Constructing exact symmetric informationally complete measurements from numerical solutions

Marcus Appleby, Tuan-Yow Chien, Steven Flammia and Shayne Waldron

1 Centre for Engineered Quantum Systems, School of Physics, University of Sydney, Sydney, Australia
2 Department of Mathematics, University of Auckland, Auckland, New Zealand
3 Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, MA, United States of America

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

Received 30 November 2017, revised 5 March 2018
Accepted for publication 7 March 2018
Published 27 March 2018

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 to 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 (except in special cases where there are additional symmetries). 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 an SIC. Using this method, we have calculated 69 new exact solutions, including nine 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 address two questions suggested by the previous work.

Keywords: SIC, design, frame, Galois, algebraic number theory
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 a $d$-dimensional complex vector space. They were originally introduced by Zauner [1] and Renes et al [2], and 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 [2, 13–17] in every dimension up to 151, and for a handful of other dimensions up to 1155. Exact solutions [1, 13, 16–20] have been calculated in dimensions 2–16, 19, 24, 28, 35, 48, 120, 124, 323. 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 [21] in dimension 8, are sometimes called sporadic SICs, on the grounds that they have a number of special properties [22, 23]. In this paper, we exclude them from consideration. In the following, the term ‘SIC’ will thus always mean ‘non-sporadic SIC’. In particular, we will always assume without comment that the dimension is greater than 3.

In physics, a numerical solution to a system of equations is usually perfectly adequate—especially when, as here, it is known to 35 digits of precision or more. However, as we discuss below, SICs have important features (important for the applications, as well as from a pure mathematical point of view) which are only accessible if one has an exact solution in hand. Here, we face the difficulty that—aside from a few low dimensional cases, where a hand calculation is possible—all previously known exact solutions were obtained using a Gröbner basis. Moreover, every solution in dimensions higher than 16 has relied on the existence of additional symmetries which are only present in special cases. The great majority of SICs do not have such symmetries, and for these the Gröbner basis method has probably been pushed about as far as it is possible to go without massive increases in computer speed and memory. We therefore need a new method for calculating exact SICs. In this paper, we describe such a method. The idea is to start with a high-precision numerical solution (much easier to calculate), and then convert it into an exact solution.

The method relies on, and is motivated by, some recently discovered connections between SICs and algebraic number theory [24, 25]. 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 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 [26–28]. We outline the most salient points of this number-theoretic connection here, assuming some familiarity with the basic concepts underlying SICs; however, we provide all of the necessary definitions and background in section 2 below.

Let $\Pi$ be an SIC fiducial projector in dimension $d \geq 4$, and let $E = \mathbb{Q}(\Pi, \tau)$ be the field generated over the rationals by the standard-basis components of $\Pi$ together with $\tau = -e^{\pi \iota \frac{d}{2}}$. We refer to $E$ as the SIC field. It is easily seen that $E$ only depends on the $\text{EC}(d)$ orbit to which $\Pi$ belongs (where $\text{EC}(d)$ is the extended Clifford group in dimension $d$). Let $K = \mathbb{Q}(\sqrt{D})$, where $D$ is the square-free part of $(d - 3)(d + 1)$. Then one finds, in every case that has been calculated,

- $\mathbb{Q} \triangleleft K \triangleleft E$,
- $\mathbb{Q} \triangleleft E$.
- The Galois group $\text{Gal}(E/K)$ is Abelian.
(Here, the notation $F_1 \triangleleft F_2$ means that $F_2$ is a normal extension of $F_1$.) 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 [27] 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 $K$ with conductor $d'$ and ramification at both infinite places (where $d' = d$ if $d$ is odd, or $2d$ if $d$ is even).

If SICs existed in every finite dimension, and if the above statements were generally true, this 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 $\omega$ 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 12th 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 12th 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 [27] 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 12th 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 [29], which describes a series of significant geometrical results none of which would have been suspected without the clue from number theory, and which cannot be properly understood in isolation from the number theory. Two of the authors are actively engaged in pursuing these connections between number theory and geometry further.

