CONSTRUCTING EXACT SYMMETRIC INFORMATIONALLY COMPLETE MEASUREMENTS FROM NUMERICAL SOLUTIONS

*MARCUS APPLEBY, †TUAN-YOW CHIEN, *,‡STEVEN FLAMMIA, AND †SHAYNE WALDRON

Abstract. Recently, several intriguing conjectures have been proposed connecting symmetric informationally complete quantum measurements (SIC POVMs, or SICs) and algebraic number theory. These conjectures relate the SICs and their minimal defining algebraic number field. Testing or sharpening these conjectures requires that the SICs are expressed exactly, rather than as numerical approximations. While many exact solutions of SICs have been constructed previously using Gröbner bases, this method has probably been taken as far as is possible with current computer technology. Here we describe a method for converting high-precision numerical solutions into exact ones using an integer relation algorithm in conjunction with the Galois symmetries of a SIC. Using this method we have calculated 69 new exact solutions, including 9 new dimensions where previously only numerical solutions were known, which more than triples the number of known exact solutions. In some cases the solutions require number fields with degrees as high as 12,288. We use these solutions to confirm that they obey the number-theoretic conjectures and we address two questions suggested by the previous work.

1. Introduction

Symmetric informationally complete quantum measurements (SIC POVMs as they are often called, or SICs as we will call them in this paper) are collections of d^2 equiangular lines in in a d-dimensional complex vector space. They were originally introduced by Zauner [1] and Renes *et al* [2], and they have many applications to quantum information [3–9], as well as playing a central role in the QBist approach to the interpretation of quantum mechanics [10]. They also have applications to classical signal processing [11,12]. SICs have been calculated numerically [13–15] in every dimension up to 151, and for a handful of other dimensions up to 323. Exact solutions [13] have been calculated in dimensions 2–16, 19, 24, 28, 35, 48. This encourages the conjecture that SICs exist in every finite dimension, but a proof continues to elude us. The SICs in dimensions 2 and 3, together with the Hoggar lines [16] in dimension 8, are sometimes called sporadic SICs, on the grounds that they have a number of special properties [17,18]. In this paper we exclude them from consideration. In the following the term "SIC" will therefore always mean "non-sporadic SIC". In particular, we will always assume without comment that the dimension is greater than 3.

We will describe a method for converting numerical SICs into exact ones. The method relies on, and is motivated by some recently discovered connections between SICs and algebraic number theory [19, 20]. Dimension 3 excepted, the standard-basis matrix elements of every known exact fiducial projector are algebraic numbers. More than that, they are expressible in radicals (i.e. the components can be built up from the integers

*Centre for Engineered Quantum Systems, School of Physics, University of Sydney, Sydney, Australia

†Department of Mathematics, University of Auckland, Auckland, New Zealand

‡Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, USA

E-mail addresses: marcus.appleby@sydney.edu.au, tuan@math.auckland.ac.nz, steven.flammia@sydney.edu.au, waldron@math.auckland.ac.nz.

using the standard arithmetical operations together with the operation of taking roots), meaning that the associated Galois group is solvable. It turns out that the number fields they generate have some remarkable properties [21, 22]. We outline the most salient points of this number-theoretic connection here assuming some familiarity with the basic concepts underlying SICs; however, in section 2 below we provide all of the necessary definitions and background.

Let Π be a SIC fiducial projector in dimension $d \geq 4$, and let $\mathbb{E} = \mathbb{Q}(\Pi, \tau)$ be the field generated over the rationals by the standard-basis components of Π together with $\tau = -e^{\frac{\pi i}{d}}$. We refer to $\mathbb{E}$ as the SIC field. It is easily seen that $\mathbb{E}$ only depends on the $\mathrm{EC}(d)$ orbit to which Π belongs (where $\mathrm{EC}(d)$ is the extended Clifford group in dimension d). Let $\mathbb{K} = \mathbb{Q}(\sqrt{D})$ where D is the square-free part of $(d-3)(d+1)$. Then one finds, in every case that has been calculated,

- $\mathbb{Q} \triangleleft \mathbb{K} \triangleleft \mathbb{E}$.
- $\mathbb{Q} \triangleleft \mathbb{E}$.
- The Galois group $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$ is Abelian.

(where the notation $\mathbb{F}_1 \triangleleft \mathbb{F}_2$ means that $\mathbb{F}_2$ is a normal extension of $\mathbb{F}_1$). In each dimension for which the full set of exact SICs has been calculated there is exactly one SIC field of minimal degree; every other SIC field being a low-degree extension of that. In ref. [22] it was shown that, in every known case, the minimal field is a very special kind of field extension: Namely, the ray class field over $\mathbb{K}$ with conductor d' and ramification at both infinite places (where $d' = d$ if d is odd, and $2d$ if d is even).

If SICs existed in every finite dimension, and if the above statements were generally true, it would be a fact of some interest to algebraic number theorists. Ray class fields are used to classify fields having an Abelian Galois group over some given base-field. The Kronecker-Weber theorem states that the ray class fields over $\mathbb{Q}$ are precisely the fields $\mathbb{Q}(\omega)$, where ω is a complex root of unity. Kronecker further conjectured, and it was subsequently proved, that the ray class fields over $\mathbb{Q}(i\sqrt{n})$, for n a positive integer, are generated by the coordinates of certain distinguished points on an elliptic curve. Hilbert's 12^{th} problem, still unsolved, asks for the generalization of these results; the obvious place to start being ray class fields over $\mathbb{Q}(\sqrt{n})$, for n a positive integer—i.e., fields of precisely the kind that SICs generate (in the handful of cases we have been able to calculate). This does not mean that solving the SIC problem is equivalent to solving Hilbert's 12^{th} problem. In the first place SICs only give us *some* of the ray class fields over a given $\mathbb{Q}(\sqrt{n})$. In the second place a solution to the SIC problem would not necessarily give us the analogues of the exponential and elliptic functions that Hilbert was asking for. Against that, it was shown in ref. [22] that, for each square-free positive integer n, there is an infinite sequence of dimensions for which $D = n$. So although a solution to the SIC problem would not give us the full set of ray class fields over a given $\mathbb{Q}(\sqrt{n})$, it might give us an infinite subset. Moreover, the SIC problem may conceivably reduce to proving a set of special-function identities. If so that would give us the functions Hilbert wanted. In short, it seems fair to say that a constructive solution to the SIC problem might be a significant step in the direction of solving Hilbert's 12^{th} problem for real quadratic fields.

We have stressed the potential relevance of SICs to a major unsolved problem in algebraic number theory. The reverse is also true: the number-theoretic aspects give important insight into SIC geometry, as appears from current work of two of the authors.

For many purposes a high-precision approximate SIC is completely satisfactory. However, if one wants to pursue the connections with number theory exact solutions are essential. Here one faces a problem. Aside from a handful of examples obtained by hand-calculation (or, in the case of dimension 19, guesswork), the exact solutions listed in ref. [13] were obtained by calculating a Gröbner basis. The Gröbner basis method is extremely demanding computationally, and has probably been pushed about as far as it is possible to go without a massive increase in computer speed and memory. We therefore need an alternative method. Fortunately, number theory, besides creating the demand, also supplies the means of satisfying it. That is, one can exploit the conjectured number-theoretic properties of a SIC to bump the high precision approximate SICs in refs [13, 14] up to infinite precision. Success in this enterprise incidentally provides additional evidence in support of the conjectures on which the method is based.

The essential idea is as follows. Suppose one is given a real number a specified to some finite degree of precision, and suppose one knows that a is an approximation to an exact real number a_{e} in a specified algebraic number field $\mathbb{F}$. Let $b_1, \dots, b_n$ be a basis for $\mathbb{F}$ over the rationals. Then $a_{\mathrm{e}} = q_1 b_1 + \cdots + q_n b_n$ for some set of rational numbers q_j. Multiplying through by the LCM of the q_j we deduce

$$m_0 a - \sum_{j=1}^{n} m_j b_j \approx 0 \tag{1}$$

for some set of integers $m_0, m_1, \dots m_n$. If we can calculate the m_j we will have managed to find an exact number which a approximates. With high enough precision and computational power, these particular integers m_j will satisfy $q_j = m_j/m_0$, and we will have recovered a_{e}, the specific exact number we're after. This procedure can be done using an integer-relation algorithm [23], such as the PSLQ algorithm [24].

A few remarks are in order. In the first place, there are infinitely many sequences m_j satisfying Eq. (1) to the specified degree of accuracy, and there is no guarantee that the algorithm will return the one we want. Basically, the algorithm is a systematic guessing procedure. However, for our purposes that is good enough, since we can verify the guess (by checking that the final result really is an exact SIC fiducial).

In the second place, one does not expect to get more information out than one initially puts in. Suppose a is given to r digits of precision. Then if one does not want to generate spurious results one needs r to be larger than a number $\sim s(n+1)$, where s is the maximum number of digits in the integers m_j. In practice [23] one needs r to be 10–15% larger than $s(n+1)$. The problem is, of course, that one does not initially know s. As a practical rule of thumb we therefore proceed by repeatedly running the algorithm at successively higher levels of precision until the result is stable. Again, the justification for this procedure is the fact that the end result demonstrably is an exact SIC fiducial.

In the third place, there is the problem that we do not always know the field $\mathbb{F}$. As discussed above, we have a conjecture regarding the minimal SIC field in each dimension. However, many fiducials lie in an extension of this field for which we currently have no conjecture. A further problem is that in the cases of interest the SIC field is often of degree 10^3 or more. For the reasons discussed above this means that we need to work to very high precision, and the calculations are correspondingly slow. For the calculations in this paper we therefore exploited a conjecture in ref. [21], which implies that the coefficients of suitably chosen polynomials lie in a much smaller field, which is easily inferred from the numerical data, and for which the calculations are much faster.

Scott-Grassl [13] calculate 179 numerical fiducials in dimensions 4–50, and they argue that with high probability their list is complete, in the sense that it includes exactly one representative of every orbit of unitarily equivalent SICs in these dimensions. In addition they calculated a large number of new exact solutions, bringing the total number of known exact solutions (for $d \geq 4$) up to 27. We have calculated exact representatives for a further 69 orbits, and of these orbits we provide a complete analysis for 52 of them. This means that we now have exact representatives for 96 total orbits, more than half of the orbits in dimensions between 4 and 50. We would have liked to calculate exact representatives and provide a complete analysis for every orbit up to dimension 50, but unfortunately our method is not completely automated and is still too time consuming for us to justify this additional effort. In choosing which fiducials to calculate we were guided by two considerations. In the first place the conjectures in ref. [25], as was there noted, cannot be true of the type-a orbits $21e$, $30d$, $39ghij$, $48e$ (where we employ the Scott-Grassl [13] labeling scheme). We have calculated exact representatives of these orbits in order to find modified conjectures which stand a chance of holding for every type-a orbit. In the second place, we noted above that the minimal SIC field in each dimension seems always to be the ray class field over $\mathbb{Q}(\sqrt{D})$ with conductor d'. This raises the question, what can be said of the *non*-minimal fields in each dimension. We therefore set out to find a *complete* set of SICs in each dimension. Thus, Scott and Grassl only give an exact representative for one of the orbits in dimensions 15, 19, 24, 28, 35 and 48. We have found exact representatives for all the other orbits in these dimensions. In particular we have found full sets of exact solutions for dimensions 35 and 39—the two dimensions less than 50 for which the number of distinct orbits is greatest. This information may help us to find a conjecture similar to the ray-class field conjecture applying to the non-minimal SIC fields.

The complete list of dimensions for which we provide exact solutions, and where previously only a numerical solution was known, is $17, 18, 20, 21, 30, 31, 37, 39, 43$. From this list, we have neglected to provide a complete analysis for $31, 37, 43$, although our methods could also be applied there by a sufficiently motivated individual.

The plan of the paper is as follows. Section 2 is devoted to necessary preliminaries. Mostly this material is in refs. [13, 21, 22, 26]. Some of it, however, is new. Section 3 is devoted to the type-a orbits $21e$, $30d$, $39ghij$, $48e$ mentioned in the last paragraph. We show how the conjectures in ref. [21] naturally generalize to these orbits also. Section 4 concerns the relationship between the SIC fields in a given dimension. Scott and Grassl [13] find at most three exact solutions in a given dimension, and no more than two distinct SIC fields. With the new solutions calculated here we now have up to ten exact solutions for a given dimension, and up to seven distinct SIC fields. In section 4 we summarize this information. In section 5 we describe the method used to calculate the new solutions. Finally, in Appendix A we present our results. Many of the fields we calculate are much higher degree[1] than the fields calculated in ref. [13], and this creates some presentational difficulties. For instance the print-out for exact fiducial $48a$ occupies almost a thousand A4 pages (font size 9 and narrow margins). There can therefore be no question of presenting the fiducials themselves in the appendix. Instead we have made the fiducials available online [32], and confined ourselves here to a description of the fields and Galois groups.

2. Preliminaries

The purpose of this section is to fix notation, and to summarize some relevant results from refs. [13, 21, 22, 26]. Let $\mathcal{H}$ be a d-dimensional Hilbert space, and let $|0\rangle, \dots |d-1\rangle$ be the standard basis. Let X, Z by the operators which act according to

$$X|r\rangle = |r+1\rangle, \qquad Z|r\rangle = \omega^r|r\rangle, \tag{2}$$

[1] Calculating with fields this enormous leads to numerous technical difficulties. For instance, we estimated that it would take many months to directly check the irreducibility of the successive polynomials used to define some of the field towers (by trying to factor them in *Magma*), and we therefore had recourse to an indirect argument based on the subfield structure. Again, when calculating with such fields it is essential to devise ways of minimizing the number of distinct arithmetical operations (especially the number of divisions) if one does not want to devote months or even years of CPU time to the task. One also needs to give careful thought to the amount of RAM taken up by some of the intermediate results.

where $\omega = e^{2\pi i/d}$ and addition of indices is *mod d*. For each $\mathbf{p} = \left(\begin{smallmatrix} p_1 \\ p_2 \end{smallmatrix}\right) \in \mathbb{Z}^2$ define the displacement operator

$$D_{\mathbf{p}} = \tau^{p_1 p_2} X^{p_1} Z^{p_2}, \tag{3}$$

where $\tau = -e^{\frac{\pi i}{d}}$. The displacement operators constitute a nice unitary error basis [27,28]. In particular, an arbitrary operator A has the expansion

$$A = \sum_{p_1,p_2=0}^{d-1} A_{\mathbf{p}} D_{\mathbf{p}}, \qquad\qquad A_{\mathbf{p}} = \frac{1}{d}\operatorname{Tr}(D_{\mathbf{p}}^\dagger A). \tag{4}$$

Let $d' = d$ (respectively $d' = 2d$) if d is odd (respectively even), and define the extended symplectic group $\mathrm{ESL}(2, \mathbb{Z}/d'\mathbb{Z})$ to consist of all 2×2 matrices with entries in $\mathbb{Z}/d'\mathbb{Z}$ and determinant ± 1. The symplectic group $\mathrm{SL}(2, \mathbb{Z}/d'\mathbb{Z})$ is the subgroup consisting of matrices with determinant $+1$. For each $F \in \mathrm{ESL}(2, \mathbb{Z}/d'\mathbb{Z})$ there exists an operator U_F on $\mathcal{H}_d$, unique up to an overall phase, such that

$$U_F D_{\mathbf{p}} U_F^\dagger = D_{F\mathbf{p}}. \tag{5}$$

The operator U_F is a unitary if $\operatorname{Det} F = 1$ and an anti-unitary if $\operatorname{Det} F = -1$. We refer to it as a symplectic unitary in the first case and an anti-symplectic anti-unitary in the second. For all $F, G \in \mathrm{ESL}(2, \mathbb{Z}/d'\mathbb{Z})$

$$U_F U_G \doteq U_{FG} \tag{6}$$

where $\doteq$ means "equal up to a phase" (so the map $F \to U_F$ is a projective representation of $\mathrm{ESL}(2, \mathbb{Z}/d'\mathbb{Z})$). The Clifford group $\mathrm{C}(d)$ (respectively extended Clifford group $\mathrm{EC}(d)$) consists of all operators of the form $e^{i\theta} D_{\mathbf{p}} U_F$ with $F \in \mathrm{SL}(2, \mathbb{Z}/d'\mathbb{Z})$ (respectively $F \in \mathrm{ESL}(2, \mathbb{Z}/d'\mathbb{Z})$ and $e^{i\theta}$ an arbitrary phase.

There are [26,29] explicit formulae for the operators U_F. If the symplectic matrix

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{7}$$

is such that $\mathrm{GCD}(\beta, d') = 1$ the associated unitary is given by

$$U_F = \frac{e^{i\theta}}{\sqrt{d}} \sum_{r,s=0}^{d-1} \tau^{\beta^{-1}(\delta r^2 - 2rs + \alpha s^2)} |r\rangle\langle s| \tag{8}$$

where $e^{i\theta}$ is an arbitrary phase, and β^{-1} is the multiplicative inverse of β considered as an element of $\mathbb{Z}/d'\mathbb{Z}$. Matrices in $\mathrm{SL}(2, \mathbb{Z}/d'\mathbb{Z})$ not satisfying the condition $\mathrm{GCD}(\beta, d') = 1$ can always be written as a product of two matrices which do satisfy it. An antisymplectic matrix F can be written as $F'J$ where $F' \in \mathrm{SL}(2, \mathbb{Z}/d'\mathbb{Z})$ and

$$J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{9}$$

The anti-unitary U_J acts by complex conjugation in the standard basis. Using these facts we can calculate U_F for arbitrary $F \in \mathrm{ESL}(2, \mathbb{Z}/d'\mathbb{Z})$. In prime dimensions there are some simplifications [29].

