_D^q \equiv 1 \pmod{d_r}$ . It is easy to see that  $q \mid 3r$ . Now the minimal polynomial of  $u_D^q$  is  $X^2 - (d_q - 1)X + 1$ , so this must vanish modulo  $d_r$  at  $X = 1$ . In other words  $d_r$  divides into  $d_q - 3$ , proving that  $r < q$  since  $(d_j)_{j \geq 1}$  is a strictly increasing sequence. So  $3 \mid q$ , since otherwise  $q \mid 3r \implies q \mid r \implies q \leq r$ . Writing  $q = 3q_0$  we see that  $q_0 \mid r$  and so  $q_0 \leq r < 3q_0 = q$ . This forces  $q_0 = r$  or  $q_0 = r/2$ . If  $r$  is odd we are done. If  $r$  is even it follows from (10), (18) that  $u_D^{-\frac{r}{2}}(u_D^{2r} + u_D^r + 1) \equiv 0 \pmod{d_r}$ , implying  $u_D^{\frac{3r}{2}} \equiv 1 - d_{\frac{r}{2}} \pmod{d_r}$ , and clearly  $d_{\frac{r}{2}} \not\equiv 0 \pmod{d_r}$ .

Finally assume that  $d_r$  is even and let  $q' \in \mathbb{N}$  be the minimal integer such that  $u_D^{q'} \equiv 1 \pmod{d_r' = 2d_r}$ . Again we must have  $q' \mid 6r$ ; moreover  $q' < 3r$  would (by reduction modulo  $d_r$ ) contradict the proof above for  $d_r$ . So either  $q' = 3r$  or  $q' = 6r$ . Using (10), (18) as above  $u_D^{3r} \equiv 1 - d_r \pmod{d_{2r}}$ ,  $d_r \not\equiv 0 \pmod{2d_r}$  and the proof is complete again observing that  $d_r$  even  $\implies 2d_r \mid d_{2r}$ .  $\square$

## 5. LINKING UNITARY GEOMETRY AND ARITHMETIC VIA SUBGROUPS OF $\mathrm{GL}_2(\mathbb{Z}/d'\mathbb{Z})$

Let  $\mathbf{v}$  be a fiducial vector taken from one of the orbits in the list (6) that is *centred* as in §2.3, and let  $\{(F, (0, 0)) : F \in \mathbf{S}_0\}$  be the preimage of the stabilizer group of the corresponding projector under the canonical homomorphism. This section and the next is devoted to a study of the  $d' \times d'$ -matrix

$$\mathcal{J} = \left[ \frac{(\mathbf{v}, \Delta_{\mathbf{j}} \mathbf{v})}{(\mathbf{v}, \mathbf{v})} \right]_{\mathbf{j} \in (\mathbb{Z}/d'\mathbb{Z})^2}$$

where the  $\Delta_{\mathbf{j}}$  are the operators defined in (8). Unlike the components of the fiducial vector the matrix  $\mathcal{J}$  is independent of both the scaling and the basis. It follows from Proposition 1 and Definition 1 that the elements of  $\mathcal{J}$  for which  $\mathbf{j} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{d}$  are all elements of  $\mathfrak{R}$  with modulus  $\frac{1}{\sqrt{d+1}}$ . In fact we have found empirically that the field  $\mathbb{Q}(\mathcal{J})$  obtained by adjoining to  $\mathbb{Q}$  all of the elements of  $\mathcal{J}$  is equal to  $\mathfrak{R}_1$  except for orbits  $6a, 9ab, 12b, 24c$ , where it equals  $\mathfrak{R}$ . In particular it is always abelian over  $K$ .

Now let  $L$  be the minimal field of definition for  $\mathcal{J}$ . That is to say  $\mathcal{J}$  splits into closed orbits under the action of  $\mathrm{Gal}(\mathbb{Q}(\mathcal{J})/L)$  and  $L$  is the smallest field for which this is true. In all of our examples in fact  $L = K$  unless the  $\mathrm{Gal}(\mathbb{Q}(\mathcal{J})/K)$ -orbit contains sets  $\mathcal{J}, \mathcal{J}', \dots$  corresponding to more than one Clifford orbit [2, §7]: see the remark at the end of this section.