For many purposes, a high-precision approximate SIC is completely satisfactory. However, if one wants to investigate the connections with number theory, exact solutions are essential. As we discussed above, the Gröbner basis method—used to obtain most of the previously known exact solutions—is extremely demanding computationally and is probably not capable of being taken much further on existing computer hardware. 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 an SIC to bump the high precision approximate SICs in [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 $F$. Let $b_1, \ldots, b_n$ be a basis for $F$ over the rationals. Then $a_e = q_1b_1 + \cdots + q_nb_n$ for some set of rational numbers $q_j$. Multiplying through by the LCM of the $q_j$, we deduce
for some set of integers \( m_0, m_1, \ldots, m_n \). If we can calculate the \( m_j \), we will have managed to find an exact number to 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 are after. This procedure can be done using an integer-relation algorithm [30], such as the PSLQ algorithm [31].

A few remarks are in order. In the first place, there are infinitely many sequences \( m_j \) satisfying equation (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 [30], 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 have therefore exploited a conjecture in [26], 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 and Grassl [13] calculated 179 numerical fiducials in dimensions 4–50, and argued 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. Scott [14] calculated a further 323 numerical fiducials in dimensions 51–90, restricting the search to fiducials having an \( F_c \) or \( F_a \) symmetry. He states that it is ‘likely’ that this list is complete (by contrast, he is ‘confident’ that the list in [13] is complete). Another 76 numerical fiducials have been calculated [14–17] in dimensions 91–121 and a handful of additional dimensions up to 1155, but with no claim as to completeness. This gives us a total of 578 unitarily inequivalent numerical fiducials for \( d \geq 4 \). By contrast, there are only 30 orbits for which an exact solution has been calculated [1], [13, 16–20] with \( d \geq 4 \). We have calculated exact representatives for a further 69 orbits, and provide a complete analysis for 52 of these. 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 for which a numerical fiducial is known, 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 [26]—as was there noted—cannot be true of the type-a orbits 21e,
30d, 39ghij, 48e (where we employ the Scott–Grassl labeling scheme [13]). 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. This material is mostly in [13, 18, 26–28]. 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 [26] also naturally generalize to these orbits. 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 the appendix, we present our results. Many of the fields we calculate are of much higher degree\(^1\) than the fields calculated in [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 thus 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 [13, 14, 18], [26–28]. Some of the statements in this section are proven facts, while others are observations only known to be true for the SICs which have actually been calculated. The latter will always be clearly identified as such. As explained in the Introduction, we assume without comment that the SICs with which we deal are non-sporadic in the sense of [23]. In particular, it will always be assumed that the dimension \( d \geq 4 \), and that the SICs with which we deal are covariant with respect to the Weyl–Heisenberg (WH) group.

We first define the WH group. Let \( \mathcal{H} \) be a \( d \)-dimensional Hilbert space, and let \(|0\), \ldots, |d-1)\) be the standard basis. Let \( X, Z \) be the operators which act according to\(^1\)

\(^1\) 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 thus 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.
\[ X |r\rangle = |r + 1\rangle, \quad Z |r\rangle = \omega^r |r\rangle, \]

where \( \omega = e^{2\pi i / d} \) and addition of indices is \( \text{mod } d \). For each \( p = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} \in \mathbb{Z}^2 \), we define the displacement operator

\[ D_p = \gamma^{p_1 p_2} X^{p_1} Z^{p_2}, \]

where \( \gamma = -e^{\pi i / d} \). The WH group then consists of all operators of the form \( \tau^r D_p \) for \( r \) an integer.

The displacement operators constitute a nice unitary error basis \([33, 34]\). In particular, an arbitrary operator \( A \) has the expansion

\[ A = \sum_{p_1, p_2 = 0}^{d-1} A_p D_p, \quad A_p = \frac{1}{d} \text{Tr}(D_p^d A). \]

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

\[ U_F D_p U_F^\dagger = D_{p'} \]

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

\[ U_F U_G \equiv U_{FG} \]

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

There are \([18, 35]\) explicit formulae for the operators \( U_F \). If the symplectic matrix

\[ F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \]