A SIC fiducial projector is a rank-1 projector Π such that

$$\operatorname{Tr}(\Pi D_{\mathbf{p}}) = \begin{cases} 1 & \text{if } \mathbf{p} = \mathbf{0} \mod d \\ \frac{e^{i\theta_{\mathbf{p}}}}{\sqrt{d+1}} & \text{otherwise} \end{cases} \tag{10}$$

for some set of phases $e^{i\theta_{\mathbf{p}}}$. We refer to the quantities $\operatorname{Tr}(\Pi D_{\mathbf{p}})$ as the overlaps, and to the numbers $e^{i\theta_{\mathbf{p}}}$ as the overlap phases. It can be seen from Eq. (4) that the overlap phases completely determine the fiducial. Although it is not needed for the calculations in this paper let us also note that, in every case which has been calculated, the overlap phases are units in the field $\mathbb{E}(\sqrt{d+1})$ generating a subgroup of the full unit group whose properties are studied in ref. [22]. If Π is a SIC fiducial projector then so is $U\Pi U^\dagger$ for every $U \in \mathrm{EC}(d)$. Consequently the fiducial projectors split into a collection of $\mathrm{EC}(d)$ orbits. Scott and Grassl [13] have, with high probability, identified every $\mathrm{EC}(d)$ orbit for $d \leq 50$ and Scott [14] has extended the calculations to higher dimensions. At the time of writing it appears [14] that, apart from $d = 3$, there are only finitely many $\mathrm{EC}(d)$ orbits in each dimension up to $d = 77$.

We define the stability group of a SIC fiducial Π to be the set of all $U \in \mathrm{EC}(d)$ such that $U\Pi U^\dagger = \Pi$. It is a striking fact, so far unexplained, that in every known case the stability group contains a unitary of the form $D_{\mathbf{p}}U_F$, where $\mathrm{Tr}(F) = -1 \mod d$ and $F \neq I$ (if $d \neq 3$ it is enough to impose the first condition as the second is then automatic). Such a unitary is necessarily order 3, up to a phase. We refer to it as canonical order 3.

It is convenient to choose standard canonical order 3 unitaries. If $d \neq 3$ or $6 \mod 9$ every such unitary is conjugate modulo a phase to U_{F_z}, where

$$F_z = \begin{pmatrix} 0 & d-1 \\ d+1 & d-1 \end{pmatrix}. \tag{11}$$

We refer to F_z as the Zauner matrix[2]. If $d = 3$ or $6 \mod 9$ there is an additional conjugacy class when $d > 3$. If $d = 6 \mod 9$ the additional conjugacy class does not give rise to SICs, in any known case. However, if $d = 3 \mod 9$ it does. Following ref. [13] we choose as class representative U_{F_a}, where

$$F_a = \begin{pmatrix} 1 & d+3 \\ \frac{4d-3}{3} & d-2 \end{pmatrix}. \tag{12}$$

We say that an orbit is type-z (respectively type-a) if it contains fiducials stabilized by U_{F_z} (respectively U_{F_a}).

We say that a subgroup of $\mathrm{EC}(d)$ is displacement-free if it consists entirely of operators of the form $e^{i\theta}U_F$, with $F \in \mathrm{ESL}(2, \mathbb{Z}/d'\mathbb{Z})$. Following ref. [22] we shall say that a fiducial is centred if its stability group (a) contains a canonical order 3 unitary, and (b) is displacement free (in ref. [21] such fiducials were called simple). Every known $\mathrm{EC}(d)$ orbit contains centred fiducials, and we conjecture that this is always the case. Given a centred fiducial Π we define $S_0(\Pi)$ to consist of all $F \in \mathrm{ESL}(2, \mathbb{Z}/d'\mathbb{Z})$ such that U_F is in the stability group of Π.

We next consider the Galois symmetries of the Clifford unitaries and SIC projectors. We say that an operator A is in (respectively generates) a field $\mathbb{F}$ as shorthand for the statement that its standard basis matrix elements are in (respectively generate) $\mathbb{F}$. Similarly we write $\mathbb{F}(A)$ to mean $\mathbb{F}\left(\bigcup_{r,s=0}^{d} \langle r|A|s\rangle\right)$. It is immediate that the displacement operators generate the cyclotomic field $\mathbb{Q}(\tau)$. The same is true of the symplectic unitaries, provided the phase in Eq. (8) is chosen appropriately. This was shown in ref. [30] for the case of prime dimensions using an argument based on Gauss sums. The argument is easily generalized to show, for arbitrary d, that if one chooses

$$e^{i\theta} = \begin{cases} 1 & d = 1 \mod 4 \\ i & d = 3 \mod 4 \\ e^{\frac{\pi i}{4}} & d = 0 \mod 2 \end{cases} \tag{13}$$

then $e^{i\theta}/\sqrt{d}$, and consequently U_F is in $\mathbb{Q}(\tau)$ for all $F \in \mathrm{SL}(2, \mathbb{Z}/d'\mathbb{Z})$. In the sequel we shall always assume that this choice of phase has been made.

---

[2] We define the Zauner matrix this way to secure consistency with ref. [13]. The Zauner matrix is often defined to be $F_z^4 = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$ which is order 3, unlike F_z which is order 6 when d is even. This makes no difference at the level of the unitaries since U_{F_z} and $U_{F_z^4}$ are equal modulo a phase.

Now let Π be any SIC fiducial projector and define $\mathbb{E} = \mathbb{Q}(\Pi, \tau)$. Since $\mathbb{E}$ contains every Clifford unitary, and also the complex conjugate Π^*, it will be the same for every other fiducial projector on the same $\mathrm{EC}(d)$ orbit. We refer to it as the SIC-field for that orbit[3].

From now on it will be assumed[4] without comment that $d \geq 4$. It was shown in ref. [21] that, for every exact fiducial in ref. [13], $\mathbb{E}$ is normal over $\mathbb{Q}$. Furthermore, $\mathbb{E}$ naturally breaks into the tower

$$\mathbb{Q} \lhd \mathbb{E}_c \lhd \mathbb{E}_0 \lhd \mathbb{E}_1 \lhd \mathbb{E} \tag{14}$$

where the notation $\mathbb{F} \lhd \mathbb{G}$ means "$\mathbb{G}$ is a normal extension of $\mathbb{F}$". We summarize the salient features of this tower. Let Π be any centred fiducial on the $\mathrm{EC}(d)$ orbit in question, let $g_{\mathrm{c}} \in \mathrm{Gal}(\mathbb{E}/\mathbb{Q})$ be complex conjugation, and let g be an arbitrary element of $\mathrm{Gal}(\mathbb{E}/\mathbb{Q})$. Then

(1) $\mathbb{E}_c$ is the fixed field of the centralizer of g_c.
(2) $\mathbb{E}_c = \mathbb{Q}(\sqrt{D})$, where D is the square-free part of $(d-3)(d+1)$.
(3) $\mathrm{Gal}(\mathbb{E}/\mathbb{E}_c)$ is Abelian.
(4) g fixes $\mathbb{E}_c$ if and only if $g(\Pi)$ is a SIC fiducial projector .
(5) g fixes $\mathbb{E}_0$ if and only if $g(\Pi)$ is a fiducial on the same $\mathrm{EC}(d)$ orbit as Π.
(6) $\mathbb{E} = \mathbb{E}_1(i\sqrt{d'})$.
(7) Let $\bar{g}_1$ be the non-trivial element of $\mathrm{Gal}(\mathbb{E}/\mathbb{E}_1)$. Then
$$\bar{g}_1 = g g_{\mathrm{c}} g^{-1} \tag{15}$$
if and only if g does not fix $\mathbb{Q}(\sqrt{D})$.
(8) For all $\mathbf{p}$ and some $\mathbf{k}_\Pi \in (\mathbb{Z}/d'\mathbb{Z})^2$
$$\bar{g}_1\big(\mathrm{Tr}(D_{\mathbf{p}}\Pi)\big) = \omega^{\langle \mathbf{k}_\Pi, \mathbf{p}\rangle}\, \mathrm{Tr}(D_{\mathbf{p}}\Pi). \tag{16}$$
(9) $\mathbb{E}_0$ is normal over $\mathbb{Q}$, but $\mathbb{E}_1$ is not.

Note that with the exception of item 1 which is a definition, item 4 (which is a consequence of item 1), item 5 (which is a definition) and the statement that $\mathbb{E}_1$ is not normal over $\mathbb{Q}$ (which is a consequence of item 7) these statements hold for all the known examples, but are not proven facts. Note also that it follows from item 7 that $\bar{g}_1(\tau) = \tau^{-1}$.

We say that a fiducial is strongly centred if it is centred and $\mathbf{k}_\Pi = 0$, so that the overlaps are all in $\mathbb{E}_1$. If $d \neq 0 \mod 3$ centred fiducials are automatically strongly centred [21]. If $d = 0 \mod 3$ the concepts are not equivalent. However, for every orbit for which an exact solution is known, the class of strongly centred fiducials is non-empty[5]. Moreover, there exist strongly centred fiducials whose stability group includes U_{F_z} (for a type-z orbit) or U_{F_a} (for a type-a orbit). If Π is strongly centred then, in every case where an exact fiducial has been calculated, the set of overlaps generates $\mathbb{E}_1$ over $\mathbb{Q}$.

The $\mathrm{EC}(d)$ orbits for a given dimension d split into sets of orbits sharing the same SIC field and mapping into each other under the associated Galois group. We refer to these sets as multiplets. In every known case there is a unique multiplet for which the associated field has minimal degree, and which we refer to as the minimal multiplet. We refer to the associated field as the minimal field.

[3] Note that in ref. [21] the extension $\bar{\mathbb{E}} = \mathbb{E}(\sqrt{d})$ was also introduced, to ensure that the Clifford unitaries would be in the field. The considerations in the previous paragraph show that this was unnecessary.

[4] This is because the SICs in dimensions 2 and 3 have some special properties, being the only known Weyl-Heisenberg covariant examples of what Stacey [18] calls "sporadic SICs" (also see Zhu [17]).

[5] This fact was not appreciated at the time ref. [21] was written. Consequently, the representatives of $\mathrm{EC}(d)$ orbits $6a$, $9ab$, $12b$, $24c$ in that paper are not strongly centred. They become strongly centred if Π is replaced with $D_{n,2n}\Pi D^\dagger_{n,2n}$, where $n = d/3$. This transformation leaves the stability group unchanged.

Let $\mathbb{E}$ be the minimal field in dimension d, and let $\mathbb{Q} \lhd \mathbb{Q}(\sqrt{D}) \lhd \mathbb{E}_0 \lhd \mathbb{E}_1 \lhd \mathbb{E}$ be the associated tower. In every known case [22]

(1) $\mathbb{E}$, $\mathbb{E}_1$ are ray class fields over $\mathbb{Q}(\sqrt{D})$ for which the finite part of the conductor is d',
(2) $\mathbb{E}$ is the ray class field with ramification allowed at both infinite places,
(3) $\mathbb{E}_1$ is the ray class field with ramification only allowed at the infinite place taking $\sqrt{D}$ to a positive real number,
(4) $\mathbb{E}_0$ is the Hilbert class field over $\mathbb{Q}(\sqrt{D})$.

We next describe the action of $\mathrm{Gal}(\mathbb{E}/\mathbb{Q})$ on the Clifford unitaries. For any operator A in $\mathbb{E}$ define

$$g(A) = \sum_{r,s=0}^{d-1} g\big(\langle r|A|s\rangle\big)|r\rangle\langle s| \tag{17}$$

where $|0\rangle, \dots, |d-1\rangle$ is the standard basis. Let k_g be the unique integer in the interval $(0, d')$ which is co-prime to d' and such that $g(\tau) = \tau^{k_g}$, and let

$$H_g = \begin{pmatrix} 1 & 0 \\ 0 & k_g \end{pmatrix}. \tag{18}$$

Then g acts on the elements of $\mathrm{C}(d)$ according to

$$g(D_{\mathbf{p}}U_F) \doteq D_{H_g\mathbf{p}}U_{H_gFH_g^{-1}}. \tag{19}$$

In dimensions where there is more than one multiplet one also finds that there is a unique multiplet for which the field is of maximal degree. We refer to this as the maximal multiplet, and to the associated field as the maximal field. Multiplets/fields which are neither maximal nor minimal we refer to as intermediate. In every known case intermediate fields contain the minimal field and are contained by the maximal field for the dimension in question.

Let $\{o_1, \dots, o_l\}$ be the $\mathrm{EC}(d)$ orbits of a multiplet in dimension d, let $\mathbb{E}$ be the associated SIC-field, and let Π_j be a strongly centered fiducial on orbit o_j. Then for each $g \in \mathrm{Gal}(\mathbb{E}/\mathbb{E}_c)$ and each index j there exists $F_{h,j} \in \mathrm{ESL}(d)$ and an index k such that

$$g(\Pi_j) = U_{F_{g,j}}\Pi_k U^{\dagger}_{F_{g,j}}. \tag{20}$$

Also

$$g\big(\mathrm{Tr}(D_{\mathbf{p}}\Pi_j)\big) = \mathrm{Tr}(D_{G_{g,j}\mathbf{p}}\Pi_k) \tag{21}$$

for all $\mathbf{p}$, where

$$G_{g,j} = (\mathrm{Det}\, F_{g,j})F^{-1}_{g,j}H_g. \tag{22}$$

If $g \in \mathbb{E}_0$ then $k = j$ in Eqs. (20) and (21). The matrices $F_{h,j}$, $G_{h,j}$ are not unique: Indeed, they can be replaced with arbitrary elements of the cosets $F_{h,j}S_0(\Pi)$, $S(\Pi)G_{h,j}$ respectively, where

$$S(\Pi) = \{(\mathrm{Det}\, F)F \colon F \in S_0(\Pi)\}. \tag{23}$$

For the automorphism $\bar{g}_1$ we can choose [21]

$$G_{\bar{g}_1,j} = I \qquad\qquad F_{\bar{g}_1,j} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{24}$$

for all j.

If $g \in \mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0)$ define $G_{g,j} = G_{g',j}$ where g' is a lift of g to $\mathrm{Gal}(\mathbb{E}/\mathbb{E}_0)$. It is easily seen that this definition does not depend on which of the two lifts is taken. It can be shown [21] that the $G_{g,j}$ are all in $N(\Pi)$, the normalizer of $S(\Pi)$ in $\mathrm{GL}(2, \mathbb{Z}/d'\mathbb{Z})$, and that for each fixed j the map $g \to G_{g,j}S(\Pi)$ is an injective homomorphism of $\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0)$

into $N(\Pi)/S(\Pi)$. It is natural to ask, what is the range of this homomorphism. The answer depends on whether the $\mathrm{EC}(d)$ orbit is type-z or type-a.

Suppose the orbit is type-z. Then, in every known case, one finds that the range of the homomorphism is $C(\Pi)/S(\Pi)$, where $C(\Pi)$ is the centralizer of $S(\Pi)$ in $\mathrm{GL}(2, \mathbb{Z}/d'\mathbb{Z})$. So we have an isomorphism [21]

$$\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0) \cong C(\Pi)/S(\Pi). \tag{25}$$

The conjecture, that this isomorphism holds generally, plays an important role in the calculations in the next section. Its restriction to the case of minimal SIC fields would, if true, also be of number-theoretical interest: For it would mean that the Galois group of a ray class field over the Hilbert class field of a real quadratic field is, in many cases, isomorphic to the quotient of two matrix groups.

Suppose, on the other hand, that the orbit is type-a. There are only two such orbits for which exact solutions are given in ref. [13]; namely, $12b$ and $48g$. For both of those one finds [21]

$$\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0) \cong C(\Pi)/S(\Pi). \tag{26}$$

just as is the case for the type-z orbits. The problem [21] is that one can see from the numerical data that the group $C(\Pi)/S(\Pi)$ is non-Abelian[6] for the type-a orbits $21d$, $30d$, $39gh$, $48e$ (by contrast, $C(\Pi)/S(\Pi)$ is Abelian for every known numerical type-z orbit). So for these orbits one of two things must be true: Either $\mathbb{E}$ is not an Abelian extension of $\mathbb{Q}(\sqrt{D})$, or else $\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0)$ is not isomorphic to $C(\Pi)/S(\Pi)$. We discuss this problem further in the next section.

3. Type-a fiducials

An alternative to the isomorphism of Eq. (25) holding for type-a fiducials was conjectured in ref. [21]. In this section we propose a stronger conjecture, which holds for the previously known fiducials $12b$, $48g$, and also for fiducial $21d$ calculated using the methods described in Section 5.

Suppose $d = 3 \mod 9$. Then $d = 3n$ where $n = 1 \mod 3$ and

$$F_a = \begin{pmatrix} 1 & 3n+3 \\ 4n-1 & 3n-2 \end{pmatrix}. \tag{27}$$

The fact that n is coprime to 3 means (see Appendix B of ref. [25]) that there is a natural isomorphism

$$\chi\colon\ \mathrm{SL}(2, \mathbb{Z}/d'\mathbb{Z}) \to \mathrm{SL}(2, \mathbb{Z}/n'\mathbb{Z}) \times \mathrm{SL}(2, \mathbb{Z}/3\mathbb{Z}). \tag{28}$$

It is straightforward to show that χ extends to an isomorphism of $\mathrm{GL}(2, \mathbb{Z}/d'\mathbb{Z})$ onto $\mathrm{GL}(2, \mathbb{Z}/n'\mathbb{Z}) \times \mathrm{SL}(2, \mathbb{Z}/3\mathbb{Z})$, and that, for arbitrary $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbb{Z}/d'\mathbb{Z})$,

$$\chi\left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right) = \left(\begin{pmatrix} \alpha & 3\beta \\ \frac{(2n+1)\gamma}{3} & \delta \end{pmatrix}, \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right) \tag{29}$$

where $n' = n$ (respectively $n' = 2n$) if n is odd (respectively even). Applying this to F_a we find that

$$\chi(F_a) = (\bar{F}_a, I) \tag{30}$$

where

$$\bar{F}_a = \begin{pmatrix} 1 & n+9 \\ \frac{4n-1}{3} & n-2 \end{pmatrix}. \tag{31}$$

[6] By contrast, it can be shown [21] that for a type-z orbit $C(\Pi)/S(\Pi)$ is Abelian whenever $S(\Pi)$ is Abelian, as it is for every known numerical fiducial (more than that, $S(\Pi)$ is cyclic in every known case).