So  $\mathrm{Gal}(\mathbb{Q}(\mathcal{J})/L)$  acts on  $\mathcal{J}$  in the natural way. At the end of section 2.2 we saw that  $\mathrm{GL}_2(\mathbb{Z}/d'\mathbb{Z})$  can also be made to act naturally upon  $\mathcal{J}$ , by permuting the index vectors  $\mathbf{j}$ . Define

$$\mathbf{S} = \{(\det F)F : F \in \mathbf{S}_0\}$$

As shown in [2],  $\mathbf{S}$  is the subgroup of  $\mathrm{ESp}_2(\mathbb{Z}/d'\mathbb{Z})$  consisting of all matrices which fix  $\mathcal{J}$  *pointwise*. Let  $\mathbf{C}(\mathbf{S})$  be the centralizer of  $\mathbf{S}$  inside  $\mathrm{GL}_2(\mathbb{Z}/d'\mathbb{Z})$ .

What follows is a tantalizing observation linking these two distinct actions upon  $\mathcal{J}$ . It is a strengthening of a statement in §7 of [2].

**Proposition 6.** *For all dimensions in (1)  $L$  is the Hilbert class field of  $K$ , and<sup>3</sup>*

$$(19) \quad \mathbf{C}(\mathbf{S})/\mathbf{S} \cong \text{Gal}(\mathfrak{R}_1/L). \quad \square$$

We are grateful to John Coates for the following observation, which we hope to address in a forthcoming paper.

**Remark.** The appearance of the Hilbert class field in (19) is not a coincidence. The LHS is ostensibly a geometrically defined abelian subgroup of  $\text{GL}_2(\mathbb{Z}/d'\mathbb{Z})$ . On the other hand the RHS contains information about a subgroup of a ray class group, and therefore also potentially about the ideal class group  $\mathcal{C}_K$  of  $K$ . But this cannot be true in general, since the structure of  $\mathcal{C}_K$  is very erratic as  $D$  varies. We can therefore be confident that  $L$  will typically contain the Hilbert class field.

Our empirical observations suggest that  $L$  may be identical with the Hilbert class field in all dimensions, not just those in (1). It follows that the  $\text{Gal}(L/K)$ -set of distinct Clifford orbits may actually be a  $\mathcal{C}_K$ -set. Preliminary numerical results communicated to us by Andrew Scott for certain higher dimensions, wherein  $\mathcal{C}_K$  is much larger than for the dimensions in (1), provide additional evidence for this speculation.

## 6. CANONICAL UNITS ASSOCIATED TO THE RAY CLASS FIELDS

We now proceed to link invariants of the geometric objects with canonical units associated to the ray class fields. The condition of equiangularity means that the inner products in  $\mathcal{J}$  for which  $\mathbf{j} \neq \binom{0}{0} \pmod{d}$  are all of the form  $e^{i\theta(\mathbf{j})}/\sqrt{d+1}$  where the  $\theta(\mathbf{j})$  are real numbers. We shall simply refer to these numbers  $e^{i\theta(\mathbf{j})}$  as *normalized inner products*. Remarkably, in every case examined they are all units in the field  $\mathfrak{R}(\sqrt{d+1})$ .

In some cases the normalized inner products are in  $\mathfrak{R}$ , or even  $\mathfrak{R}_1$ . It is therefore useful to understand the relationship between  $\sqrt{d+1}$  and the ray class fields. Recall that  $D$  is defined to be the square-free part of  $(d+1)(d-3)$ , where  $d \geq 4$  is the ambient dimension of the Hilbert space containing the equiangular lines. From this definition it follows that  $K = \mathbb{Q}(\sqrt{D})/\mathbb{Q}$  always has degree 2 and  $\sqrt{d+1} \in K$  if and only if either  $(d+1)$  or  $(d-3)$  is a square in  $\mathbb{Z}$ .

Suppose that  $\sqrt{d+1} \notin K$ . Let  $p$  be an *odd* prime dividing  $(d+1)$  to an *odd* power. In particular  $p \nmid (d-3)$ , so the biquadratic extension  $K(\sqrt{d+1})$  contains three distinct quadratic subextensions  $K$ ,  $\mathbb{Q}(\sqrt{d+1})$  and  $\mathbb{Q}(\sqrt{d-3})$ : and  $p$  only ramifies in the first two of these. So  $K(\sqrt{d+1})/K$  is unramified above every odd  $p$  and therefore being a totally real quadratic extension it can only ramify at the primes of  $K$  above 2.