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

\[ U_F = \frac{e^{i\theta}}{\sqrt{d}} \sum_{r,s=0}^{d-1} \tau^r \beta^{-1} (d' \tau^2 - 2r \alpha \gamma) |r\rangle \langle s|, \]

where \( e^{i\theta} \) is an arbitrary phase, and \( \beta^{-1} \) is the multiplicative inverse of \( \beta \) considered as an element of \( \mathbb{Z}/d' \mathbb{Z} \). Matrices in SL(\( 2, \mathbb{Z}/d' \mathbb{Z} \)) not satisfying the condition \( \text{GCD}(\beta, d') = 1 \) 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 \( F' \in SL(2, \mathbb{Z}/d' \mathbb{Z}) \) and

\[ J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \]
The anti-unitary $U_J$ acts by complex conjugation in the standard basis. Using these facts, we can calculate $U_F$ for arbitrary $F \in \text{ESL}(2, \mathbb{Z}/d')$.

By definition a WH-covariant SIC consists of the $d^2$ operators $D_p \Pi D_p^\dagger$ where $\Pi$ is a rank-1 projector with the property

$$\text{Tr}(\Pi D_p) = \begin{cases} 1 & \text{if } p = 0 \mod d \\ \frac{e^{ip}}{\sqrt{d+1}} & \text{otherwise} \end{cases}$$

for some set of phases $e^{ip}$. We refer to $\Pi$ as the fiducial, to the quantities $\text{Tr}(\Pi D_p)$ as the overlaps, and to the numbers $e^{ip}$ as the overlap phases. It can be seen from equation (4) that the overlap phases completely determine the fiducial.

**Observation 1.** 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 described in [27].

If $\Pi$ is an SIC fiducial projector then so is $U \Pi U^\dagger$ for every $U \in \text{EC}(d)$. Consequently the fiducial projectors split into a collection of $\text{EC}(d)$ orbits. Scott and Grassl [13] have, with high probability, identified every $\text{EC}(d)$ orbit for $d \leq 50$, and Scott [14] has extended the calculations to higher dimensions.

**Observation 2.** At the time of writing it appears that there are only finitely many $\text{EC}(d)$ orbits in every dimension $d \leq 90$.

We define the stability group of an SIC fiducial $\Pi$ to be the set of all $U \in \text{EC}(d)$ such that $U \Pi U^\dagger = \Pi$.

**Observation 3.** In every known case the stability group contains a unitary of the form $D_p U_F$, where $\text{Tr}(F) = -1 \mod d$.

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 canonical order 3 unitary is conjugate modulo a phase to $U_F$, where

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

We refer to $F_z$ as the Zauner matrix.

**Observation 4.** In the cases where it is likely that we know the full set of $\text{EC}(d)$ orbits, it is found that if $d = 6 \mod 9$ the additional conjugacy class never gives rise to SICs, while if $d = 3 \mod 9$ it always does.

When $d = 3 \mod 9$ we choose [13], as representative of the additional conjugacy class $U_F$, where

$$F_a = \begin{pmatrix} 1 & d+3 \\ \frac{d+1}{3} & d-2 \end{pmatrix}. \quad (12)$$

We define the Zauner matrix this way to secure consistency with [13]. The Zauner matrix is often defined to be $F_z^4 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ 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 $U_F$ and $U_{F_z}$ are equal modulo a phase.

---

2 We define the Zauner matrix this way to secure consistency with [13]. The Zauner matrix is often defined to be $F_z^4 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ 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 $U_F$ and $U_{F_z}$ are equal modulo a phase.
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 \(EC(d)\) is displacement-free if it consists entirely of operators of the form \(e^{i\theta}U_{F}\), with \(F \in \text{ESL}(2,\mathbb{Z}/d'\mathbb{Z})\). Following [27, 28] 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 [26] such fiducials were called simple).

**Observation 5.** Every known \(EC(d)\) orbit of SIC fiducials contains at least one centred fiducial.

Given a centred fiducial \(\Pi\), we define \(S_0(\Pi)\) to consist of all \(F \in \text{ESL}(2,\mathbb{Z}/d'\mathbb{Z})\) such that \(UF\) is in the stability group of \(\Pi\).