Observe that $\mathrm{Tr}(\bar{F}_a) = -1 \mod n$, implying that $\bar{F}_a$ is conjugate to the Zauner matrix in dimension n.

Now consider the isomorphism of Eq. (25). Suppose, to begin with, that Π is a strongly centred type-z fiducial. Without loss of generality we may assume that Π is an eigenvector of U_{F_z}. Assume also that $S(\Pi)$ is Abelian (as is the case for every known fiducial with $d \geq 4$). It is shown in ref. [21] that $C(F_z)$, the centralizer of F_z in $\mathrm{GL}(2, \mathbb{Z}/d'\mathbb{Z})$, is Abelian, from which it follows that $C(\Pi) = C(F_z)$ so that the isomorphism becomes

$$\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0) \cong C(F_z)/S(\Pi). \tag{32}$$

On the assumption that the left hand side is Abelian (as is the case for every known exact fiducial) this relation cannot hold for an arbitrary type-a orbit. Indeed, it can be seen from Eq. (30) that

$$C(F_a) \cong C(\bar{F}_a) \times \mathrm{GL}(2, \mathbb{Z}_3). \tag{33}$$

The fact that $\bar{F}_a$ is conjugate to the Zauner matrix in dimension n means that $C(\bar{F}_a)$ is Abelian; however $\mathrm{GL}(2, \mathbb{Z}_3)$ is non-Abelian, implying that $C(F_a)$ is non-Abelian. This means that, if $S(\Pi)$ is generated by F_a (as it is in, for example, orbits $21d$, $30d$, $39gh$, $48e$), then $C(F_a)/S(\Pi)$ is non-Abelian.

As a generalization of Eq. (32) holding for every orbit, irrespective of whether it is type-z or type-a, we propose:

Conjecture 1. *Let Π be a strongly-centred fiducial, and let $F \in S(\Pi)$ be such that the unitary U_F is canonical order 3. Then*

$$\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0) \cong \mathcal{M}/S(\Pi). \tag{34}$$

where $\mathcal{M}$ is a maximal Abelian subgroup of $\mathrm{GL}(2, \mathbb{Z}/d'\mathbb{Z})$ containing F.

Note that in the case of type-z fiducials this conjecture reduces to Eq. (32). It holds for every known exact fiducial. In particular, it holds for the type-a fiducials $12b$ and $48g$ (calculated in ref. [13]) and $21d$ (calculated here).

In the case of a type-z fiducial there is exactly one maximal Abelian subgroup $\mathcal{M}$ containing F; namely, the centralizer $C(F)$. But for a type-a fiducial there are several. Indeed, one sees from Eq. (30) that a subgroup $\mathcal{M}$ containing F_a is maximal Abelian if and only if

$$\chi(\mathcal{M}) = C(\bar{F}_a) \times \bar{\mathcal{M}} \tag{35}$$

where $\bar{\mathcal{M}}$ is an arbitrary maximal Abelian subgroup of $\mathrm{GL}(2, \mathbb{Z}_3)$. One finds that $\bar{\mathcal{M}}$ must be conjugate to one of the three groups

$$\bar{\mathcal{H}}_4 = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle, \tag{36}$$

$$\bar{\mathcal{H}}_6 = \left\langle \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} \right\rangle, \tag{37}$$

$$\bar{\mathcal{H}}_8 = \left\langle \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \right\rangle, \tag{38}$$

which are order 4, 6 and 8 respectively. Consequently, $\mathcal{M}$ must be conjugate to one of the three groups

$$\mathcal{H}_j = \chi^{-1}\big(C(\bar{F}_a) \times \bar{\mathcal{H}}_j\big), \qquad j = 4, 6, 8. \tag{39}$$

We say that an orbit is type-a_j if $\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0)$ is isomorphic to $\mathcal{H}_j$. Of the known cases orbit $12b$ is type-a_4 while orbits $21e$, $48g$ are type-a_8. It is an open question, whether there exist any type-a_6 orbits.

In ref. [25] the following, weaker conjecture was proposed for strongly-centred type-a fiducials:

Conjecture 2. *Let* Π *be a strongly-centred type-a fiducial and let* $F \in S$ *be such that* U_F *is a canonical order 3 unitary. Then*

$$\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0) \cong \mathcal{A}/S(\Pi) \tag{40}$$

where

$$\mathcal{A} = \{rI + sG \colon r, s \in \mathbb{Z}/d'\mathbb{Z} \text{ and } rI + sG \in \mathrm{GL}(2, \mathbb{Z}/d'\mathbb{Z}\} \tag{41}$$

for some matrix G *such that* $F = I + 3G$*.*

To see that this conjecture is indeed weaker, let Π be a strongly centred type-a fiducial satisfying Conjecture 1. Then $\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0) \cong \mathcal{H}_j/S(\Pi)$ for some j. The fact that $\bar{F}_a$ is conjugate to the Zauner matrix in dimension n means, in view of Lemma 12 in ref. [21],

$$C(\bar{F}_a) = \{rI + s\bar{F}_a \colon r, s \in \mathbb{Z}/n'\mathbb{Z} \text{ and } rI + s\bar{F}_a \in \mathrm{GL}(2, \mathbb{Z}/n'\mathbb{Z})\}. \tag{42}$$

Define

$$\bar{G} = \frac{2n+1}{3}(\bar{F}_a - I) \tag{43}$$

(note that the fact that $n = 1 \mod 3$ means $(2n+1)/3$ is an integer). Then we also have $\bar{F}_a = I + 3\bar{G}$, implying

$$C(\bar{F}_a) = \{rI + s\bar{G} \colon r, s \in \mathbb{Z}/n'\mathbb{Z} \text{ and } rI + s\bar{G} \in \mathrm{GL}(2, \mathbb{Z}/n'\mathbb{Z})\}. \tag{44}$$

It is straightforward to show that

$$\bar{\mathcal{H}}_j = \{rI + s\bar{H}_j \colon r, s \in \mathbb{Z}/3\mathbb{Z} \text{ and } rI + s\bar{H}_j \in \mathrm{GL}(2, \mathbb{Z}/3\mathbb{Z}\} \tag{45}$$

where

$$\bar{H}_4 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \bar{H}_6 = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}, \qquad \bar{H}_8 = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}. \tag{46}$$

Using the Chinese Remainder Theorem [31] one finds

$$\mathcal{H}_j = \{rI + sH_j \colon r, s \in \mathbb{Z}/d'\mathbb{Z} \text{ and } rI + sH_j \in \mathrm{GL}(2, \mathbb{Z}/d'\mathbb{Z})\} \tag{47}$$

where

$$H_j = \chi^{-1}(\bar{G}, \bar{H}_j). \tag{48}$$

The fact that

$$\chi(I + 3H_j) = (I + 3\bar{G}, I) = \chi(F_a), \tag{49}$$

means $I + 3G_j = F_a$. So Π satisfies Conjecture 2. To see that Conjecture 2 is strictly weaker than Conjecture 1 consider the order 2 subgroup of $\mathrm{GL}(2, \mathbb{Z}/3\mathbb{Z})$.

$$\bar{\mathcal{H}}_2 = \langle -I \rangle = \{rI + s\bar{H}_2 \colon r, s \in \mathbb{Z}/3\mathbb{Z} \text{ and } rI + s\bar{H}_2 \in \mathrm{GL}(2, \mathbb{Z}/3\mathbb{Z})\} \tag{50}$$

where $\bar{H}_2 = -I$. Let $\mathcal{H}_2 = \chi^{-1}\big((\bar{G}, \bar{\mathcal{H}}_2)\big)$. Then

$$\mathcal{H}_2 = \{rI + sH_2 \colon r, s \in \mathbb{Z}/d'\mathbb{Z} \text{ and } rI + sH_2 \in \mathrm{GL}(2, \mathbb{Z}/d'\mathbb{Z})\} \tag{51}$$

where

$$H_2 = \chi^{-1}(\bar{G}, \bar{H}_2). \tag{52}$$

Moreover $I + 3H_2 = F_a$. So a fiducial for which $\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0) \cong \mathcal{H}_2/S(\Pi)$ would satisfy Conjecture 2. However, it would not satisfy Conjecture 1 because $\mathcal{H}_2$ is not maximal Abelian, being properly contained in $\mathcal{H}_4$, $\mathcal{H}_6$, $\mathcal{H}_8$.

The group $\mathcal{H}_2$ plays an important role in the reconstruction of exact type-a fiducials from numerical ones, as we will discuss in the next section. This is because $\bar{\mathcal{H}}_2$ is the centre of $\mathrm{GL}(2, \mathbb{Z}/3\mathbb{Z})$, which means that $\mathcal{H}_2$ is contained in every maximal Abelian subgroup of $\mathrm{GL}(2,\mathbb{Z}/d'\mathbb{Z})$ containing F_a. In view of its importance it may be worth noting that, in addition to Eq. (51), one also has

$$\mathcal{H}_2 = \{rI + sF_a \colon r,s \in \mathbb{Z}/d'\mathbb{Z} \text{ and } rI + sF_a \in \mathrm{GL}(2,\mathbb{Z}/d'\mathbb{Z})\}. \tag{53}$$

Indeed, it is easily verified that

$$H_2 = \frac{2n+1}{3}F_a + \frac{4n-1}{3}I \tag{54}$$

(note that the fact that $n = 1 \mod 3$ means $2n+1$ and $4n-1$ are both divisible by 3). Together with the relation $F_a = I + 3H_2$ this means

$$\begin{aligned} &\{rI + sH_2 \colon r,s \in \mathbb{Z}/d'\mathbb{Z} \text{ and } rI + sH_2 \in \mathrm{GL}(2,\mathbb{Z}/d'\mathbb{Z})\} \\ &\qquad = \{rI + sF_a \colon r,s \in \mathbb{Z}/d'\mathbb{Z} \text{ and } rI + sF_a \in \mathrm{GL}(2,\mathbb{Z}/d'\mathbb{Z})\}. \end{aligned} \tag{55}$$

4. Fields and Multiplets

It is shown in ref. [22] that in every known case the minimal SIC field in each dimension is the ray-class field over $\mathbb{Q}(\sqrt{D})$ with conductor d' and ramification at both infinite places. We will refer to the conjecture, that this is always the case, as the ray-class conjecture. However in many dimensions (not all) there are other SIC fields, having higher degree. This raises the question, whether one can generalize the ray-class conjecture to these additional fields.

For the dimensions where Scott and Grassl give a full set of exact solutions there are either one or two SIC fields. We refer to the field of lowest (respectively highest) degree as the minimal field, denoted $\mathbb{E}_{\text{min}}$ (respectively maximal field, denoted $\mathbb{E}_{\text{max}}$). Associated to the two fields are two multiplets, which we refer to as the minimal and maximal multiplets. This information is presented in Table 1. It raises several questions:

d	minimal multiplet	maximal multiplet	$[\mathbb{E}_{\text{max}} \colon \mathbb{E}_{\text{min}}]$
4	$4a$		
5	$5a$		
6	$6a$		
7	$7b$	$7a$	2
8	$8b$	$8a$	4
9	$9ab$		
10	$10a$		
11	$11c$	$11ab$	2
12	$12b$	$12a$	3
13	$13ab$		
14	$14ab$		
16	$16ab$		

Table 1. Minimal and maximal multiplets for dimensions where Scott and Grassl [13] give a full set of exact fiducials. We only list the maximal multiplet when it is distinct from the minimal one. The right-most column gives the degree of the extension $\mathbb{E}_{\text{max}}/\mathbb{E}_{\text{min}}$, where $\mathbb{E}_{\text{max}}$ is the maximal field and $\mathbb{E}_{\text{min}}$ is the minimal one.

(1) In the four dimensions listed for which there are two distinct SIC fields, the maximal field is an extension of the minimal one. One would like to know if that is merely a low dimensional accident, or whether it is generally true.
(2) There are at most two distinct fields in the dimensions listed. One would like to know if in higher dimensions there are sometimes more than two.

(3) In the dimensions listed it never happens that there is more than one multiplet associated to a given field. One would like to know if this $1:1$ correspondence between fields and multiplets persists in higher dimensions.

(4) In the dimensions listed $\mathbb{E}_{\text{min}}$ is the ray class field over $\mathbb{Q}(\sqrt{D})$ with conductor d' and ramification at both infinite place. One would like to formulate a conjecture applying to the non-minimal fields in each dimension. For this purpose it would be useful to have more examples than the four cases $7a$, $8a$, $11ab$, $12a$.

One of our aims in the calculations reported here was to address these questions. Our results reveal that the number of fields in a given dimension can be larger than 2. However, in every case calculated, one continues to find that there is a unique field $\mathbb{E}_{\text{min}}$ of minimal degree over $\mathbb{Q}$, and a unique field $\mathbb{E}_{\text{max}}$ of maximal degree over $\mathbb{Q}$. The field $\mathbb{E}_{\text{min}}$ is always the ray class field over $\mathbb{Q}(\sqrt{D})$ with conductor d' and ramification at both infinite places. The field $\mathbb{E}_{\text{max}}$ always contains $\mathbb{E}_{\text{min}}$, and additional fields $\mathbb{E}$, when they exist, always lie between these two:

$$\mathbb{E}_{\text{min}} \subseteq \mathbb{E} \subseteq E_{\text{max}}. \tag{56}$$

We accordingly refer to them as intermediate fields, and to the associated multiplets as intermediate multiplets. Finally, one continues to find that there is a $1:1$ correspondence between fields and multiplets. This information is summarized in Table 2 and Fig. 1

d	minimal multi-plet	intermediate multiplet(s)	maximal multi-plet	$[\mathbb{E}_{\text{max}} : \mathbb{E}_{\text{min}}]$
15	$15d$	$15b$	$15ac$	4
17	$17c$		$17ab$	2
18	$18ab$			
19	$19e$	$19a$, $19d$	$19bc$	12
20	$20ab$			
21	$21e$		$21abcd$	3
24	$24c$		$24ab$	4
28	$28c$		$28ab$	4
30	$30d$		$30abc$	3
35	$35j$	$35i$, $35e$, $35h$, $35af$	$35bcdg$	16
39	$39ij$	$39bf$, $39gh$	$39acde$	6
48	$48g$	$48e$, $48f$	$48abcd$	24

Table 2. Minimal, maximal and intermediate multiplets for the dimensions calculated in this paper. Note that exact fiducials for orbits $15d$, $19e$, $24c$, $28c$, $35j$, $48g$ were already known; all other exact fiducials in these dimensions are new, however.

5. Method for Calculating Exact Fiducials

We first describe the obvious, or "brute-force" approach to the problem. We then describe the refinements actually used to perform the calculations in this paper. Suppose that Π is a high precision, approximate SIC-fiducial in dimension d such that $\mathbb{Q}(\Pi, \tau)$ is the minimal SIC-field for that dimension. If the conjectures in ref. [22] are correct $\mathbb{Q}(\Pi, \tau)$ is then the ray class field over $\mathbb{Q}(\sqrt{D})$ with conductor d' and ramification at both infinite places. Using *Magma* we can easily calculate a basis for the field over $\mathbb{Q}$.

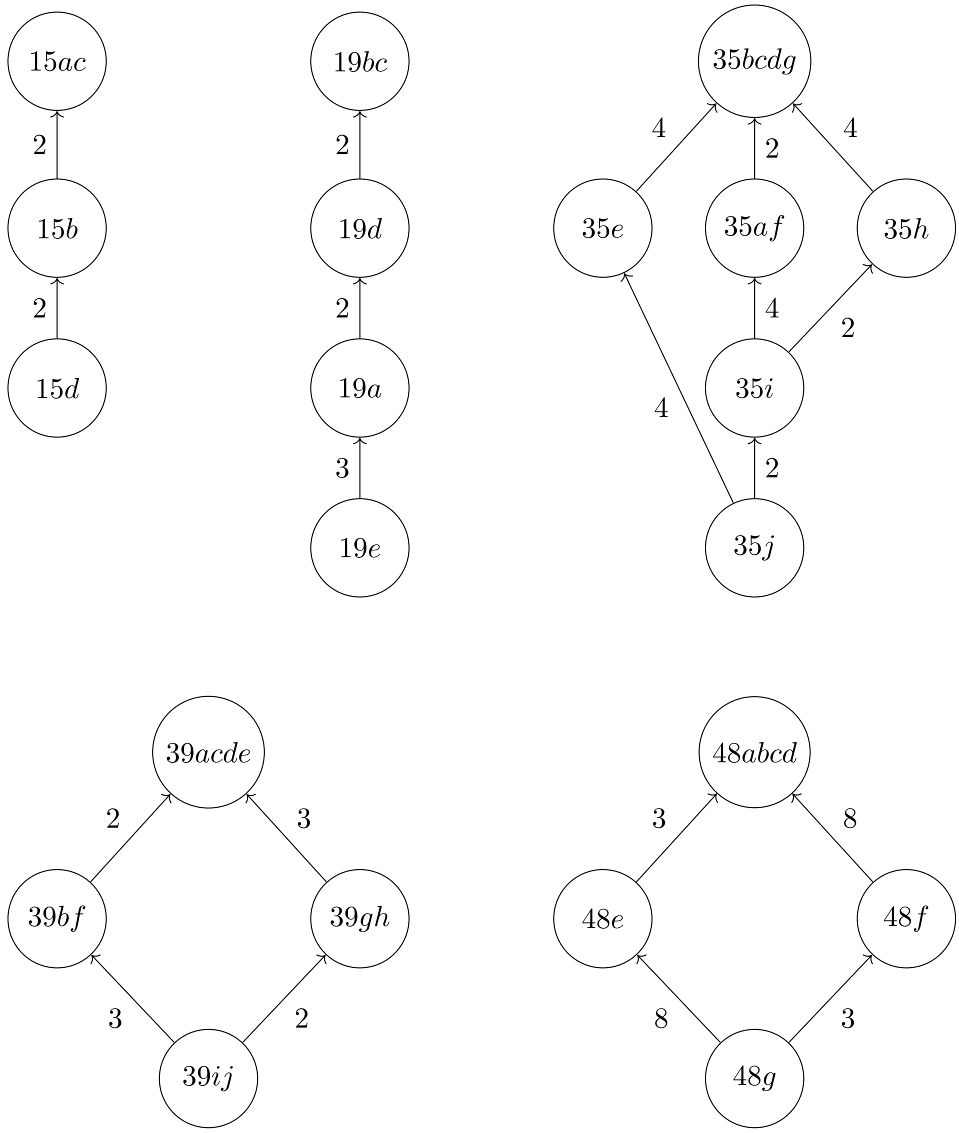

FIGURE 1. Field inclusions for cases where there are one or more intermediate fields. The arrows run from the smaller field to the larger; numbers beside the arrows are the degrees of the extensions.