When  $d$  is odd, the finite part  $d'$  of the modulus of the ray class field is not divisible by 2. Thus the only *odd* values of  $d$  for which  $\sqrt{d+1}$  can possibly lie in the ray class field  $\mathfrak{R}_0$ , other than when  $\sqrt{d+1} \in K$ , are those where 2 does *not* ramify in the extension  $K(\sqrt{d+1})/K$ . Of course this forces the class number of  $K$  to be  $\geq 2$ , since there is no ramification but it is nevertheless a non-trivial abelian extension, by construction.

On the other hand, if  $d$  is even then  $(d+1)$  is a product of odd primes and so once again adjoining  $\sqrt{d+1}$  to  $K$  produces a totally real abelian extension unramified outside  $d'$ , since by definition  $\gcd(d', d+1) = 1$ . We must further show that the power of 2 dividing the conductor of  $K(\sqrt{d+1})/K$  is less than that dividing  $d'$ . But the former is at most  $2^2$ , and the latter is at least  $2^2$ , so we are done. So  $\sqrt{d+1} \in \mathfrak{R}_0$  for all even values of  $d$ .

For the dimensions in list (1), we calculate that  $\sqrt{d+1} \in \mathfrak{R}_0$  except for  $d = 5, 9, 11, 13, 17$ . By adjoining  $\sqrt{2}$  to the field  $\mathfrak{R}$  in each of these dimensions we obtain an abelian extension of  $K$ , being the compositum of the abelian extensions  $K(\sqrt{2})/K$  and  $\mathfrak{R}_0/K$ .

**Definition 3.** *Let  $\mathcal{S}$  denote the field  $\mathbb{Q}(\mathcal{J}, \sqrt{d+1})$ .*

**Remark.**  $\mathcal{S}$  is defined so as to contain all of the normalized inner products. From the discussions above we observe that  $\mathcal{S} = \mathfrak{R}_1$  for minimal fiducial vectors in every dimension in (1) except for  $d = 6, 12, 24$  where it is equal to  $\mathfrak{R}$ ;  $d = 5, 11, 13, 17$  where  $\mathcal{S} = \mathfrak{R}_1(\sqrt{2})$ ; and finally  $d = 9$  where  $\mathcal{S} = \mathfrak{R}(\sqrt{2})$ .

We can now formalise the claim at the beginning of this section.

**Proposition 7.** *For all dimensions in (1), the normalized inner products are all units in the ring of integers of  $\mathcal{S}$ .*  $\square$

<sup>3</sup> Formula (19) needs to be modified slightly in certain dimensions not in (1); more will be said on this when exact solutions for these dimensions are published. See the end of §7 of [2].

For a given  $EC(d)$ -orbit, choose  $u_d$  to be some fixed overlap phase of maximal degree over  $\mathbb{Q}$ .

**Proposition 8.** *For all dimensions in (1),  $u_d$  generates  $\mathcal{S}$  over  $K(\sqrt{d+1})$  except in orbit 12b where we also need to adjoin  $\sqrt{-1}$ .  $\square$*

**Remark.** Note that for the minimal vectors in  $d = 4, 7, 8, 10, 14, 15, 16, 18, 19, 20, 28, 35$  and 48 this just means that  $K(u_d) = \mathfrak{R}_1$ . Similarly for  $d = 6, 12$  and 24 we have  $K(u_d) = \mathfrak{R}$ .

While the actual units can be calculated from the set of inner products using the fiducial vectors in [2] and Definition 1, most of the minimal polynomials are too cumbersome to include in this short note. However in Appendix A we give a worked example for the case  $d = 19$ .

Now let  $f_d(x)$  be the minimal polynomial of  $u_d$  over  $K$  of degree  $n_d = [\mathcal{S} : K]$ .