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 \(F\) as shorthand for the statement that its standard basis matrix elements are in (respectively generate) \(F\). Similarly, we write \(F(A)\) to mean \(F(\bigcup_{s=0}^{d'} \langle r|A|s \rangle)\). 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 equation (8) is chosen appropriately. This was shown in [36] 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

\[
e^{i\theta} = \begin{cases} 
1 & d = 1 \text{ mod } 4 \\
i & d = 3 \text{ mod } 4 \\
e^{\frac{\pi i}{2}} & d = 0 \text{ mod } 2
\end{cases}
\]  

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

Now let \(\Pi\) be any SIC fiducial projector and define \(E = \mathbb{Q}(\Pi, \tau)\).

**Observation 6.** In every known case, the extension \(E/\mathbb{Q}\) is finite degree and normal. In particular, \(\text{Gal}(E/\mathbb{Q})\) contains complex conjugation implying \(\Pi^* \in E\).

Observation 6 means that in every known case \(E\) is the same for every fiducial projector on the same \(EC(d)\) orbit. We refer to it as the SIC-field for that orbit.

**Observation 7.** Let \(\Pi\) be a centred fiducial, and let \(g_c\) be complex conjugation. In every known case \(E\) breaks into the tower

\[
\mathbb{Q} \subsetneq E_c \subsetneq E_0 \subsetneq E_1 \subsetneq E
\]  

where

1. The notation \(F \triangleleft G\) means ‘\(G\) is a normal extension of \(F\)’.
2. \(E_c\) is the fixed field of the centralizer of \(g_c\).
3. \(E_c = \mathbb{Q}(\sqrt{D})\), where \(D\) is the square-free part of \((d-3)(d+1)\).
4. \(\text{Gal}(E_c/\mathbb{Q})\) is Abelian.
5. For all \(g \in \text{Gal}(E_c/\mathbb{Q})\)
   a. \(g\) fixes \(E_c\) if and only if \(g(\Pi)\) is an SIC fiducial projector,
   b. \(g\) fixes \(E_0\) if and only if \(g(\Pi)\) is a fiducial on the same \(EC(d)\) orbit as \(\Pi\).

\(\text{Note that in [26] the extension } E = \mathbb{R}(\sqrt{d}) \text{ was also introduced, to ensure that the Clifford unitaries would be in the field. The considerations in the previous paragraph show that this was unnecessary.}\)
(6) $E = E_1(i\sqrt{d})$. In particular $E$ is a degree 2 extension of $E_1$.

(7) Let $g_1$ be the non-trivial element of $\text{Gal}(E/E_1)$ and let $g$ be any element of $\text{Gal}(E/Q)$ which does not fix $Q(\sqrt{D})$. Then

$$\bar{g}_1 = g_1 g^{-1}.$$  

(15)

(8) For all $p$ and some $k_{\Pi} \in (\mathbb{Z}/d'\mathbb{Z})^2$

$$\bar{g}_1(\text{Tr}(D_p\Pi)) = \omega^{(k_{\Pi},p)} \text{Tr}(D_p\Pi).$$  

(16)

(9) $E_c, E_0, E$ are normal over $Q$, but $E_1$ is not.

Note that it follows from item (7) that $\bar{g}_1(\tau) = \tau^{-1}$.

We say that a fiducial to which observation 7 applies is strongly centred if it is centred and $k_{\Pi} = 0$, so that the overlaps are all in $E_1$. If $d \neq 0 \mod 3$ centred fiducials are automatically strongly centred [26]. If $d = 0 \mod 3$ the concepts are not equivalent. However,

**Observation 8.** For every EC$(d)$ orbit for which an exact solution is known, there exist strongly centred fiducials whose stability group includes $U_{F_c}$ (for a type-$z$ orbit) or $U_{F_a}$ (for a type-$a$ orbit).4

We refer to a set of EC$(d)$ orbits sharing the same SIC field as a multiplet.

**Observation 9.** In every known case, the Galois group acts transitively on the elements of a multiplet.

**Observation 10.** In those cases where Scott and Grassl [13] give exact fiducials for what is probably the full set of EC$(d)$ orbits, there are at most two distinct multiplets. We refer to the field of lowest (respectively highest) degree as the minimal (respectively maximal) field, and to the corresponding multiplet as the minimal (respectively maximal) multiplet. It is found that when there are two multiplets, so that the minimal and maximal fields are distinct, the minimal field is a subfield of the maximal field.