Let $b_1, \dots, b_n$ be such a basis, and let $\langle j|\Pi|k\rangle$ be an arbitrary matrix element. Then there exist integers $\mu_0, \mu_1, \dots, \mu_n$ such that

$$\mu_0 \langle j|\Pi|k\rangle - \sum_{j=1}^{n} \mu_j b_j = 0 \tag{57}$$

to a high degree of precision. If the precision is sufficiently great we can use an integer relation algorithm to find the integers μ_j. Substituting these integers in

$$\sum_{j=1}^{n} \frac{\mu_j}{\mu_0} b_j \tag{58}$$

gives us an *exact* expression for the matrix element. There are two problems with this "brute-force" approach:

- We do not currently have a conjecture for $\mathbb{Q}(\Pi,\tau)$ when it is not the minimal field.
- In the cases of interest to us the degree of the minimal field is large, which means that the required precision is large, and the calculation correspondingly slow.

To deal with these problems we therefore modified the procedure. We actually employed two different methods, which we refer to as methods 1 and 2. Method 1 was the original method used to calculate the exact fiducials in dimensions 17–21. Method 2 is a much improved method used to calculate the exact fiducials for $d \geq 24$ (and also for $d = 15$ which, although the dimension is smallest, were actually calculated last).

Method 1. Instead of the matrix elements $\langle j|\Pi|k\rangle$ we calculate the overlaps

$$\chi_{\mathbf{p}} = \mathrm{Tr}\big(D_{\mathbf{p}}\Pi\big). \tag{59}$$

We describe the method as it applies for a type-z fiducial, and then indicate the modifications needed to deal with a type-a fiducial at the end. Let $C(\Pi)$ be the centralizer of $S(\Pi)$, and let $\mathcal{O}_1 \dots \mathcal{O}_m$ be the orbits of $\big(\mathbb{Z}/d'\mathbb{Z}\big)^2$ under the action of $C(\Pi)$. If $d \neq 0 \mod 3$ (respectively[7] $d = 0 \mod 3$) let $\mathcal{S}_j$ be the set of distinct numbers $\chi_{\mathbf{p}}$ (respectively $\chi^3_{\mathbf{p}}$) obtained as $\mathbf{p}$ runs over $\mathcal{O}_j$, and define

$$Q_j(x) = \prod_{r\in\mathcal{S}_j}(x-r). \tag{60}$$

Note that we can calculate $S(\Pi)$ and $C(\Pi)$ just from a knowledge of the numerical fiducial. Consequently, the polynomials $Q_j(x)$ can be calculated numerically. If the conjecture that $\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0)$ is isomorphic to $C\Pi)/S(\Pi)$, is correct (*c.f.* Eq. (25)) then the coefficients of the exact polynomial $Q_j(x)$ all belong to the field $\mathbb{E}_0$. Since the degree of $\mathbb{E}_0/\mathbb{Q}$ is much less than that of $\mathbb{E}/\mathbb{Q}$ (no greater than 8 for the fiducials calculated in this paper), it is possible to find the exact coefficients from the numerical ones without knowing the field in advance, and without an impractically high degree of precision and CPU time (using, for instance, the *Magma* function `MinimalPolynomial` or the *Mathematica* function `RootApproximant`). In practice it is most efficient to use this method to find an exact expression for the next-to-leading coefficient of the lowest degree polynomial $Q_j(x)$ (because this is the coefficient which involves the smallest integers, and is therefore easiest to find). Once $\mathbb{E}_0$ has been ascertained one can then use a function such as `IntegerRelation` (in *Magma*) or `FindIntegerNullVector` (in *Mathematica*) which assumes a knowledge of the field to find every coefficient of every polynomial. The total CPU time needed to obtain exact expressions for the full set of polynomials $Q_j(x)$ was ~ 1 second or less in every case. The precision needed was 10^3 decimal digits or less. We then used *Magma* to construct the the ray class field over $\mathbb{Q}(\sqrt{D})$ with conductor d' and ramification at both infinite places. For a minimal SIC fiducial exact values of the overlaps were found directly, by factoring the $Q_j(x)$ over this field. If the fiducial was not minimal we factored the $Q_j(x)$ as far as possible, and then used *Magma* to find simplified generators for $\mathbb{E}$ as an extension of the ray class field. The overlaps can then be expressed in terms of the generators. This part of the calculation took ~ 1 day of CPU time. Finally, the exact fiducial was calculated from the overlaps using Eq. (4).

For a type-a fiducial the above procedure needs to be modified slightly. This is because, if Conjecture 1 is correct, $\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0)$ is isomorphic to $\mathcal{M}/S(\Pi)$ for some maximal Abelian subgroup $\mathcal{M}$ which, unlike $C(\Pi)$ for a type-z fiducial, cannot be determined

[7] We need to treat the case when $d = 0 \mod 3$ differently because one cannot tell if a numerical fiducial is strongly centred or not. If the fiducial is not strongly centred then $g(\chi_{\mathbf{p}})$ only equals $\chi_{G_g\mathbf{p}}$ up to a cube root of unity [21] (where g is any element of $\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0)$), and the coefficients of $Q_j(x)$ are consequently guaranteed to be in the field $\mathbb{E}_0$. Cubing the overlaps obviates this difficulty.

from the numerical data. To get round this problem we use the fact that, as shown in Section 3, the group $\mathcal{M}$ necessarily contains the group $\mathcal{H}_2$, which can be calculated in advance of knowing the exact fiducial from Eq. (53). The calculation then mirrors the calculation for a type-z fiducial, but using $\mathcal{H}_2$ instead of $C(\Pi)$. Specifically, let $\mathcal{O}_1 \dots \mathcal{O}_m$ be the orbits of $\left(\mathbb{Z}/d'\mathbb{Z}\right)^2$ under the action of $C(\Pi)$, and let $\mathcal{S}_j$ be the set of distinct numbers $\chi^3_{\mathbf{p}}$ obtained as $\mathbf{p}$ runs over $\mathcal{O}_j$; then define $Q_j(x) = \prod_{r\in\mathcal{S}_j}(x-r)$. Let

$$f\colon \operatorname{Gal}(\mathbb{E}_1/\mathbb{E}_0) \to \mathcal{M}/S(\Pi) \tag{61}$$

Then the coefficients of $Q_j(x)$ are in $\mathbb{F}$, the fixed field of $f^{-1}(\mathcal{H}_2)$. It follows from the results in Section 3 that $[\mathcal{M}\colon \mathcal{H}_2] \leq 4$. Consequently, the degree of $\mathbb{F}/\mathbb{Q}$ is no more than 4 times greater than the degree of $\mathbb{E}_0/\mathbb{Q}$, which means one can apply the technique described in the last paragraph for a type-z fiducial to determine the exact values of the coefficients of the $Q_j(x)$, and hence to determine the exact fiducial.

There are two main steps to the method just described. The first step is to find the exact values of the coefficients of the polynomials $Q_j(x)$ using an integer relation algorithm; the second is to factor the polynomials. As we noted above the first step is fast, taking $\lesssim 1$ second of CPU time in every case tried. The second step is much slower. Moreover, the computation time grows rapidly with the degree of the number field. To deal with this problem we developed a new method, which does not rely so heavily on factoring, and is therefore much more efficient. While developing this method we also discovered the fact noted in Section 2, that every known centred fiducial becomes strongly centred when multiplied by the appropriate displacement operator. This obviated the need when $d = 0 \mod 3$ to first calculate the cubed overlaps and then to take the cube root at the end of the calculation.

Method 2. As before we first describee method as it applies to type-z fiducials, the modifications needed to handle type-a fiducials being described afterwards.

As with method 1, we begin by calculating high precision numerical approximations to the polynomials $Q_j(x)$; with, however, the difference that even when $d = 0 \mod 3$ the numbers r in Eq. (60) are the overlaps themselves, as opposed to their cubes. We then use the *Magma* function `MinimalPolynomial` to obtain exact versions of the coefficients. If $d \neq 0 \mod 3$ we take $\mathbb{E}_0$ to be the field generated by the coefficients. If $d = 0 \mod 3$ we repeat the calculation for each of the nine fiducial vectors $D_p|\psi\rangle$ for which $p = 0 \mod d/3$, and then take the desired strongly centred fiducial to be the one for which the polynomials obtained by applying `MinimalPolynomial` to the coefficients have lowest degree. If the SIC is minimal $\mathbb{E}_1$ can be taken to be the appropriate ray-class field. Otherwise $\mathbb{E}_1$ is an extension of this field. We find a set of generators for the extension by factoring some of the polynomials $Q_j(x)$. It is crucial to the success of this method that in practice one does not need to factor all the $Q_j(x)$. More than that: it turns out that one can get the additional field generators by factoring a polynomial whose degree is order 10 or less (which particular polynomial being ascertained by trial and error). The fact that the degree is so small means that the factoring can be done in minutes at most. If instead one had to factor the $Q_j(x)$ of highest degree this method would have few, if any advantages over Method 1 described above.

Once the fields $\mathbb{E}_0$ and $\mathbb{E}_1$ have been determined we use the conjectured isomorphism of Eq. (25) to reduce the rest of the calculation to a problem in linear algebra. Let $b_1, \dots, b_n$ be a basis for the extension $\mathbb{E}_1/\mathbb{E}_0$, let $g_1, \dots, g_n$ and $G_1S(\Pi), \dots, G_nS(\Pi)$ be explicit listings of the elements of $\operatorname{Gal}(\mathbb{E}_1/\mathbb{E}_0$ and $C(\Pi)/S(\Pi)$ respectively, and let $\mathcal{P}$ be the set of permutations f with the property that

$$g_j \to G_{f(j)}S(\Pi) \tag{62}$$

is an isomorphism of $\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0)$ onto $C(\Pi)/S(\Pi)$. Given any overlap $\mathrm{Tr}(D_{\mathbf{p}}\Pi)$

$$\sum_{k=1}^{n} s_k b_k = \mathrm{Tr}(D_{\mathbf{p}}\Pi) \tag{63}$$

for some $s_k \in \mathbb{E}_0$. The conjecture is that for some permutation $f \in \mathcal{P}$

$$g_j\big(\mathrm{Tr}(D_{\mathbf{p}}\Pi)\big) = \mathrm{Tr}(D_{G_{f(j)}\mathbf{p}}\Pi) \tag{64}$$

for all j. If correct this means

$$S = B^{-1}V_f \tag{65}$$

where B is the matrix

$$B = \begin{pmatrix} g_1(b_1) & g_1(b_2) & \dots \\ g_2(b_1) & g_2(b_2) & \dots \\ \vdots & \vdots & \end{pmatrix} \tag{66}$$

and S, V_f are the vectors

$$S = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \end{pmatrix}, \qquad\qquad V_{f_0} = \begin{pmatrix} \mathrm{Tr}(D_{G_{f(1)}\mathbf{p}}\Pi) \\ \mathrm{Tr}(D_{G_{f(2)}\mathbf{p}}\Pi) \\ \vdots \end{pmatrix}. \tag{67}$$

Of course, we do not know the permutation f. To find it we consider in turn each of the permutations in $\mathcal{P}$, and use it in conjunction with Eq. (65) to calculate a high-precision candidate for the vector S (in practice 10^3 digits of precision was sufficient). Let s_j be the j^{th} component of this candidate vector, and let $e_1, \dots, e_m$ be a basis for $\mathbb{E}_0/\mathbb{Q}$. We use the *Magma* function `IntegerRelation` to find integers $l_{j,0}, \dots, l_{j,m}$ solving the equation $l_{j,0}s_j - l_{j,1}e_1 - \dots - l_{j,m}e_m = 0$. We find that for one choice of permutation f the norms $\sqrt{l_{j,0}^2 + \dots + l_{j,m}^2}$ are many orders of magnitude smaller than they are for any of the others. We take this permutation to correspond to the true isomorphism between $\mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0)$ and $C(\Pi)/S(\Pi)$, and

$$S = \sum_{a=1}^{m} e_a \begin{pmatrix} \frac{l_{1,a}}{l_{1,0}} \\ \frac{l_{2,a}}{l_{2,0}} \\ \vdots \end{pmatrix} \tag{68}$$

to be the exact value of the vector S. We then invert Eq. (65) to obtain the exact value of the overlaps $\mathrm{Tr}(D_{G_{f(j)}\mathbf{p}}\Pi)$. By repeating this procedure we obtain an exact value for every overlap and then use Eq. (4) to obtain the exact fiducial. Finally, we check that the vector so obtained really is an exact fiducial.

In this description we have assumed that the fiducial to be calculated is type-z. To calculate a type-a fiducial the method can be modified along the lines indicated at the end of our description of method 1.

Appendix A. Results

We used the method described in Section exact fiducials for $\mathrm{EC}(d)$ orbits $17abc$, $18ab$, $19abcd$, $20ab$, $21abcde$. The fiducials themselves are available online [32]. The purpose of this appendix is to describe the associated fields, Galois groups and the isomorphism of Eq. (34).

When d is not a multiple of 3 we always calculate an exact version of the corresponding Scott-Grassl [13] numerical fiducial. When d is a multiple of 3 we transform the Scott-Grassl fiducial so as to make it strongly-centred. Let Π_{sg} be an exact version of the

Scott-Grassl numerical fiducial in such a dimension, and let Π_{sc} be the strongly-centred fiducial we have calculated. Then

$$\Pi_{\text{sc}} = U\Pi_{\text{sg}}U^\dagger \tag{69}$$

where U is the displacement operator specified in Table 3.

orbit	U	orbit	U	orbit	U	orbit	U
$15a$	$D_{5,10}$	$21bcd$	$D_{14,7}$	$30d$	$D_{20,20}$	$39h$	$D_{26,0}$
$15c$	$D_{10,5}$	$21e$	$D_{7,0}$	$39abcd$	$D_{26,13}$	$39i$	$D_{26,26}$
$15bd$	I	$24abc$	$D_{8,16}$	$39e$	I	$39j$	$D_{13,13}$
$18ab$	$D_{12,6}$	$30ac$	$D_{30,10}$	$39f$	$D_{13,26}$	$48adfg$	I
$21a$	$D_{7,14}$	$30b$	I	$39g$	$D_{0,13}$	$48bc$	$D_{16,32}$
						$48e$	$D_{16,16}$

TABLE 3. Displacement operators converting Scott-Grassl numerical fiducials to strongly-centred ones in dimensions divisible by 3.

The multiplet structure for these dimensions is specified in Table 2. The maximal field for each dimension is specified in Tables 4–8, using the same notational conventions as in ref. [21] to denote the field generators:

- a denotes D, the square-free part of $(d-3)(d+1)$.
- $r_1, \dots, r_j$ denote square roots of integers.
- t denotes $\cos \pi/d$ or $\sin \pi/d$.
- $b_1, \dots, b_k$ denote numbers constructed recursively from $\mathbb{Q}(a, r_1, \dots, r_j, t)$ by taking sums, products and roots.
- i denotes the square root of -1.

The a, r and t generators are tabulated in Table 4; the b generators in Tables 5, 6, 7. The minimal polynomials of the cubic b generators are tabulated in Table 8. The fields in the tower of Eq. (14) are tabulated in Table 9, for both the maximal and the minimal and intermediate multiplets in each dimension.

Information regarding the Galois group is tabulated dimension by dimension, in a series of boxes. Let $\mathbb{Q} \lhd \mathbb{E}_c \lhd \mathbb{E}_0 \lhd \mathbb{E}_1 \lhd \mathbb{E}$ be the tower for the maximal multiplet in dimension d. The first box specifies the action of the generators of $\text{Gal}(\mathbb{E}/\mathbb{Q})$. The generators are denoted g_a, $g_1, \dots, g_m$, $\bar{g}_1$ and are chosen so that

(1) g_a is an order 2 extension of the non-trivial element of $\text{Gal}(\mathbb{E}_c/\mathbb{Q})$.
(2) $g_1, \dots, g_m, \bar{g}_1$ fix $\mathbb{E}_c$. In particular, they are mutually commuting. Moreover

$$\text{Gal}(\mathbb{E}/\mathbb{E}_c) = \langle g_1 \rangle \oplus \cdots \oplus \langle g_m \rangle \oplus \langle \bar{g}_1 \rangle \tag{70}$$

(3) $\bar{g}_1$ is the non-trivial element of $\text{Gal}(\mathbb{E}/\mathbb{E}_1)$.
(4) Complex conjugation is given by $g_c = g_a \bar{g}_1 g_a$ (*c.f.* Eq. (15)).