**Proposition 9.** *With notation as above, for all dimensions in (1):*

- (i) *all of the  $n_d$  different  $\text{Gal}(\mathcal{S}/K)$ -conjugates of  $u_d$  lie on the unit circle  $U(1)$ .*
- (ii)  *$f_d(x)$  is a reciprocal polynomial: that is,  $x^{n_d} f_d(\frac{1}{x}) = f_d(x)$ .*

*Proof.* Let  $\sigma_c \in \text{Gal}(\mathcal{S}/K)$  be the unique element which acts as complex conjugation. Notice that as  $u_d$  lies on the unit circle,  $\sigma_c(u_d) = u_d^{-1}$ . So for any  $g$  in the abelian group  $\text{Gal}(\mathcal{S}/K)$ :

$$\sigma_c(g(u_d)) = g(\sigma_c(u_d)) = g(u_d^{-1}) = (g(u_d))^{-1}.$$

Thus  $g(u_d)$  also lies on the unit circle, proving (i). To prove (ii), if  $u \neq \pm 1$  is any complex unimodular root of  $f_d$ , the fact that  $f_d$  has totally real coefficients means  $u^{-1}$  is also a (distinct) root. So  $f_d$  is a product of reciprocal polynomials of the form  $x^2 - (u + u^{-1})x + 1$ , hence is itself reciprocal.  $\square$

For more on the Galois theory of fields generated by reciprocal polynomials see Theorem 2 of [12].

The final result of this paper is striking but the size of the necessary calculations has prevented us from testing dimensions 16–18 and 20 in list (1). Furthermore, in order to make the calculations tractable we have used a trick which reduces the degree of the field one needs to consider in dimensions divisible by 3. Specifically, let  $d$  be any dimension in list (1) which is divisible by 3, and let  $\omega$  be a primitive cube root of unity. Then it is an empirically observed fact that if  $u$  is any overlap phase for a minimal fiducial in dimension  $d$ , there exists an integer  $\epsilon \in \{0, 1, 2\}$  such that  $\hat{u} = \omega^\epsilon u \in \mathfrak{R}_1(\sqrt{d+1})$ . Otherwise, if  $u$  is an overlap phase for a minimal fiducial in a dimension not divisible by 3, we define  $\hat{u} = u$ . It will be seen that, with these definitions, the renormalized inner products  $\hat{u}$  are in  $\mathfrak{R}_1(\sqrt{d+1})$  for every minimal fiducial in every dimension in list (1).

Now let  $\mathbb{U}$  denote the group of units of the ring of integers of the field  $\mathfrak{R}_1(\sqrt{d+1})$  under any one of its complex embeddings, and let  $\mathbb{V}$  be the subgroup generated by the renormalized inner products. By construction  $\mathbb{V}$  is contained in the unit circle subgroup  $\mathbb{U} \cap U(1)$  of  $\mathbb{U}$ . It is natural to ask, what are the relative ranks of  $\mathbb{V}$  and  $\mathbb{U} \cap U(1)$ . Let  $\hat{n}_d = [\mathfrak{R}_1(\sqrt{d+1}) : K]$ . From Proposition 4 we know that  $\mathfrak{R}_1(\sqrt{d+1})$  has  $\hat{n}_d$  real places and  $\frac{\hat{n}_d}{2}$  pairs of complex places; so by Dirichlet's unit theorem  $\mathbb{U}$  is an abelian group of rank  $\frac{3\hat{n}_d}{2} - 1$ . By the same Proposition  $\mathfrak{R}_0(\sqrt{d+1})$  is the maximal real subfield of  $\mathfrak{R}_1(\sqrt{d+1})$  and has index 2: so it is a consequence of the lemma in §5 of [16] that the unit circle subgroup  $\mathbb{U} \cap U(1)$  of  $\mathbb{U}$  has  $\mathbb{Z}$ -rank  $\frac{\hat{n}_d}{2}$ .