**Observation 11.** Let $E$ be the minimal field in dimension $d$, and let $Q \lhd Q(\sqrt{D}) \lhd E_0 \lhd E_1 \lhd E$ be the associated tower. In every known case [27, 28],

(1) $E, E_1$ are ray class fields over $Q(\sqrt{D})$ for which the finite part of the conductor is $d'$,

(2) $E$ is the ray class field with ramification allowed at both infinite places,

(3) $E_1$ is the ray class field with ramification only allowed at the infinite place taking $\sqrt{D}$ to a positive real number,

(4) $E_0$ is the Hilbert class field over $\mathbb{Q}(\sqrt{D})$.

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

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

(17)

4 This fact was not appreciated at the time [26] was written. Consequently, the representatives of EC$(d)$ orbits 6a, 9ab, 12b, 24c in that paper are not strongly centred. They become strongly centred if $\Pi$ is replaced with $D_{n^2} \Pi J_{d^2}^\perp$, where $n = d/3$. This transformation leaves the stability group unchanged. Furthermore, if $\Pi$ is strongly-centred then in every known case the set of overlaps $\text{Tr}(D_p\Pi)$ generates $E_1$ over $Q$. 

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

\[
H_\tau = \begin{pmatrix} 1 & 0 \\ 0 & k_\tau \end{pmatrix}.
\]  
(18)

Then \(g\) acts on the elements of \(C(d)\) according to

\[
g(D_p U_\tau) = D_{k_\tau} U_{H_\tau^{-1}}.
\]  
(19)

\section*{Observation 12.}

Let \(\{a_1, \ldots, a_l\}\) be the \(\text{EC}(d)\) orbits of any of the known multiplets in dimension \(d\). Let \(Q \subset E_c \subset E_0 \subset E_1 \subset E\) be the associated tower, and let \(F_{\tau j}\) be a strongly centered fiducial on orbit \(a_j\). Then one finds that for each \(g \in \text{Gal}(E/E_c)\) and each index \(j\), there exist \(F_{\tau j} \in \text{ESL}(d)\) and an index \(k\) such that

\[
g(F_{\tau j}) = U_{F_{\tau j}} \Pi_k U_{F_{\tau j}}^\dagger.
\]  
(20)

Also

\[
g(\text{Tr}(D_p F_{\tau j})) = \text{Tr}(D_{G_{\tau j} p} \Pi_k)
\]  
(21)

for all \(p\), where

\[
G_{\tau j} = (\text{Det } F_{\tau j}) F_{\tau j}^{-1} H_\tau.
\]  
(22)

If \(g \in E_0\), then \(k = j\) in equations (20) and (21). The matrices \(F_{\tau j}, G_{\tau j}\) are not unique: indeed, they can be replaced with arbitrary elements of the cosets \(F_{\tau j} S_0(\Pi)\), \(S(\Pi) G_{\tau j}\) respectively, where

\[
S(\Pi) = \{(\text{Det } F) F : F \in S_0(\Pi)\}.
\]  
(23)

For the automorphism \(\bar{g}_{\tau}\) (as defined in observation 7) we can choose [26]

\[
G_{\bar{g}_{\tau} j} = I \quad F_{\bar{g}_{\tau} j} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}
\]  
(24)

for all \(j\).

Let \(Q \subset E_c \subset E_0 \subset E_1 \subset E\) be a tower to which the previous observations apply. With notation as in observation 12, choose \(g \in \text{Gal}(E_1/E_0)\) and let \(G_{\tau j} = G'_{\tau j}\) where \(g'\) is a lift of \(g\) to \(\text{Gal}(E/E_0)\). It is easily seen that this definition does not depend upon which of the two lifts is taken. Then it can be shown [26] that the \(G_{\tau j}\) are all in \(N(\Pi)\), the normalizer of \(S(\Pi)\) in \(\text{GL}(2, \mathbb{Z}/d'\mathbb{Z})\), and that for each fixed \(j\), the map \(g \to G_{\tau j} S(\Pi)\) is an injective homomorphism of \(\text{Gal}(E_1/E_0)\) into \(N(\Pi)/S(\Pi)\). It is natural to ask, what is the range of this homomorphism? The answer depends on whether the \(\text{EC}(d)\) orbit is type-\(z\) or type-\(a\).