For each generator h, Box 1 also tabulates the order of h, and $g_a h g_a$. In view of Eq. (70) it therefore completely specifies $\text{Gal}(\mathbb{E}/\mathbb{Q})$. Box 2 specifies $\text{Gal}(\mathbb{E}/\mathbb{Q})$ and its various subgroups for every multiplet in dimension d. It also specifies how the Galois group switches between the different $\text{EC}(d)$ orbits in a multiplet. Finally, we tabulate the G matrices defined by Eq. (21). In dimension d let dx, dy be two $\text{EC}(d)$ orbits such that generator g_j takes dx to dy, and let Π_x, Π_y be the exact fiducials on these orbits given in ref. [32]. Then

$$g_j\big(\text{Tr}(D_{\mathbf{p}}\Pi_x)\big) = \text{Tr}(D_{G_{xj}\mathbf{p}}\Pi_y) \tag{71}$$

where G_{xj} are the matrices tabulated in box 3. We only tabulate the matrices for cases where the action is non-trivial, so that $g_j(\Pi_x) \neq \Pi_x$. The F matrices in Eq. (20) can then be obtained by inverting Eq. (22).

d	a	r_1	r_2	r_3	r_4	ir_3	t	minimal polynomial of t over $\mathbb{Q}(a, r_1, \ldots, r_j)$
15	$\sqrt{3}$	$\sqrt{5}$					$\cos\frac{\pi}{15}$	$8x^2 - 2(r_1 - 1)x - (r_1 + 3)$
17	$\sqrt{7}$	$\sqrt{3}$	$\sqrt{17}$				$\sin\frac{\pi}{17}$	$x^8 + \frac{1}{8}(r_2 - 17)x^6 - \frac{1}{32}(7r_2 - 51)x^4 + \frac{1}{64}(7r_2 - 34)x^2 - \frac{1}{256}(4r_2 - 17)$
18	$\sqrt{285}$	$\sqrt{5}$	$\sqrt{3}$				$\cos\frac{\pi}{18}$	$x^3 - \frac{3}{4}x - \frac{1}{8}r_2$
19	$\sqrt{5}$	$\sqrt{19}$	$\sqrt{2}$				$\cos\frac{\pi}{19}$	$512x^9 - 256x^8 - 1024x^7 + 448x^6 + 672x^5 - 240x^4 - 160x^3 + 40x^2 + 10x - 1$
20	$\sqrt{357}$	$\sqrt{17}$	$\sqrt{3}$	$\sqrt{6}$	$\sqrt{5}$		$\cos\frac{\pi}{20}$	$x^2 - \frac{1}{12}r_2r_3(r_4 + 1)x + \frac{1}{8}(r_4 - 1)$
21	$\sqrt{11}$	$\sqrt{3}$	$\sqrt{7}$				$\cos\frac{\pi}{21}$	$x^3 - \frac{1}{4}(r_1r_2 - 1)x^2 - \frac{1}{8}(r_1r_2 + 1)x + \frac{1}{16}(r_1r_2 + 5)$
24	$\sqrt{21}$	$\sqrt{2}$	$\sqrt{3}$	$\sqrt{5}$			$\cos\frac{\pi}{24}$	$8x^2 - (4 + r_1 + r_1r_2)$
28	$\sqrt{29}$	$\sqrt{2}$	$\sqrt{7}$	$\sqrt{5}$			$\cos\frac{\pi}{28}$	$16x^3 - 4r_1(r_2 - 1)x^2 - 4(r_2 + 1)x + r_1(r_2 + 3)$
30	$\sqrt{93}$	$\sqrt{3}$	$\sqrt{5}$				$\cos\frac{\pi}{30}$	$8x^2 - 2r_1(r_2 + 1)x + r_2 + 1$
35	$\sqrt{2}$	$\sqrt{5}$	$\sqrt{7}$	$\sqrt{3}$				
39	$\sqrt{10}$	$\sqrt{20}$	$\sqrt{13}$			$i\sqrt{3}$		
48	$\sqrt{5}$	$\sqrt{2}$	$\sqrt{3}$	$\sqrt{105}$			$\cos\frac{\pi}{48}$	$32x^4 - 32x^2 + (4 - r_1 - r_1r_2)$

TABLE 4. a, r and t generators

	$d=15$	$d=17$	$d=18$	$d=19$
b_1	$i\big(-30+28a-6r_1+4ar_1+(-60+24a-12r_1+8ar_1)t\big)^{\frac{1}{2}}$	$32i\big(-1938+765a+462r_2-181ar_2-2(171-72a-67r_2+32ar_2)t+2(5844-2303a-1404r_2+551ar_2)t^2+4(173-64a-229r_2+112ar_2)t^3-8(2592-1021a-624r_2+245ar_2)t^4-16(-39+24a-113r_2+56ar_2)t^5+32(348-137a-84r_2+33ar_2)t^6+512(-2+a)(1+r_2)t^7\big)^{\frac{1}{2}}$	$i\big((a+15)(r_1+5)\big)^{\frac{1}{2}}$	$i(2a+1)^{\frac{1}{2}}$
b_2	$2\,\mathrm{Re}\Big(\big(10+30i\big)^{\frac{1}{3}}\Big)$	$2\,\mathrm{Re}\Big(\big(17(44+3i\sqrt{21})\big)^{\frac{1}{3}}\Big)$	$2\,\mathrm{Re}\Big(\big(-11+i\sqrt{95}\big)^{\frac{1}{3}}\Big)$	$2\,\mathrm{Re}\Big(\big(38(13+3i\sqrt{5})\big)^{\frac{1}{3}}\Big)$
b_3	$i\sqrt{2a}$		$2\,\mathrm{Re}\Big(\big(\tfrac{3}{2}(1+i\sqrt{95})\big)^{\frac{1}{3}}\Big)$	
b_4	$\sqrt{a+2}$			

TABLE 5. b generators for $d=15$, 17–19

	$d=20$	$d=21$	$d=24$	$d=28$
b_1	$i\big((a+17)(r_1+17)\big)^{\frac{1}{2}}$	$(9+4r_1)^{\frac{1}{2}}$	$i\sqrt{a-3}$	$i\sqrt{a+1}$
b_2	$2\,\mathrm{Re}\Big(\big(10(19+i9\sqrt{119})\big)^{\frac{1}{3}}\Big)$	$i\big(-33+66a-22r_1+33ar_1-(11+8a+5ar_1)b_1\big)^{\frac{1}{2}}$	$\sqrt{(4+r_1)(3+r_2)}$	$i\sqrt{a+5}$
b_3	$\Big(\frac{1}{3}\Big(((a+39)r_3r_4+(7a+21)r_3\big)t-\big((2a+15)r_2-3a\big)r_4-3(a+18)r_2+195\Big)^{\frac{1}{2}}$	$\big(363-66a+66r_1-33ar_1+(55-24a+7ar_1)b_1\big)^{\frac{1}{2}}$	$4\,\mathrm{Re}\Big(\big(1+i\sqrt{7}\big)^{\frac{1}{3}}\Big)$	$2\,\mathrm{Re}\Big(\big(189+21i\sqrt{87}\big)^{\frac{1}{3}}\Big)$
b_4		$\mathrm{Re}\Big(\big(4(-4-9a+i\sqrt{465-72a})\big)^{\frac{1}{3}}\Big)$	$i\sqrt{(a+1)(r_3+5)}$	$i\sqrt{20a+50+(6a+36)r_3}$

TABLE 6. b generators for $d=20$, 21, 24, 28

	$d=30$	$d=35$	$d=39$	$d=48$
b_1	$\frac{1}{2}\big(4(-5r_1r_2+(4a-23)r_1)t+2((-4a+21)r_2-8a+111)\big)^{\frac{1}{2}}$	$i\sqrt{2a+1}$	$\sqrt{3r_1+18}$	$i\sqrt{a-1}$
b_2	$2\,\mathrm{Re}\big((1+2i\sqrt{31})^{\frac{1}{3}}\big)$	$2\,\mathrm{Re}\big((280+210i\sqrt{6})^{\frac{1}{3}}\big)$	$\sqrt{18r_2+78}$	$\sqrt{6+r_1r_2}$
b_3	$2\,\mathrm{Re}\Big(\big(4+b_2+i\sqrt{48-8b_2-b_2^2}\big)^{\frac{1}{3}}\Big)$	$\sqrt{14(r_1+5)}$	$\sqrt{(4a+15)(r_1+5)}$	$\sqrt{6-2r_1r_2+(r_2-r_1)b_2}$
b_4	$2\,\mathrm{Re}\Big(\big(70+10i\sqrt{31}\big)^{\frac{1}{3}}\Big)$	$\mathrm{Re}\Big(\big(28+84i\sqrt{3}\big)^{\frac{1}{3}}\Big)$	$\big((2a-5)(r_1-2)b_3-(8a-35)(r_1-10)\big)^{\frac{1}{2}}$	$\sqrt{2r_3+42}$
b_5	$\frac{i}{2}\sqrt{2a+18}$	$\sqrt{3-r_3}$	$\mathrm{Re}\big((-676+10140i\sqrt{3})^{\frac{1}{3}}\big)$	$\big((5(a+1)-(3a-5)r_3)b_4-2(a+5)r_3+210(3-a)\big)^{\frac{1}{2}}$
b_6		$\frac{i}{7}\sqrt{245a-7r_2b_3-49ar_1}$	$\mathrm{Re}\big((180-4a+4i\sqrt{6753+90a})^{\frac{1}{3}}\big)$	$2\,\mathrm{Re}\big((7+i\sqrt{15})^{\frac{1}{3}}\big)$
b_7			$i\sqrt{6a-3}$	

TABLE 7. b generators for $d=30$, 35, 39, 48

d	generator	in terms of radicals	minimal polynomial
15	b_2	$2\,\mathrm{Re}\Big(\big(10+30i\big)\big)^{\frac{1}{3}}\Big)$	$x^3-30x-20$
17	b_2	$2\,\mathrm{Re}\Big(\big(17(44+3i\sqrt{21})\big)^{\frac{1}{3}}\Big)$	$x^3-255x-1496$
18	b_2	$2\,\mathrm{Re}\Big(\big(-11+i\sqrt{95}\big)^{\frac{1}{3}}\Big)$	$x^3-18x+22$
	b_3	$2\,\mathrm{Re}\Big(\big(\frac{3}{2}(1+i\sqrt{95})\big)^{\frac{1}{3}}\Big)$	$x^3-18x-3$
19	b_2	$\mathrm{Re}\Big(\big(38(13+3i\sqrt{5})\big)^{\frac{1}{3}}\Big)$	$x^3-228x-988$
20	b_2	$2\,\mathrm{Re}\Big(\big(10(19+9i\sqrt{119})\big)^{\frac{1}{3}}\Big)$	$x^3-300x-380$
21	b_4	$\mathrm{Re}\Big(\big(4(-4-9a+i\sqrt{465-72a})\big)^{\frac{1}{3}}\Big)$	$x^3-21x+9a+4$
24	b_3	$4\,\mathrm{Re}\Big(\big(1+i\sqrt{7}\big)^{\frac{1}{3}}\Big)$	$x^3-24x-16$
28	b_3	$2\,\mathrm{Re}\Big(\big(189+21i\sqrt{87}\big)^{\frac{1}{3}}\Big)$	$x^3-126x-378$
30	b_2	$2\,\mathrm{Re}\big((1+2i\sqrt{31})^{\frac{1}{3}}\big)$	$x^3-15x-2$
	b_3	$2\,\mathrm{Re}\Big(\big(4+b_2+i\sqrt{48-8b_2-b_2^2}\big)^{\frac{1}{3}}\Big)$	$x^3-12x-2b_2-8$
	b_4	$2\,\mathrm{Re}\Big(\big(70+10i\sqrt{31}\big)^{\frac{1}{3}}\Big)$	$x^3-60x-140$
35	b_2	$2\,\mathrm{Re}\big((280+210i\sqrt{6})^{\frac{1}{3}}\big)$	$x^3-210x-560$
	b_4	$\mathrm{Re}\Big(\big(28+84i\sqrt{3}\big)^{\frac{1}{3}}\Big)$	$x^3-21x-7$
39	b_5	$\mathrm{Re}\big((-676+10140i\sqrt{3})^{\frac{1}{3}}\big)$	$x^3-507x+169$
	b_6	$\mathrm{Re}\big((180-4a+4i\sqrt{6753+90a})^{\frac{1}{3}}\big)$	$x^3-39x+a-45$
48	b_6	$2\,\mathrm{Re}\big((7+i\sqrt{15})^{\frac{1}{3}}\big)$	$x^3-12x-14$

TABLE 8. Minimal polynomials for cubic b generators

multiplet	$\mathbb{E}_0$	$\mathbb{E}_1$	$\mathbb{E}$	$\deg(\mathbb{E}/\mathbb{Q})$
$15ac$	$\mathbb{Q}(a, b_4)$	$\mathbb{E}_0(r_1, t, b_1, b_2, b_3)$	$\mathbb{E}_1(i)$	384
$15b$	$\mathbb{Q}(a)$	$\mathbb{E}_0(r_1, t, b_1, b_2, b_3)$	$\mathbb{E}_1(i)$	192
$15d$	$\mathbb{Q}(a)$	$\mathbb{E}_0(r_1, t, b_1, b_2)$	$\mathbb{E}_1(i)$	96
$17ab$	$\mathbb{Q}(a, r_1)$	$\mathbb{E}_0(r_2, t, b_1, b_2)$	$\mathbb{E}_1(i)$	768
$17c$	$\mathbb{Q}(a)$	$\mathbb{E}_0(r_2, t, b_1, b_2)$	$\mathbb{E}_1(i)$	384
$18ab$	$\mathbb{Q}(a, r_1)$	$\mathbb{E}_0(r_2, t, b_1, b_2, b_3)$	$\mathbb{E}_1(i)$	864
$19bc$	$\mathbb{Q}(a, r_2)$	$\mathbb{E}_0(r_1, t, b_1, b_2)$	$\mathbb{E}(i)$	864
$19a$	$\mathbb{Q}(a)$	$\mathbb{E}_0(r_1, t, b_1, b_2)$	$\mathbb{E}_1(i)$	432
$19d$	$\mathbb{Q}(a)$	$\mathbb{E}_0(t, b_1, b_2)$	$\mathbb{E}(ir_1)$	216
$19e$	$\mathbb{Q}(a)$	$\mathbb{E}_0(t, b_1)$	$\mathbb{E}(ir_1)$	72
$20ab$	$\mathbb{Q}(a, r_1)$	$\mathbb{E}_0(r_2, r_3, r_4, t, b_1, b_2, b_3)$	$\mathbb{E}_1(i)$	1536
$21abcd$	$\mathbb{Q}(a, r_1, b_1)$	$\mathbb{E}_0(r_2, t, b_2, b_3, b_4)$	$\mathbb{E}_1(i)$	1152
$21e$	$\mathbb{Q}(a)$	$\mathbb{E}_0(r_1, r_2, t, b_1, b_2, b_3)$	$\mathbb{E}_1(i)$	384
$24ab$	$\mathbb{Q}(a, r_3)$	$\mathbb{E}_0(r_1, r_2, t, b_1, b_2, b_3, b_4)$	$\mathbb{E}_1(i)$	1536
$24c$	$\mathbb{Q}(a)$	$\mathbb{E}_0(r_1, r_2, t, b_1, b_2, b_3)$	$\mathbb{E}_1(i)$	384
$28ab$	$\mathbb{Q}(a, r_3)$	$\mathbb{E}_0(r_1, r_2, t, , b_1, b_2, b_3, b_4)$	$\mathbb{E}_1(i)$	2304
$28c$	$\mathbb{Q}(a)$	$\mathbb{E}_0(r_1, r_2, t, , b_1, b_2, b_3)$	$\mathbb{E}_1(i)$	576
$30abc$	$\mathbb{Q}(a, b_2)$	$\mathbb{E}_0(r_1, r_2, t, b_1, b_3, b_4, b_5)$	$\mathbb{E}_1(i)$	3456
$30d$	$\mathbb{Q}(a)$	$\mathbb{E}_0(r_1, r_2, t, b_1, b_2, b_4, b_5)$	$\mathbb{E}_1(i)$	1152
$35bcdg$	$\mathbb{Q}(a, r_3, b_5)$	$\mathbb{E}_0(r_1, r_2, b_1, b_2, b_3, b_4, b_6)$	$\mathbb{E}_1(i)$	4608
$35af$	$\mathbb{Q}(a, r_3)$	$\mathbb{E}_0(r_1, r_2, b_1, b_2, b_3, b_4, b_5b_6)$	$\mathbb{E}_1(i)$	2304
$35e$	$\mathbb{Q}(a)$	$\mathbb{E}_0(r_1, r_2r_3, b_1, b_2, b_3, b_4, c)$	$\mathbb{E}_1(ir_2)$	1152
$35h$	$\mathbb{Q}(a)$	$\mathbb{E}_0(r_1, r_2, b_1, b_2, b_3, b_4, b_6)$	$\mathbb{E}_1(i)$	1152
$35i$	$\mathbb{Q}(a)$	$\mathbb{E}_0(r_1, r_2, b_1, b_2, b_3, b_4)$	$\mathbb{E}_1(i)$	576
$35j$	$\mathbb{Q}(a)$	$\mathbb{E}_0(r_1, b_1, b_2, b_3, b_4)$	$\mathbb{E}_1(ir_2)$	288
$39acde$	$\mathbb{Q}(a, r_1, b_1)$	$\mathbb{E}_0(r_2, b_2, b_3, b_4, b_5, b_6, b_7)$	$\mathbb{E}(ir_3)$	4608
$39bf$	$\mathbb{Q}(a, r_1)$	$\mathbb{E}_0(r_2, b_2, b_3, b_4, b_5, b_6, b_7)$	$\mathbb{E}(ir_3)$	2304
$39gh$	$\mathbb{Q}(a, r_1)$	$\mathbb{E}_0(r_2, b_1, b_2, b_3, b_4, b_5, b_7)$	$\mathbb{E}(ir_3)$	1536
$39ij$	$\mathbb{Q}(a, r_1)$	$\mathbb{E}_0(r_2, b_2, b_3, b_4, b_5, b_7)$	$\mathbb{E}(ir_3)$	768
$48abcd$	$\mathbb{Q}(a, r_3, b_4)$	$\mathbb{E}_0(r_1, r_2, t, b_1, b_2, b_3, b_5, b_6)$	$\mathbb{E}_1(i)$	12288
$48e$	$\mathbb{Q}(a)$	$\mathbb{E}_0(r_1, r_2, r_3, t, b_1, b_2, b_3, b_4, b_5)$	$\mathbb{E}_1(i)$	4096
$48f$	$\mathbb{Q}(a)$	$\mathbb{E}_0(r_1, r_2, t, b_1, b_2, b_3, b_6)$	$\mathbb{E}_1(i)$	1536
$48g$	$\mathbb{Q}(a)$	$\mathbb{E}_0(r_1, r_2, t, b_1, b_2, b_3)$	$\mathbb{E}_1(i)$	512

TABLE 9. Fields. The exact fiducials for orbits $15d$, $19e$, $24c$, $28c$, $35j$, $48g$ were calculated by Scott and Grassl [13]. They are included here for the sake of comparison.The generator c in the field for $35e$ is given by $c = (r_2(ar_1 + r_3 + 2a + 1)b_3 + 42r_1 + 70)b_5b_6$.