**Proposition 10.** *In dimensions 7, 15, 19, 35*

$$\text{rank}(\mathbb{V}) = \text{rank}(\mathbb{U} \cap U(1)),$$

*while in dimensions 4–6, 8–14, 24, 28, 48*

$$\text{rank}(\mathbb{V}) = \frac{1}{2} \text{rank}(\mathbb{U} \cap U(1)).$$

*In dimensions 4–8, 12 and 19, where we have been able to calculate  $\mathbb{U}$ ,  $\mathbb{V}$  is a direct summand of  $\mathbb{U} \cap U(1)$ . In particular,  $\mathbb{U} = \mathbb{U} \cap U(1)$  in dimensions 7 and 19.  $\square$*

Finally, let  $\hat{u}_d$  be the renormalized version of the unit  $u_d$  defined above. Then

**Proposition 11.** *In dimensions 4–15, 19, 24, 35, 48 the group  $\mathbb{V}$  is generated by the  $\text{Gal}(\mathfrak{R}_1(\sqrt{d+1})/K)$ -orbit of  $\hat{u}_d$ .  $\square$*

## 7. VERIFICATION OF PROPOSITION 1

In this final section we give a very cursory outline of the steps necessary in verifying the claim for each dimension in Proposition 1. Let  $d$  be one of the dimensions in (1) and let  $D$  be the square-free part of  $(d-1)^2 - 4$ . As usual  $K$  will denote  $\mathbb{Q}(\sqrt{D})$ . For each orbit in the list (6), choose a fiducial vector  $\mathbf{v}$ ; these may be found in [2] and [3]. Choose a distinguished basis and fix the representation for  $\mathcal{H}(d)$ . This defines a SIC  $E$  with a fiducial projector  $\Pi$  corresponding to  $\mathbf{v}$ .

Let  $S(E)$  be the set of all matrix elements of the projectors in  $E$  in the distinguished basis. As in the Introduction, write  $K(E)$  for  $K(S(E))$ . Then we need to check that:

- $[K(E) : K] = [\mathfrak{R} : K]$ ; and
- the defining polynomials for  $\mathfrak{R}$  factorize completely over  $K(E)$ .

The degrees of the field extensions may be deduced from the explicit generators in [2, 3]. The verification that these equal the orders of the appropriate ray class groups was done in MAGMA [4]. Similarly, MAGMA was used first to find the generating polynomials for  $\mathfrak{R}$  and then subsequently to prove that they do indeed factor over the respective field extensions  $K(E)$ . This completes the verification of Proposition 1.  $\square$

We illustrate these calculations for  $d = 19$  in Appendix A.

**Acknowledgements.** It is a pleasure to thank John Coates and Andrew Scott for their continuing support and guidance. Also thanks to Steve Donnelly for his help with the MAGMA code and with interpreting the number-theoretic results. Finally, we are grateful to James McKee and Chris Smyth for explaining various aspects of the theory of reciprocal units, and Brian Conrad for comments on an earlier draft.

This research was supported by the Australian Research Council via EQuS project number CE11001013, and SF acknowledges support from an Australian Research Council Future Fellowship FT130101744 and JY from National Science Foundation Grant No. 116143.