Dimension 15

1.

h	a	r_1	t	b_1	b_2	b_3	b_4	i	order	$g_a h g_a^{-1}$
g_a	$-a$	r_1	t	b_1'	b_2	b_3'	b_4'	$-i$	2	g_a
g_1	a	r_1	t	b_1	b_2	b_3	$-b_4$	i	2	g_1
g_2	a	$-r_1$	t'	b_1''	b_2'	b_3	b_4	i	24	g_2^5
g_3	a	r_1	t	b_1	b_2	$-b_3$	b_4	i	2	g_3
$\bar{g}_1$	a	r_1	t	b_1	b_2	b_3	b_4	$-i$	2	$g_c = g_2^{12} g_3 \bar{g}_1$

$t' = \cos\frac{7\pi}{15}$

$b_1' = \sqrt{30 + 28a + 6r_1 + 4ar_1 + (60 + 24a + 12r_1 + 8ar_1)t}$

$b_1'' = i\sqrt{16a + (60 - 32a - 36r_1 + 16ar_1)t}$

$b_2' = 2\,\mathrm{Re}\Big(e^{\frac{2\pi i}{3}}(10 + 30i)^{\frac{1}{3}}\Big)$

$b_3' = \sqrt{2a}$

$b_4' = \sqrt{-a + 2}$

2.

orbit	$\mathrm{Gal}(\mathbb{E}/\mathbb{Q})$	$\mathrm{Gal}(\mathbb{E}/\mathbb{E}_0)$
$15ac$	$\langle g_a, g_1, g_2, g_3, \bar{g}_1\rangle$	$\langle g_2, g_3, \bar{g}_1\rangle$
$15b$	$\langle g_a, g_2, g_3, \bar{g}_1\rangle$	$\langle g_2, g_3, \bar{g}_1\rangle$
$15d$	$\langle g_a, g_2, \bar{g}_1\rangle$	$\langle g_2, \bar{g}_1\rangle$

g_1 interchanges $15a$, $15c$ and restricts to the identity on $15b$, $15d$; g_3 restricts to the identity on $15d$

3.

$G_{a1} = G_{c1}$	$G_{a2} = G_{b2}$	$G_{c2} = G_{d2}$	$G_{a3} = G_{b3} = G_{c3}$
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 12 \\ 3 & 13 \end{pmatrix}$	$\begin{pmatrix} 3 & 14 \\ 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 0 & 4 \\ 11 & 4 \end{pmatrix}$

Dimension 17

1.

h	a	r_1	r_2	t	b_1	b_2	i	order	$g_a h g_a^{-1}$
g_a	$-a$	r_1	r_2	t	b_1'	b_2	i	2	g_a
g_1	a	$-r_1$	r_2	t	b_1	b_2	i	2	g_1
g_2	a	r_1	$-r_2$	t'	b_1''	b_2'	i	96	g_2^{17}
$\bar{g}_1$	a	r_1	r_2	t	b_1	b_2	$-i$	2	$g_c = g_2^{48}\bar{g}_1$

$t' = \sin\frac{20\pi}{17}$

$b_1' = 32\Big(1938+765a-462r_2-181ar_2-2(-171-72a+67r_2+32ar_2)t2(-5844-2303a+1404r_2+551ar_2)t^2+4(-173-64a+229r_2+112ar_2)t^3-8(-2592-1021a+624r_2+245ar_2)t^4-16(39+24a+113r_2+56ar_2)t^5+32(-348-137a+84r_2+33ar_2)t^6+512(2+a)(1+r_2)t^7\Big)^{\frac{1}{2}}$

$b_1'' = 32i\Big(\frac{1}{2}(-204+119a+60r_2-33ar_2)-8(-39+20a-3r_2)t+16(-81+25a-39r_2+17ar_2)t^2+4(-491+240a-51r_2)t^3-8(-600+211a-216r_2+91ar_2)t^4-16(-243+112a-27r_2)t^5+96(-36+13a-12r_2+5ar_2)t^6+256(-9+4a-r_2)t^7\Big)^{\frac{1}{2}}$

$b_2' = 2\,\mathrm{Re}\Big(e^{\frac{4\pi i}{3}}\big(17(44+3i\sqrt{21})\big)^{\frac{1}{3}}\Big)$

2.

orbit	$\mathrm{Gal}(\mathbb{E}/\mathbb{Q})$	$\mathrm{Gal}(\mathbb{E}/\mathbb{E}_0)$
$17ab$	$\langle g_a, g_1, g_2, \bar{g}_1\rangle$	$\langle g_2, \bar{g}_1\rangle$
$17c$	$\langle g_a, g_2, \bar{g}_1\rangle$	$\langle g_2, \bar{g}_1\rangle$

g_1 interchanges orbits $17a$, $17b$ and restricts to the identity on $17c$.

3.

G_{a1}	G_{b1}	G_{a2}	G_{b2}	G_{c2}
$\begin{pmatrix}2 & 7\\ 9 & 15\end{pmatrix}$	$\begin{pmatrix}15 & 10\\ 8 & 2\end{pmatrix}$	$\begin{pmatrix}1 & 11\\ 6 & 12\end{pmatrix}$	$\begin{pmatrix}6 & 16\\ 1 & 5\end{pmatrix}$	$\begin{pmatrix}1 & 11\\ 6 & 12\end{pmatrix}$

Dimension 18

1.

h	a	r_1	r_2	t	b_1	b_2	b_3	i	order	$g_a h g_a^{-1}$
g_a	$-a$	r_1	r_2	t	b_1'	b_2	b_3	i	2	g_a
g_1	a	$-r_1$	r_2	t	b_1''	b_2	b_3'	i	12	g_1^{11}
g_2	a	r_1	$-r_2$	$-t$	b_1	b_2'	b_3	i	6	$g_1^6 g_2^5$
g_3	a	r_1	r_2	t'	b_1	b_2	b_3	i	3	g_3
$\bar{g}_1$	a	r_1	r_2	t	b_1	b_2	b_3	$-i$	2	$g_c = g_1^3\bar{g}_1$

$t' = \cos\frac{11\pi}{18}$

$b_1' = -\big((a-15)(5+r_1)\big)^{\frac{1}{2}}$

$b_1'' = i\big(a+15)(5-r_1)\big)^{\frac{1}{2}}$

$b_2' = 2\,\mathrm{Re}\Big(e^{\frac{4\pi i}{3}}\big(-11+i\sqrt{95}\big)^{\frac{1}{3}}\Big)$

$b_3' = 2\,\mathrm{Re}\Big(e^{\frac{4\pi i}{3}}\big(\frac{3}{2}(1+i\sqrt{95})^{\frac{1}{3}}\big)\Big)$

2.

orbit	Gal($\mathbb{E}/\mathbb{Q}$)	Gal($\mathbb{E}/\mathbb{E}_0$)
$18ab$	$\langle g_a, g_1, g_2, g_3, \bar{g}_1\rangle$	$\langle g_1^2, g_2, g_3, \bar{g}_1\rangle$

g_1 interchanges orbits $18a$, $18b$.

3.

G_{a1}	G_{b1}	G_{a2}	G_{b2}	G_{a3}, G_{b3}
$\begin{pmatrix}1 & 8\\ 9 & 35\end{pmatrix}$	$\begin{pmatrix}4 & 3\\ 7 & 32\end{pmatrix}$	$\begin{pmatrix}9 & 17\\ 19 & 26\end{pmatrix}$	$\begin{pmatrix}1 & 9\\ 27 & 10\end{pmatrix}$	$\begin{pmatrix}0 & 5\\ 31 & 5\end{pmatrix}$

Dimension 19

1.

h	a	r_1	r_2	t	b_1	b_2	ir_1	order	$g_a h g_a^{-1}$
g_a	$-a$	r_1	r_2	t	b_1'	b_2	ir_1	2	g_a
g_1	a	r_1	$-r_2$	t	b_1	b_2	ir_1	2	g_1
g_2	a	r_1	r_2	t'	$-b_1$	b_2	ir_1	18	g_2
g_3	a	r_1	r_2	t	b_1	b_2'	ir_1	3	g_3^2
g_4	a	$-r_1$	r_2	t	b_1	b_2	ir_1	2	g_4
$\bar{g}_1$	a	r_1	r_2	t	b_1	b_2	$-ir_1$	2	$g_c = g_2^9\bar{g}_1$

$t' = \cos\frac{3\pi}{19}$

$b_1' = (2a-1)^{\frac{1}{2}}$

$b_2' = 2\,\mathrm{Re}\Big(e^{\frac{4\pi i}{3}}\big(38(13+3i\sqrt{5})\big)^{\frac{1}{3}}\Big)$

2.

orbit	Gal($\mathbb{E}/\mathbb{Q}$)	Gal($\mathbb{E}/\mathbb{E}_0$)
$19bc$	$\langle g_a, g_1, g_2, g_3, g_4, \bar{g}_1\rangle$	$\langle g_2, g_3, g_4, \bar{g}_1\rangle$
$19a$	$\langle g_a, g_2, g_3, g_4, \bar{g}_1\rangle$	$\langle g_2, g_3, g_4, \bar{g}_1\rangle$
$19d$	$\langle g_a, g_2, g_3, \bar{g}_1\rangle$	$\langle g_2, g_3, \bar{g}_1\rangle$
$19e$	$\langle g_a, g_2, \bar{g}_1\rangle$	$\langle g_2, \bar{g}_1\rangle$

g_1 interchanges orbits $19b$, $19c$ and restricts to the identity on $19a$, $19d$, $19e$. g_3 restricts to the identity on $19e$; g_4 restricts to the identity on $19d$, $19e$.

3.

G_{b1}	G_{c1}	G_{a2}, G_{b2}, G_{c2}, G_{d2}, G_{e2}	G_{a3}	G_{b3}, G_{c3}	G_{d3}	G_{a4}	G_{b4}, G_{c4}
$\begin{pmatrix}2 & 5\\ 14 & 7\end{pmatrix}$	$\begin{pmatrix}7 & 14\\ 5 & 2\end{pmatrix}$	$\begin{pmatrix}15 & 0\\ 0 & 15\end{pmatrix}$	$\begin{pmatrix}7 & 14\\ 5 & 2\end{pmatrix}$	$\begin{pmatrix}2 & 5\\ 14 & 7\end{pmatrix}$	$\begin{pmatrix}7 & 14\\ 5 & 2\end{pmatrix}$	$\begin{pmatrix}10 & 14\\ 5 & 5\end{pmatrix}$	$\begin{pmatrix}5 & 5\\ 14 & 10\end{pmatrix}$

Dimension 20

1.

h	a	r_1	r_2	r_3	r_4	t	b_1	b_2	b_3	i	order	$g_a h g_a^{-1}$
g_a	$-a$	r_1	r_2	r_3	r_4	t	b_1'	b_2	b_3'	i	2	g_a
g_1	a	$-r_1$	r_2	r_3	r_4	t	b_1''	b_2	b_3	i	4	g_1^3
g_2	a	r_1	r_2	r_3	$-r_4$	t'	b_1	b_2'	b_3''	i	24	g_2^5
g_3	a	r_1	$-r_2$	r_3	r_4	t''	b_1	b_2	b_3	i	2	$g_2^{12} g_3$
g_4	a	r_1	r_2	$-r_3$	r_4	$-t$	b_1	b_2	b_3	i	2	g_4
$\bar{g}_1$	a	r_1	r_2	r_3	r_4	t	b_1	b_2	b_3	$-i$	2	$g_c = g_1^2 \bar{g}_1$

$$t' = \cos\tfrac{17\pi}{20}$$

$$t'' = \cos\tfrac{11\pi}{20}$$

$$b_1' = \big((a-17)(17+r_1)\big)^{\frac{1}{2}}$$

$$b_1'' = i\big((a+17)(17-r_1)\big)^{\frac{1}{2}}$$

$$b_2' = 2\,\mathrm{Re}\big(10e^{\frac{2\pi i}{3}}(19+i\sqrt{119})^{\frac{1}{3}}\big)$$

$$b_3' = \Big(\tfrac{1}{3}\Big(\big((-a+39)r_3r_4 + (-7a+21)r_3\big)t - \big((-2a+15)r_2 + 3a\big)r_4 - 3(-a+18)r_2 + 195\Big)\Big)^{\frac{1}{2}}$$

$$b_3'' = -\Big(\tfrac{1}{3}\Big(\big(-(a+39)r_3r_4 + (7a+21)r_3\big)t' + \big((2a+15)r_2 - 3a\big)r_4 - 3(a+18)r_2 + 195\Big)\Big)^{\frac{1}{2}}$$

2.

orbit	$\mathrm{Gal}(\mathbb{E}/\mathbb{Q})$	$\mathrm{Gal}(\mathbb{E}/\mathbb{E}_0)$
$20ab$	$\langle g_a, g_1, g_2, g_3, g_4, \bar{g}_1\rangle$	$\langle g_1^2, g_2, g_3, g_4, \bar{g}_1\rangle$

g_1 interchanges orbits $20a$, $20b$.

3.

G_{a1}	G_{b1}	G_{a2}, G_{b2}	G_{a3}, G_{b3}	G_{a4}, G_{b4}
$\begin{pmatrix}1 & 24\\ 16 & 25\end{pmatrix}$	$\begin{pmatrix}15 & 24\\ 16 & 39\end{pmatrix}$	$\begin{pmatrix}1 & 32\\ 8 & 33\end{pmatrix}$	$\begin{pmatrix}10 & 31\\ 9 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 20\\ 20 & 21\end{pmatrix}$

Dimension 21

1.

h	a	r_1	r_2	t	b_1	b_2	b_3	b_4	i	order	$g_a h g_a^{-1}$
g_a	$-a$	r_1	r_2	t	b_1	b_2'	b_3'	b_4'	i	2	g_a
g_1	a	$-r_1$	r_2	t'	b_1'	b_2''	b_3''	b_4	i	24	$g_1^{19} g_4^2$
g_2	a	r_1	$-r_2$	t''	b_1	b_2	b_3	b_4	i	2	$g_2 g_3$
g_3	a	r_1	r_2	t	b_1	b_2	$-b_3$	b_4	i	2	g_3
g_4	a	r_1	r_2	t	b_1	b_2	b_3	b_4''	i	2	g_4^2
$\bar{g}_1$	a	r_1	r_2	t	b_1	b_2	b_3	b_4	$-i$	2	$g_c = g_1^{12} g_3 \bar{g}_1$

$$t' = \cos \tfrac{19\pi}{21}$$

$$t'' = \cos \tfrac{13\pi}{21}$$

$$b_1' = -(9 - 4r_1)^{\frac{1}{2}}$$

$$b_2' = -\big(33 + 66a + 22r_1 + 33ar_1 + (11 - 8a - 5ar_1)b_1\big)^{\frac{1}{2}}$$

$$b_2'' = i\big(-33 + 66a + 22r_1 - 33ar_1 - (77 + 4a - 44r_1 - 3ar_1)b_1\big)^{\frac{1}{2}}$$

$$b_3' = \big(363 + 66a + 66r_1 + 33ar_1 + (55 + 24a - 7ar_1)b_1\big)^{\frac{1}{2}}$$

$$b_3'' = -\big(363 - 66a - 66r_1 + 33ar_1 - (33 - 20a - 44r_1 + 15ar_1)b_1\big)^{\frac{1}{2}}$$

$$b_4' = \mathrm{Re}\Big(e^{\frac{4\pi i}{3}}\big(4(-4 + 9a + i\sqrt{465 + 72a})\big)^{\frac{1}{3}}\Big)$$

$$b_4'' = \mathrm{Re}\Big(e^{\frac{2\pi i}{3}}\big(4(-4 - 9a + i\sqrt{465 - 72a})\big)^{\frac{1}{3}}\Big)$$

2.

orbit	$\mathrm{Gal}(\mathbb{E}/\mathbb{Q})$	$\mathrm{Gal}(\mathbb{E}/\mathbb{E}_0)$
$21abcd$	$\langle g_a, g_1, g_2, g_3, g_4, \bar{g}_1 \rangle$	$\langle g_1^4, g_2, g_3, g_4, \bar{g}_1 \rangle$
$21e$	$\langle g_a, g_1, g_2, g_3, \bar{g}_1 \rangle$	$\langle g_1, g_2, g_3, \bar{g}_1 \rangle$

g_1 cycles orbits $21abcd$ in the order $21a \to 21d \to 21b \to 21c \to 21a \to \ldots$; g_4 restricts to the identity on $21e$.

3.

G_{a1}	G_{b1}	G_{c1}	G_{d1}	G_{e1}	G_{a2}, G_{b2}, G_{c2}, G_{d2}	G_{e2}	$G_{a3}, G_{b3}, G_{c3}, G_{d3}$	G_{e3}	G_{a4}, G_{b4}, G_{c4}, G_{d4}
$\begin{pmatrix} 2 & 9 \\ 12 & 11 \end{pmatrix}$	$\begin{pmatrix} 11 & 12 \\ 9 & 2 \end{pmatrix}$	$\begin{pmatrix} 2 & 3 \\ 18 & 5 \end{pmatrix}$	$\begin{pmatrix} 11 & 19 \\ 2 & 9 \end{pmatrix}$	$\begin{pmatrix} 4 & 7 \\ 7 & 18 \end{pmatrix}$	$\begin{pmatrix} 10 & 15 \\ 6 & 4 \end{pmatrix}$	$\begin{pmatrix} 7 & 9 \\ 18 & 19 \end{pmatrix}$	$\begin{pmatrix} 0 & 8 \\ 13 & 8 \end{pmatrix}$	$\begin{pmatrix} 13 & 0 \\ 0 & 13 \end{pmatrix}$	$\begin{pmatrix} 6 & 8 \\ 13 & 14 \end{pmatrix}$

Dimension 24

1.

h	a	r_1	r_2	r_3	t	b_1	b_2	b_3	b_4	i	order	$g_a h g_a^{-1}$
g_a	$-a$	r_1	r_2	r_3	t	b_1'	b_2	b_3	b_4'	i	2	g_a
g_1	a	r_1	r_2	$-r_3$	t	b_1	b_2	b_3	b_4''	i	4	g_1^3
g_2	a	r_1	$-r_2$	r_3	t'	b_1	b_2'	b_3'	b_4	i	12	$g_2^5 g_4$
g_3	a	$-r_1$	r_2	r_3	t''	b_1	b_2''	b_3	b_4	i	4	$g_2^6 g_3$
g_4	a	r_1	r_2	r_3	t	$-b_1$	b_2	b_3	b_4	i	2	g_4
$\bar{g}_1$	a	r_1	r_2	r_3	t	b_1	b_2	b_3	b_4	$-i$	2	$g_c = g_1^2 g_4 \bar{g}_1$

$$t' = \cos\tfrac{7\pi}{24}$$

$$t'' = \cos\tfrac{11\pi}{24}$$

$$b_1' = \sqrt{a+3}$$

$$b_2' = \sqrt{(4+r_1)(3-r_2)}$$

$$b_2'' = \sqrt{(4-r_1)(3+r_2)}$$

$$b_3' = 4\,\mathrm{Re}\Big(e^{\frac{2\pi i}{3}}(1+i\sqrt{7})^{\frac{1}{3}}\Big)$$

$$b_4' = -\sqrt{(a-1)(r_3+5)}$$

$$b_4'' = i\sqrt{(a+1)(-r_3+5)}$$

2.

orbit	$\mathrm{Gal}(\mathbb{E}/\mathbb{Q})$	$\mathrm{Gal}(\mathbb{E}/\mathbb{E}_0)$
$24ab$	$\langle g_a, g_1, g_2, g_3, g_4, \bar{g}_1\rangle$	$\langle g_1^2, g_2, g_3, g_4, \bar{g}_1\rangle$
$24c$	$\langle g_a, g_2, g_3, g_4, \bar{g}_1\rangle$	$\langle g_2, g_3, g_4, \bar{g}_1\rangle$

g_1 interchanges $24a$, $24b$ and restricts to the identity on $24c$.

3.

G_{a1}	G_{b1}	G_{a2}	$G_{b2} = G_{c2}$	G_{a3}	$G_{b3} = G_{c3}$	$G_{a4} = G_{b4}$	G_{c4}
$\begin{pmatrix} 9 & 23 \\ 32 & 39 \end{pmatrix}$	$\begin{pmatrix} 3 & 5 \\ 8 & 45 \end{pmatrix}$	$\begin{pmatrix} 11 & 46 \\ 2 & 9 \end{pmatrix}$	$\begin{pmatrix} 2 & 37 \\ 11 & 39 \end{pmatrix}$	$\begin{pmatrix} 17 & 36 \\ 12 & 5 \end{pmatrix}$	$\begin{pmatrix} 5 & 12 \\ 36 & 17 \end{pmatrix}$	$\begin{pmatrix} 5 & 24 \\ 24 & 29 \end{pmatrix}$	$\begin{pmatrix} 0 & 25 \\ 23 & 25 \end{pmatrix}$

Dimension 28

1.

h	a	r_1	r_2	r_3	t	b_1	b_2	b_3	b_4	i	order	$g_a h g_a^{-1}$
g_a	$-a$	r_1	r_2	r_3	t	b_1'	b_2'	b_3	b_4'	i	2	g_a
g_1	a	r_1	r_2	$-r_3$	t	b_1	b_2	b_3	b_4''	i	4	g_1^3
g_2	a	$-r_1$	r_2	r_3	t'	b_1	b_2	b_3	b_4	i	6	g_2
g_3	a	r_1	r_2	r_3	t	b_1	$-b_2$	b_3'	b_4	i	6	g_3^5
g_4	a	r_1	$-r_2$	r_3	t''	b_1	b_2	b_3	b_4	i	2	$g_1^2 g_3^3 g_4 g_5$
g_5	a	r_1	r_2	r_3	t	$-b_1$	$-b_2$	b_3	b_4	i	2	g_5
$\bar{g}_1$	a	r_1	r_2	r_3	t	b_1	b_2	b_3	b_4	$-i$	2	$g_c = g_1^2 g_5 \bar{g}_1$

$t' = \cos \frac{3\pi}{28}$

$t'' = \cos \frac{15\pi}{28}$

$b_1' = \sqrt{a-1}$

$b_2' = \sqrt{a-5}$

$b_3' = 2\,\mathrm{Re}\Big(e^{\frac{2\pi i}{3}}\,(189 + 21i\sqrt{87})^{\frac{1}{3}}\Big)$

$b_4' = -\sqrt{20a - 50 + (6a-36)r_3}$

$b_4'' = i\sqrt{20a + 50 - (6a+36)r_3}$

2.

orbit	$\mathrm{Gal}(\mathbb{E}/\mathbb{Q})$	$\mathrm{Gal}(\mathbb{E}/\mathbb{E}_0)$
$28ab$	$\langle g_a, g_1, g_2, g_3, g_4, g_5, bar g_1\rangle$	$\langle g_1^2, g_2, g_3, g_4, g_5, \bar{g}_1\rangle$
$28c$	$\langle g_a, g_2, g_3, g_4, g_5, \bar{g}_1\rangle$	$\langle g_2, g_3, g_4, g_5, \bar{g}_1\rangle$

g_1 interchanges $28a$, $28b$ and restricts to the identity on $28c$.

3.

G_{a1}	G_{b1}	$G_{a2} = G_{b2}$	G_{c2}	$G_{a3} = G_{b3}$	G_{c3}	$G_{a4} = G_{b4}$	G_{c4}	$G_{a5} = G_{b5}$	G_{c5}
$\begin{pmatrix}17 & 50\\ 6 & 11\end{pmatrix}$	$\begin{pmatrix}0 & 29\\ 27 & 29\end{pmatrix}$	$\begin{pmatrix}13 & 30\\ 26 & 43\end{pmatrix}$	$\begin{pmatrix}9 & 19\\ 37 & 28\end{pmatrix}$	$\begin{pmatrix}8 & 49\\ 7 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 7\\ 49 & 8\end{pmatrix}$	$\begin{pmatrix}14 & 55\\ 1 & 13\end{pmatrix}$	$\begin{pmatrix}1 & 42\\ 14 & 43\end{pmatrix}$	$\begin{pmatrix}17 & 50\\ 6 & 11\end{pmatrix}$	$\begin{pmatrix}0 & 29\\ 27 & 29\end{pmatrix}$

Dimension 30

1.

h	a	r_1	r_2	t	b_1	b_2	b_3	b_4	b_5	i	order	$g_a h g_a^{-1}$
g_a	$-a$	r_1	r_2	t	b_1'	b_2	b_3	b_4	b_5'	i	2	g_a
g_1	a	r_1	r_2	t	b_1	b_2'	b_3'	b_4	b_5	i	9	g_1^8
g_2	a	r_1	$-r_2$	t'	b_1''	b_2	b_3	b_4	b_5	i	8	g_2^5
g_3	a	r_1	r_2	t	b_1	b_2	b_3	b_4'	b_5	i	3	g_3^2
g_4	a	$-r_1$	r_2	$-t$	b_1	b_2	b_3	b_4	b_5	i	2	$g_4 g_5$
g_5	a	r_1	r_2	t	b_1	b_2	b_3	b_4	$-b_5$	i	2	g_5
$\bar{g}_1$	a	r_1	r_2	t	b_1	b_2	b_3	b_4	b_5	$-i$	2	$g_5 \bar{g}_1$

$$t' = \cos \frac{23\pi}{30}$$

$$b_1' = -\frac{1}{2}\sqrt{4(-5r_1r_2 - (4a+23)r_1)t + 2((4a+21)r_2 + 8a + 111)}$$

$$b_1'' = \frac{1}{2}\sqrt{4(5r_1r_2 + (4a-23)r_1)t' + 2((4a-21)r_2 - 8a + 111)}$$

$$b_2' = 2\,\mathrm{Re}\Big(e^{\frac{2\pi i}{3}}(1 + 2i\sqrt{31})^{\frac{1}{3}}\Big)$$

$$b_3' = 2\,\mathrm{Re}\Big(e^{\frac{2\pi i}{3}}\Big(4 + b_2' + i\sqrt{48 - 8b_2' - b_2'^2}\Big)^{\frac{1}{3}}\Big)$$

$$b_4' = 2\,\mathrm{Re}\Big(e^{\frac{2\pi i}{3}}(70 + 10i\sqrt{31})^{\frac{1}{3}}\Big)$$

$$b_5' = -\frac{1}{2}\sqrt{2a - 18}$$

2.

orbit	$\mathrm{Gal}(\mathbb{E}/\mathbb{Q})$	$\mathrm{Gal}(\mathbb{E}/\mathbb{E}_0)$
$30abc$	$\langle g_a, g_1, g_2, g_3, g_4, g_5, \bar{g}_1\rangle$	$\langle g_1^3, g_2, g_3, g_4, g_5, \bar{g}_1\rangle$
$30d$	$\langle g_a, g_1, g_2, g_3, g_4, g_5, \bar{g}_1\rangle$	$\langle g_1, g_2, g_3, g_4, g_5, \bar{g}_1\rangle$

g_1 cycles orbits $30abc$ in the order $30a \to 30b \to 30c \to 30a$, and restricts to an order 3 automorphism on $30d$.

3.

G_{a1}	G_{b1}	G_{c1}	G_{d1}	$G_{a2} = G_{c2}$	G_{b2}	G_{d2}
$\begin{pmatrix}15 & 49\\ 4 & 45\end{pmatrix}$	$\begin{pmatrix}9 & 56\\ 5 & 51\end{pmatrix}$	$\begin{pmatrix}21 & 40\\ 20 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 20\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}13 & 24\\ 36 & 37\end{pmatrix}$	$\begin{pmatrix}7 & 36\\ 24 & 43\end{pmatrix}$	$\begin{pmatrix}1 & 21\\ 3 & 40\end{pmatrix}$
$G_{a3} = G_{c3}$	G_{b3}	G_{d3}	$G_{a4} = G_{b4} = G_{c4}$	G_{d4}	$G_{a5} = G_{b5} = G_{c5}$	G_{d5}
$\begin{pmatrix}11 & 25\\ 35 & 36\end{pmatrix}$	$\begin{pmatrix}5 & 19\\ 41 & 24\end{pmatrix}$	$\begin{pmatrix}1 & 48\\ 24 & 13\end{pmatrix}$	$\begin{pmatrix}1 & 30\\ 30 & 31\end{pmatrix}$	$\begin{pmatrix}1 & 3\\ 9 & 58\end{pmatrix}$	$\begin{pmatrix}0 & 31\\ 29 & 31\end{pmatrix}$	$\begin{pmatrix}29 & 0\\ 0 & 29\end{pmatrix}$

Dimension 35

1.

h	a	r_1	r_2	r_3	b_1	b_2	b_3	b_4	b_5	b_6	i	order	$g_a h g_a^{-1}$
g_a	$-a$	r_1	r_2	r_3	b_1'	b_2	b_3	b_4	b_5	b_6'	i	2	g_a
g_1	a	r_1	r_2	$-r_3$	b_1	b_2	b_3	b_4	b_5'	b_6	i	4	g_1^3
g_2	a	$-r_1$	r_2	r_3	b_1	b_2	b_3'	b_4'	b_5	b_6''	i	24	g_2^{13}
g_3	a	r_1	r_2	r_3	$-b_1$	b_2'	b_3	b_4	b_5	b_6	i	6	g_3^5
g_4	a	r_1	$-r_2$	r_3	b_1	b_2	$-b_3$	b_4	b_5	b_6	i	2	$g_3^3 g_4$
$\bar{g}_1$	a	r_1	r_2	r_3	b_1	b_2	b_3	b_4	b_5	b_6	$-i$	2	$g_c = g_2^{12} g_2^3 \bar{g}_1$

$$b_1' = \sqrt{2a-1}$$

$$b_2' = 2\,\mathrm{Re}\Big(e^{\frac{2\pi i}{3}}\,(280+210i\sqrt{6})^{\frac{1}{3}}\Big)$$

$$b_3' = \sqrt{14(5-r_1)}$$

$$b_4' = \mathrm{Re}\Big(e^{\frac{2\pi i}{3}}\,(28+84i\sqrt{3})^{\frac{1}{3}}\Big)$$

$$b_5' = \sqrt{3+r_3}$$

$$b_6' = -\tfrac{1}{7}\sqrt{245a+7r_2b_3-49ar_1}$$

$$b_6'' = \tfrac{i}{7}\sqrt{245a-7r_2b_3'+49ar_1}$$

2.

orbit	$\mathrm{Gal}(\mathbb{E}/\mathbb{Q})$	$\mathrm{Gal}(\mathbb{E}/\mathbb{E}_0)$
$35bcdg$	$\langle g_a, g_1, g_2, g_3, g_4, \bar{g}_1\rangle$	$\langle g_2, g_3, g_4, \bar{g}_1\rangle$
$35af$	$\langle g_a, g_1, g_2, g_3, g_4, \bar{g}_1\rangle$	$\langle g_2, g_3, g_4, \bar{g}_1\rangle$
$35e$	$\langle g_a, g_2, g_3, g_4, \bar{g}_1\rangle$	$\langle g_2, g_3, g_4, \bar{g}_1\rangle$
$35h$	$\langle g_a, g_2, g_3, g_4, \bar{g}_1\rangle$	$\langle g_2, g_3, g_4, \bar{g}_1\rangle$
$35i$	$\langle g_a, g_2, g_3, g_4, \bar{g}_1\rangle$	$\langle g_2, g_3, g_4, \bar{g}_1\rangle$
$35j$	$\langle g_a, g_2, g_3, g_4, \bar{g}_1\rangle$	$\langle g_2, g_3, g_4, \bar{g}_1\rangle$

g_1 cycles orbits $35bcdg$ in the order $35b \to 35c \to 35d \to 35g \to 35b$ and interchanges orbits $35af$; it satisfies the relations $g_1^2 = g_2^{12}$ on $35af$, $g_1 = g_2^6 g_4 \bar{g}_1$ on $35e$; it restricts to the identity on $35h$, $35i$, $35j$. g_2 satisfies the relations $g_2^{12} = e$ on $35i$ (where e is the identity) and $g_2^6 = g_4\bar{g}_1$ on $35j$.

3.