## REFERENCES

- [1] D. M. Appleby, *Symmetric Informationally Complete Positive Operator Valued Measures and the Extended Clifford Group*, J. Math. Phys. **46**, 052107 (2005).
- [2] D. M. Appleby, H. Yadsan-Appleby and G. Zauner, *Galois Automorphisms of a Symmetric Measurement*, Quantum Information & Computation **13**, 672–720 (2013).
- [3] Marcus Appleby, Steven T. Flammia, Tuan-Yow Chien and Shayne Waldron *Systematically Constructing Exact SIC-POVMs from Numerics*, in preparation.
- [4] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24**, 235–265 (1997).
- [5] Carl Caves, personal notes, <http://info.phys.unm.edu/~caves/reports/infopovm.pdf>, (1999).
- [6] Tuan-Yow Chien, *Equiangular lines, projective symmetries and nice error frames*, Doctoral Thesis at the University of Auckland (2015). Available at <https://www.math.auckland.ac.nz/~waldron/Tuan/Thesis.pdf>
- [7] Harvey Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, Universitext, Springer-Verlag NY, second printing (1988).
- [8] P. Delsarte, J. M. Goethals, and J. J. Seidel, *Bounds for systems of lines and Jacobi polynomials*, Philips Res. Rep. **30**, 91 (1975).
- [9] D. M. Appleby, S. T. Flammia, and C. A. Fuchs, *The Lie Algebraic Significance of Symmetric Informationally Complete Measurements*, J. Math. Phys. **52**, 022202 (2011).
- [10] Stuart G. Hoggar, *64 lines from a quaternionic polytope*, Geom. Dedicata **69** (3), 287–289 (1998).
- [11] Lane P. Hughston and Simon M. Salamon, *Surveying points in the complex projective plane*, Advances in Mathematics **286**, 1017 (2016).
- [12] Franck Lalonde, *Corps de nombres engendr es par un nombre de Salem*, Acta Arithmetica LXXXVIII.2, 191–200 (1999).
- [13] Serge Lang, *Algebraic Number Theory*, GTM **110**, Springer-Verlag New York (1986).
- [14] P. W. H. Lemmens and J. J. Seidel, *Equiangular Lines*, Journal of Algebra **24**, 494–512 (1973).
- [15] David Mumford (with Madhav Nori and Peter Norman), *Tata Lectures on Theta III*, Modern Birkh user Classics, Birkh user reprint of the 1991 original (2007).
- [16] Noboru Nakahata, *On Units of Galois Extensions over  $\mathbb{Q}$* , Proceedings of the Faculty of Science of Tokai University **15**, 23–27 (1980).
- [17] J. M. Renes, R. Blume-Kohout, A. J. Scott and C. M. Caves, *Symmetric Informationally Complete Quantum Measurements*, J. Math. Phys. **45**, 2171–2180 (2004).
- [18] Sage Mathematics Software (Version 7.0), The Sage Developers, 2016, <http://www.sagemath.org>.
- [19] K. Scharnhorst, *Angles in Complex Vector Spaces*, Acta Applicandae Mathematicae **69**, 95–103 (2001).
- [20] A. J. Scott and M. Grassl, *SIC-POVMs: A New Computer Study*, J. Math. Phys. **51**, 042203 (2010).
- [21] Andrew Scott, *private communication*, (2015).

- [22] Goro Shimura and Yutaka Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publications of the Mathematical Society of Japan, **6** The Mathematical Society of Japan, Tokyo (1961).
- [23] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences, *Maximal size of a set of equiangular lines in  $n$  dimensions*, published electronically at <http://oeis.org/A002853>.
- [24] Eugene Wigner, *Group theory, and its Application to the Quantum Mechanics of Atomic Spectra*, Academic Press, (1959).
- [25] G. Zauner, *Quantendesigns. Grundzüge einer nichtkommutativen Designtheorie*, PhD thesis, University of Vienna (1999). English translation: *Quantum Designs: Foundations of a Non-Commutative Design Theory*, Int. J. Quantum Inf. **9**, 445–507 (2011).
- [26] Gerhard Zauner personal website, <http://www.gerhardzauner.at/sicfiducials.html>.
- [27] Huangjun Zhu, *SIC POVMs and Clifford groups in prime dimensions*, J. Phys. A: Math. Theor. **43** (2010).

#### APPENDIX A. EXAMPLE OF A UNIT GENERATOR FOR $\mathfrak{R}_1 : \mathbb{Q}(\sqrt{D})$ IN DIMENSION 19

We illustrate the foregoing for the case  $d = 19$ . The associated value of  $D$  is 5 and clearly  $\sqrt{d+1} \in K = \mathbb{Q}(\sqrt{5})$ . There are  $19 \times 18$  values of inner products which upon normalisation yield a set of 21 units falling into three Galois orbits, as expressed by their minimal polynomials:

$$f_1(y) = y - 1, \quad f_2(y) = y^2 + \frac{1}{2}(\sqrt{5} - 5)y + 1,$$

$$\begin{aligned} f_3(y) = & y^{18} + \frac{1}{2}(5\sqrt{5} - 5)y^{17} + (5\sqrt{5} - 6)y^{16} + (-57\sqrt{5} + 134)y^{15} + (41\sqrt{5} - 83)y^{14} \\ & + \frac{1}{2}(1031\sqrt{5} - 2285)y^{13} + (-445\sqrt{5} + 1004)y^{12} + (-2130\sqrt{5} + 4769)y^{11} \\ & + \frac{1}{2}(1757\sqrt{5} - 3917)y^{10} + (4297\sqrt{5} - 9602)y^9 + \frac{1}{2}(1757\sqrt{5} - 3917)y^8 \\ & + (-2130\sqrt{5} + 4769)y^7 + (-445\sqrt{5} + 1004)y^6 + \frac{1}{2}(1031\sqrt{5} - 2285)y^5 \\ & + (41\sqrt{5} - 83)y^4 + (-57\sqrt{5} + 134)y^3 + (5\sqrt{5} - 6)y^2 + \frac{1}{2}(5\sqrt{5} - 5)y + 1. \end{aligned}$$

The polynomials  $f_2, f_3$  illustrate the *reciprocal* property referred to above.