G_{a1}	G_{b1}	G_{c1}	G_{d1}	G_{f1}	G_{g1}	$G_{a2} = G_{b2} = G_{d2} = G_{i2}$	$G_{c2} = G_{e2} = G_{f2} = G_{g2} = G_{h2}$
$\begin{pmatrix}15 & 34\\ 14 & 20\end{pmatrix}$	$\begin{pmatrix}3 & 15\\ 18 & 32\end{pmatrix}$	$\begin{pmatrix}8 & 10\\ 18 & 27\end{pmatrix}$	$\begin{pmatrix}8 & 17\\ 25 & 27\end{pmatrix}$	$\begin{pmatrix}6 & 14\\ 20 & 29\end{pmatrix}$	$\begin{pmatrix}3 & 22\\ 25 & 32\end{pmatrix}$	$\begin{pmatrix}2 & 21\\ 14 & 23\end{pmatrix}$	$\begin{pmatrix}14 & 33\\ 2 & 12\end{pmatrix}$
G_{j2}	$G_{a3} = G_{b3} = G_{d3}$	$G_{c3} = G_{e3} = G_{f3} = G_{g3} = G_{h3} = G_{i3}$	G_{j3}	$G_{a4} = G_{b4} = G_{d4}$	$G_{c4} = G_{e4} = G_{f4} = G_{g4} = G_{h4}$	G_{i4}	G_{j4}
$\begin{pmatrix}1 & 33\\ 2 & 34\end{pmatrix}$	$\begin{pmatrix}15 & 34\\ 1 & 14\end{pmatrix}$	$\begin{pmatrix}1 & 20\\ 15 & 21\end{pmatrix}$	$\begin{pmatrix}3 & 22\\ 13 & 25\end{pmatrix}$	$\begin{pmatrix}4 & 11\\ 24 & 15\end{pmatrix}$	$\begin{pmatrix}15 & 24\\ 11 & 4\end{pmatrix}$	$\begin{pmatrix}15 & 31\\ 4 & 11\end{pmatrix}$	$\begin{pmatrix}0 & 27\\ 8 & 27\end{pmatrix}$

Dimension 39

1.

h	a	r_1	r_2	b_1	b_2	b_3	b_4	b_5	b_6	b_7	ir_3	order	$g_a h g_a^{-1}$
g_a	-a	r_1	r_2	b_1	b_2	b_3'	b_4'	b_5	b_6'	b_7'	ir_3	2	g_a
g_1	a	$-r_1$	r_2	b_1'	b_2	b_3''	b_4''	b_5	b_6	b_7	ir_3	8	g_1^7
g_2	a	r_1	r_2	$-b_1$	b_2	b_3	b_4	b_5	b_6	b_7	ir_3	2	g_2
g_3	a	r_1	$-r_2$	b_1	b_2'	b_3	b_4	b_5	b_6	b_7	ir_3	4	$g_1^6 g_3 g_6$
g_4	a	r_1	r_2	b_1	b_2	b_3	b_4	b_5'	b_6	b_7	ir_3	3	$g_4 g_5^2$
g_5	a	r_1	r_2	b_1	b_2	b_3	b_4	b_5	b_6''	b_7	ir_3	3	g_5^2
g_6	a	r_1	r_2	b_1	b_2	b_3	b_4	b_5	b_6	$-b_7$	ir_3	2	g_6
$\bar{g}_1$	a	r_1	r_2	b_1	b_2	b_3	b_4	b_5	b_6	b_7	$-ir_3$	2	$g_c = g_6 \bar{g}_1$

$$b_1' = \sqrt{-3r_1 + 18}$$

$$b_2' = -\sqrt{-18r_2 + 78}$$

$$b_3' = \sqrt{(-4a + 15)(r_1 + 5)}$$

$$b_3'' = -\sqrt{(4a + 15)(-r_1 + 5)}$$

$$b_4' = -\sqrt{-(2a + 5)(r_1 - 2)b_3' + (8a + 35)(10 - r_1)}$$

$$b_4'' = \sqrt{-(2a - 5)(r_1 + 2)b_3'' - (8a - 35)(10 + r_1)}$$

$$b_5' = \mathrm{Re}\Big(e^{\frac{2\pi i}{3}} \big(-676 + 10140 i\sqrt{3}\big)^{\frac{1}{3}}\Big)$$

$$b_6' = \mathrm{Re}\Big(\big(180 + 4a + 4i\sqrt{6753 - 90a}\big)^{\frac{1}{3}}\Big)$$

$$b_6'' = \mathrm{Re}\Big(e^{\frac{2\pi i}{3}} \big(180 - 4a + 4i\sqrt{6753 + 90a}\big)^{\frac{1}{3}}\Big)$$

$$b_7' = \sqrt{6a + 3}$$

2.

orbit	$\mathrm{Gal}(\mathbb{E}/\mathbb{Q})$	$\mathrm{Gal}(\mathbb{E}/\mathbb{E}_0)$
$39acde$	$\langle g_a, g_1, g_2, g_3, g_4, g_5, g_6, \bar{g}_1 \rangle$	$\langle g_1^2, g_3, g_4, g_5, g_6, \bar{g}_1 \rangle$
$39bf$	$\langle g_a, g_1, g_3, g_4, g_5, g_6, \bar{g}_1 \rangle$	$\langle g_1^2, g_3, g_4, g_5, g_6, \bar{g}_1 \rangle$
$39gh$	$\langle g_a, g_1, g_2, g_3, g_4, g_6, \bar{g}_1 \rangle$	$\langle g_1^2, g_2, g_3, g_4, g_6, \bar{g}_1 \rangle$
$39ij$	$\langle g_a, g_1, g_3, g_4, g_6 \bar{g}_1 \rangle$	$\langle g_1^2, g_3, g_4, g_6, \bar{g}_1 \rangle$

g_1 interchanges the pairs $39ae$, $39cd$, $39bf$, $39gh$ and $39ij$. g_2 interchanges the pairs $39ac$ and $39de$ and restricts to the identity on $39bf$ and $39ij$. g_5 restricts to the identity on $39gh$ and $39ij$.

3.

G_{a1}	G_{b1}	G_{c1}	G_{d1}	G_{e1}	G_{f1}	G_{g1}	G_{h1}	G_{i1}	G_{j1}
$\begin{pmatrix}12 & 14\\25 & 26\end{pmatrix}$	$\begin{pmatrix}0 & 25\\14 & 25\end{pmatrix}$	$\begin{pmatrix}10 & 32\\3 & 29\end{pmatrix}$	$\begin{pmatrix}13 & 27\\1 & 26\end{pmatrix}$	$\begin{pmatrix}3 & 7\\32 & 10\end{pmatrix}$	$\begin{pmatrix}16 & 33\\6 & 10\end{pmatrix}$	$\begin{pmatrix}4 & 30\\29 & 13\end{pmatrix}$	$\begin{pmatrix}2 & 3\\38 & 38\end{pmatrix}$	$\begin{pmatrix}0 & 7\\28 & 6\end{pmatrix}$	$\begin{pmatrix}4 & 21\\6 & 22\end{pmatrix}$
G_{a2}	G_{c2}	$G_{d2} = G_{e2}$	G_{g2}	G_{h2}	$G_{a3} = G_{b3} = G_{c3} = G_{e3} = G_{f3}$	G_{d3}	$G_{g3} = G_{h3}$	$G_{i3} = G_{j3}$	
$\begin{pmatrix}19 & 23\\16 & 3\end{pmatrix}$	$\begin{pmatrix}3 & 16\\23 & 19\end{pmatrix}$	$\begin{pmatrix}1 & 12\\13 & 38\end{pmatrix}$	$\begin{pmatrix}7 & 7\\15 & 26\end{pmatrix}$	$\begin{pmatrix}20 & 7\\15 & 13\end{pmatrix}$	$\begin{pmatrix}21 & 25\\14 & 7\end{pmatrix}$	$\begin{pmatrix}7 & 14\\25 & 21\end{pmatrix}$	$\begin{pmatrix}11 & 18\\33 & 32\end{pmatrix}$	$\begin{pmatrix}9 & 28\\34 & 33\end{pmatrix}$	
$G_{a4} = G_{b4} = G_{c4} = G_{e4} = G_{f4}$	G_{d4}	$G_{g4} = G_{h4}$	$G_{i4} = G_{j4}$	$G_{a5} = G_{b5} = G_{c5} = G_{e5} = G_{f5}$	G_{d5}	$G_{a6} = G_{b6} = G_{c6} = G_{d6} = G_{e6} = G_{f6}$	$G_{g6} = G_{h6}$	$G_{i6} = G_{j6}$	
$\begin{pmatrix}4 & 9\\30 & 13\end{pmatrix}$	$\begin{pmatrix}13 & 30\\9 & 4\end{pmatrix}$	$\begin{pmatrix}22 & 0\\0 & 22\end{pmatrix}$	$\begin{pmatrix}0 & 2\\8 & 24\end{pmatrix}$	$\begin{pmatrix}12 & 14\\25 & 26\end{pmatrix}$	$\begin{pmatrix}25 & 27\\12 & 13\end{pmatrix}$	$\begin{pmatrix}0 & 1\\38 & 1\end{pmatrix}$	$\begin{pmatrix}2 & 3\\12 & 38\end{pmatrix}$	$\begin{pmatrix}0 & 7\\28 & 6\end{pmatrix}$	

Dimension 48

1.

h	a	r_1	r_2	r_3	t	b_1	b_2	b_3	b_4	b_5	b_6	i	order	$g_a h g_a^{-1}$
g_a	$-a$	r_1	r_2	r_3	t	b_1'	b_2	b_3	b_4	b_5'	b_6	i	2	g_a
g_1	a	r_1	r_2	$-r_3$	t	b_1	b_2	b_3	b_4'	b_5''	b_6	i	8	g_1^7
g_2	a	$-r_1$	r_2	r_3	t'	b_1	b_2'	b_3'	b_4	b_5	b_6	i	8	$g_2 g_3^6$
g_3	a	r_1	$-r_2$	r_3	t''	b_1	b_2'	b_3''	b_4	b_5	b_6	i	8	$g_1^4 g_3^3$
g_4	a	r_1	r_2	r_3	t	b_1	b_2	b_3	b_4	b_5	b_6'	i	3	g_4^2
g_5	a	r_1	r_2	r_3	t	$-b_1$	b_2	b_3	b_4	b_5	b_6	i	2	g_5
$\bar{g}_1$	a	r_1	r_2	r_3	t	b_1	b_2	b_3	b_4	b_5	b_6	$-i$	2	$g_c = g_5 \bar{g}_1$

$$t' = \cos\tfrac{37\pi}{48}$$

$$t'' = \cos\tfrac{17\pi}{48}$$

$$b_1' = \sqrt{a+1}$$

$$b_2' = -\sqrt{6 - r_1 r_2}$$

$$b_3' = \sqrt{6 + 2r_1 r_2 + (r_2 + r_1) b_2'}$$

$$b_3'' = -\sqrt{6 + 2r_1 r_2 - (r_2 + r_1) b_2'}$$

$$b_4' = -\sqrt{-2r_3 + 42}$$

$$b_5' = -\sqrt{(-5(a-1) + (3a+5)r_3) b_4 + 2(a-5) r_3 + 210(3+a)}$$

$$b_5'' = -\sqrt{(5(a+1) + (3a-5)r_3) b_4' + 2(a+5) r_3 + 210(3-a)}$$

$$b_6' = 2\,\mathrm{Re}\Big(e^{\frac{2\pi i}{3}} \big(7 + i\sqrt{15}\big)^{\frac{1}{3}}\Big)$$

2.

orbit	$\mathrm{Gal}(\mathbb{E}/\mathbb{Q})$	$\mathrm{Gal}(\mathbb{E}/\mathbb{E}_0)$
$48abcd$	$\langle g_a, g_1, g_2, g_3, g_4, g_5, \bar{g}_1 \rangle$	$\langle g_1^4, g_2, g_3, g_4, g_5, \bar{g}_1 \rangle$
$48e$	$\langle g_a, g_1, g_2, g_3, g_5, \bar{g}_1 \rangle$	$\langle g_1, g_2, g_3, g_5, \bar{g}_1 \rangle$
$48f$	$\langle g_a, g_2, g_3, g_4, g_5, \bar{g}_1 \rangle$	$\langle g_2, g_3, g_4, g_5, \bar{g}_1 \rangle$
$48g$	$\langle g_a, g_2, g_3, g_5, \bar{g}_1 \rangle$	$\langle g_2, g_3, g_5, \bar{g}_1 \rangle$

g_1 cycles $48abcd$ in the order $48a \to 48d \to 48b \to 48c \to 48a$ and restricts to the identity on $48f$, $48g$. g_4 restricts to the identity on $48e$, $48g$.

3.

G_{a1}	G_{b1}	G_{c1}	G_{d1}	G_{e1}	$G_{a2} = G_{b2} = G_{f2}$	$G_{c2} = G_{d2}$	G_{e2}	G_{g2}
$\begin{pmatrix} 13 & 56 \\ 69 & 83 \end{pmatrix}$	$\begin{pmatrix} 5 & 19 \\ 24 & 91 \end{pmatrix}$	$\begin{pmatrix} 8 & 21 \\ 29 & 88 \end{pmatrix}$	$\begin{pmatrix} 5 & 72 \\ 77 & 91 \end{pmatrix}$	$\begin{pmatrix} 11 & 50 \\ 58 & 89 \end{pmatrix}$	$\begin{pmatrix} 1 & 11 \\ 85 & 12 \end{pmatrix}$	$\begin{pmatrix} 12 & 85 \\ 11 & 1 \end{pmatrix}$	$\begin{pmatrix} 23 & 36 \\ 84 & 83 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 37 & 95 \end{pmatrix}$

$G_{a3} = G_{b3} = G_{f3}$	$G_{c3} = G_{d3}$	G_{e3}	G_{g3}	$G_{a4} = G_{b4} = G_{f4}$	$G_{c4} = G_{d4}$	$G_{a5} = G_{b5} = G_{c5} = G_{d5} = G_{e5} = G_{f5} = G_{g5}$
$\begin{pmatrix} 17 & 37 \\ 59 & 54 \end{pmatrix}$	$\begin{pmatrix} 11 & 31 \\ 65 & 42 \end{pmatrix}$	$\begin{pmatrix} 25 & 93 \\ 81 & 28 \end{pmatrix}$	$\begin{pmatrix} 4 & 47 \\ 11 & 53 \end{pmatrix}$	$\begin{pmatrix} 15 & 17 \\ 79 & 32 \end{pmatrix}$	$\begin{pmatrix} 31 & 33 \\ 63 & 64 \end{pmatrix}$	$\begin{pmatrix} 95 & 0 \\ 0 & 95 \end{pmatrix}$

References

[1] G. Zauner, *Quantendesigns. Grundzüge einer nichtkommutativen designtheorie.* PhD thesis, University of Vienna, 1999. Published in English translation: G. Zauner, "Quantum designs: foundations of a noncommutative design theory," *Int. J. Quantum Inf.* **9** (2011) 445–508.

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

[3] C. A. Fuchs and M. Sasaki, "Squeezing quantum information through a classical channel: Measuring the quantumness of a set of quantum states," *Quantum Inf. Comput.* **3** (2003) 377–404.

[4] J. Řeháček, B.-G. Englert, and D. Kaszlikowski, "Minimal qubit tomography," *Phys. Rev. A* **70** (2004) 052321.

[5] B.-G. Englert, D. Kaszlikowski, H. K. Ng, W. K. Chua, J. Řeháček, and J. Anders, "Efficient and robust quantum key distribution with minimal state tomography," quant-ph/0412075.

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

[7] T. Durt, C. Kurtsiefer, A. Lamas-Linares, and A. Ling, "Wigner tomography of two-qubit states and quantum cryptography," *Phys. Rev. A* **78** (2008) 042338.

[8] H. Zhu and B.-G. Englert, "Quantum state tomography with fully symmetric measurements and product measurements," *Phys. Rev. A* **84** (2011) 022327.

[9] H. Zhu, "Quasiprobability representations of quantum mechanics with minimal negativity," arXiv:1604.06974.

[10] C. A. Fuchs and R. Schack, "Quantum-bayesian coherence," *Rev. Mod. Phys.* **85** (2013) 1693–1715.

[11] S. D. Howard, A. R. Calderbank, and W. Moran, "The finite Heisenberg-Weyl groups in radar and communications," *EURASIP Journal on Applied Signal Processing* **2006** (2006) 1–11.

[12] R.-D. Malikiosis, "Spark deficient Gabor frames," arXiv:1602.09012.

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

[14] A. J. Scott, "SICs: Extending the list of solutions," arXiv:1703.03993.

[15] C. A. Fuchs, M. C. Hoang, and B. C. Stacey, "SICs: More numerical solutions." To appear.

[16] S. G. Hoggar, "64 lines from a quaternionic polytope," *Geometriae Dedicata* **69** (1998) 287–289.

[17] H. Zhu, "Super-symmetric informationally complete measurements," *Ann. Phys. (NY)* **362** (2015) 311–326.

[18] B. C. Stacey, "Sporadic SICs and the normed division algebras," arXiv:1605.01426.

[19] D. A. Marcus, *Number Fields.* Springer, 1977.

[20] H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields. With Two Appendices by Olga Taussky.* Springer, 1978.

[21] D. M. Appleby, H. Yadsan-Appleby, and G. Zauner, "Galois automorphisms of a symmetric measurement," *Quantum Inf. Comput.* **13** (2013) 672–720.

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

[23] D. H. Bailey, J. M. Borwein, N. J. Calkin, R. Girgensohn, D. R. Luke, and V. H. Moll, *Experimental Mathematics in Action.* A. K. Peters, Wellesley, MA, USA, 2007.

[24] H. Ferguson, D. Bailey, and S. Arno, "Analysis of PSLQ, an integer relation finding algorithm," *Mathematics of Computation* **68** (1999) 351–369.

[25] D. M. Appleby, I. Bengtsson, S. Brierley, M. Grassl, D. Gross, and J.-Å. Larsson, "The monomial representations of the Clifford group," *Quantum Inf. Comput.* **12** (2012) 404–431.

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

[27] E. Knill, "Group representations, error bases and quantum codes," arXiv:9608049.

[28] A. A. Klappenecker and M. Rötteler, "Beyond stabilizer codes. i. nice error bases," *IEEE Transactions on Information Theory* **48** no. 8, (2002) 2392–2395.

[29] D. M. Appleby, "Properties of the extended Clifford group with applications to SIC-POVMs and MUBs," arXiv:0909.5233.

[30] D. M. Appleby, I. Bengtsson, and H. B. Dang, "Galois unitaries, mutually unbiased bases, and MUB-balanced states," *Quantum Inf. Comput.* **15** (2015) 1261–1294.

[31] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory.* Graduate Texts in Mathematics, no. 84. Springer, second ed., 1990.

[32] See http://www.physics.usyd.edu.au/~sflammia/SIC for a table of the known exact solutions.