All three polynomials split inside the field  $\mathbb{Z}_K[y]/(f_3(y))$ . Separately, the defining polynomials for  $\mathfrak{R}_1$  over  $\mathbb{Q}(\sqrt{5})$  are  $y^2 + 2\sqrt{5} + 1$  and

$$\begin{aligned} y^9 - 9747y^7 + 136458y^6 + 25001055y^5 - 320013504y^4 - 24511034322y^3 \\ + 97474113234y^2 + 9503726040315y + 66721030508673. \end{aligned}$$

These generate abelian extensions of degree 2 and 9 respectively and so together generate a Galois extension of degree 18, as expected. So it remains to check that they split over the field  $\mathbb{Z}_K[y]/(f_3(y))$ , which is straightforward using a program like MAGMA [4] or Sage [18].

Write  $t = \cos \frac{\pi}{19}$ . An example of one of the roots of  $f_3$  is

$$\begin{aligned} \frac{i}{19} \left[ (-192\sqrt{5} + 704)t^7 + (48\sqrt{5} - 176)t^6 + (312\sqrt{5} - 1144)t^5 + (-28\sqrt{5} + 204)t^4 \right. \\ \left. + (-150\sqrt{5} + 550)t^3 + (-14\sqrt{5} - 50)t^2 + (21\sqrt{5} - 77)t + (4\sqrt{5} - 2) \right] \sqrt{2\sqrt{5} + 1} \\ + (16\sqrt{5} - 16)t^6 + (-8\sqrt{5} + 8)t^5 + (-20\sqrt{5} + 20)t^4 + (10\sqrt{5} - 10)t^3 \\ + (6\sqrt{5} - 6)t^2 + (-3\sqrt{5} + 3)t + \frac{1}{2}(-\sqrt{5} + 1). \end{aligned}$$

This unit generates  $\mathfrak{R}_1/K$ . Together with its  $\text{Gal}(\mathfrak{R}_1/K)$ -conjugates it generates a subgroup of the unit group  $\mathbb{U}(\mathfrak{R}_1)$  of rank  $\frac{19-1}{2} = 9$ , which is also the rank of the subgroup  $\mathbb{U}(\mathfrak{R}_1) \cap \mathbb{U}(1)$  consisting of all units of  $\mathfrak{R}_1$  of modulus 1 [16, §5].

#### APPENDIX B. BACKGROUND AND HISTORY OF THE PROBLEM

In the early 1970's Lemmens and Seidel [14] considered the question of how large a set of *equiangular lines* one could find in Euclidean real space. That is to say, a set of lines in  $\mathbb{R}^d$  such that any pair of lines subtends a constant angle  $\alpha$ .

As an example consider  $\mathbb{R}^2$ , where the three axes joining pairs of opposite vertices of a hexagon are a maximal set of such lines; or  $\mathbb{R}^3$  where a maximal set is given by the six axes joining opposite

pairs of vertices of an icosahedron. The current state of knowledge is given at [23], but it is striking that beyond the few algebraic solutions and some strong bounds in low dimensions, little is known.

In this *real* Euclidean setting the problem seems quintessentially combinatorial. Indeed although it is perhaps most easily stated as a geometric problem, the techniques applied to its solution all reduce to discrete mathematics. Loosely speaking, this seems to be because the notion of *angle* is only ambiguous up to the units  $\{\pm 1\}$ .

However in *complex* Euclidean space  $\mathbb{C}^d$  equipped with the usual hermitian inner product  $(\cdot, \cdot)$ , the notion of *angle* has a degree of freedom corresponding to the full unit circle  $U(1)$  rather than just  $\{\pm 1\}$ . We take our definition of angle from (4) of [19] so that if  $\mathbf{u}, \mathbf{v}$  are two complex unit vectors generating the lines, then we may write  $(\mathbf{u}, \mathbf{v}) = \rho e^{i\phi}$  for some  $0 \leq \rho \leq 1$  and  $0 \leq \phi < 2\pi$ . The inverse cosine of  $\rho$  is the *hermitian angle* between the two lines spanned by  $\mathbf{u}$  and  $\mathbf{v}$ ; while the argument  $\phi$  is referred to as the *pseudo-angle* between the vectors.

Complete sets of complex equiangular lines are called SICPOVMs or just SICs (pronounced “seeks”) in the quantum information literature, and one can show [8] that any set of pairwise equiangular complex lines in  $\mathbb{C}^d$  has at most  $d^2$  elements, with the common hermitian angle for a complete set being  $\cos^{-1}(\frac{1}{\sqrt{d+1}})$ . Owing to this upper bound if a complete equiangular set exists then it is also maximal.

Zauner [25], and independently Caves [5], seem to have been the first to posit the existence of complete structures of this sort in any dimension. In Zauner’s thesis he set out solutions to his conjecture for dimensions 2,3,4,5,6,7, some of which were algebraic and some of which were numerical. Independently, in [17] the authors devised a numerical search algorithm to find complete  $\mathcal{H}(d)$ -sets of complex equiangular lines for low values of  $d$ . By building the  $\mathcal{H}(d)$  symmetry into the numerical search, the problem was transformed from the initial  $O(d^4)$  equations in  $O(d^3)$  variables down to just  $O(d^2)$  equations in  $O(d)$  variables. This made it tractable in low dimensions [17, 20, 21]. In addition the searches were guided by a remarkable intuition of Zauner’s [25] placing the putative vectors within an eigenspace of a certain unitary matrix [20, Conjecture 3.1].

This method did indeed yield many numerical approximations to solutions for dimensions  $d \leq 45$  [17]; it was subsequently extended to  $d \leq 67$  [20]. Scott [21] has since extended the set of approximations to

$$d = 1, 2, 3, \dots, 121; 124; 143; 147; 168; 172; 195; 199; 323;$$

though we should stress that at this stage these are almost all still just high-precision numerical solutions. By an exhaustive numerical search, Scott and Grassl [20] have likely found every orbit for  $d \leq 50$ . A necessary and sufficient condition for unitary equivalence of orbits is given in [9, Thm. 3].

However in many cases the numerical approximations in [17] have been converted into algebraic solutions [20, 2, 6, 3]: indeed these were used in the main part of this paper. All currently known published algebraic solutions appear in [20] and [6]; however more solutions have actually been calculated and some of these will be published shortly [3]. In brief, the dimensions  $d$  for which algebraic solutions have been published are:

$$d = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18^*, 19, 20^*, 24, 28, 35, 48,$$

where an asterisk refers to [3].

The observation that in every dimension apart from  $d = 3$  the numbers  $\gamma_d$  are expressible in radicals led the authors of [2] to make a more detailed study of the Galois groups first calculated in [20]. Their most relevant observation for the present purposes is that the fields (for  $d \geq 4$ ) of the known solutions are abelian extensions of  $\mathbb{Q}(\sqrt{D})$ . They also established a number of other results, including a weaker version of Proposition 6 of the present paper. Conjecture 1 in this paper follows this trajectory, and substantially strengthens the conjectures in [2].

CENTRE FOR ENGINEERED QUANTUM SYSTEMS, SCHOOL OF PHYSICS, UNIVERSITY OF SYDNEY  
*E-mail address:* `marcus.appleby@sydney.edu.au`

CENTRE FOR ENGINEERED QUANTUM SYSTEMS, SCHOOL OF PHYSICS, UNIVERSITY OF SYDNEY  
*E-mail address:* `steven.flammia@sydney.edu.au`

CONTROLLED QUANTUM DYNAMICS THEORY GROUP, IMPERIAL COLLEGE, LONDON  
*E-mail address:* `g.mcconnell@imperial.ac.uk`

QUANTUM ARCHITECTURES AND COMPUTATION GROUP, MICROSOFT RESEARCH  
*E-mail address:* `jonyard@microsoft.com`