\section*{Observation 13.}

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 \(\text{GL}(2, \mathbb{Z}/d'\mathbb{Z})\). Thus, we have an isomorphism

\[
\text{Gal}(E_1/E_0) \cong C(\Pi)/S(\Pi).
\]  
(25)

The conjecture that this isomorphism is generally true of a type-\(z\) orbit plays an important role in the calculations in the next section. Its restriction to the case of minimal SIC fields
should, if true, also be of number-theoretical interest: For it will 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.

Turning to type-$a$ orbits, one has:

**Observation 14.** For the two type-$a$ orbits for which exact solutions are given in [13], one finds [26]

$$\Gal(E_1/E_0) \cong C(\Pi)/S(\Pi), \quad (26)$$

just as is the case for the type-$z$ orbits.

However, this observation is of limited significance. The problem [26] is that one can see from the numerical data that the group $C(\Pi)/S(\Pi)$ is non-Abelian for the type-$a$ orbits $21d$, $30d$, $39gh$, $48e$. So, for these orbits, one of two things must be true: Either $E$ is not an Abelian extension of $\mathbb{Q}(\sqrt{D})$, or else $\Gal(E_1/E_0)$ 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 equation (25) holding for type-$a$ fiducials was conjectured in [26]. 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 $d \equiv 3 \pmod{9}$. Then $d = 3n$ where $n = 1 \pmod{3}$ and

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

The fact that $n$ is coprime to 3 means (see appendix B of [19]) that there is a natural isomorphism $\chi: \SL(2, \mathbb{Z}/d' \mathbb{Z}) \to \SL(2, \mathbb{Z}/n' \mathbb{Z}) \times \SL(2, \mathbb{Z}/3 \mathbb{Z}). \quad (28)$

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

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

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

$$\chi(F_a) = (F_a, I), \quad (30)$$

where

$$F_a = \begin{pmatrix} 1 & n + 9 \\ 4n - 1 & n - 2 \end{pmatrix}. \quad (31)$$

Observe that $\Tr(F_a) = -1 \pmod{n}$, implying that $F_a$ is conjugate to the Zauner matrix in dimension $n$.

---

5 By contrast, it can be shown [26] that for a type-$z$ orbit, $C(\Pi)/S(\Pi)$ is necessarily Abelian.
Now consider the isomorphism of equation (25). Suppose, to begin with, that \( \Pi \) is a strongly centred type-\( z \) fiducial. Without loss of generality we may assume that \( \Pi \) is an eigenvector of \( U_F \). Assume also that \( S(\Pi) \) is Abelian (as is the case for every known fiducial with \( d \geq 4 \)). It is shown in [26] that \( C(F_z) \), the centralizer of \( F_z \) in \( GL(2, \mathbb{Z}/d'\mathbb{Z}) \), is Abelian—from which it follows that \( C(\Pi) = C(F_z) \), so that the isomorphism becomes

\[
\text{Gal}(E_1/E_0) \cong C(F_z)/S(\Pi).
\] (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 equation (30) that

\[
C(F_a) \cong C(\bar{F}_a) \times GL(2, \mathbb{Z}/3\mathbb{Z}).
\] (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, \( GL(2, \mathbb{Z}/3\mathbb{Z}) \) 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 21\( d \), 30\( d \), 39\( gh \), 48\( e \)), then \( C(F_a)/S(\Pi) \) is non-Abelian.

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

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

\[
\text{Gal}(E_1/E_0) \cong \mathcal{M}/S(\Pi),
\] (34)

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

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

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

\[
\chi(\mathcal{M}) = C(F_a) \times \bar{H}_j,
\] (35)

where \( \bar{H} \) is an arbitrary maximal Abelian subgroup of \( GL(2, \mathbb{Z}/3\mathbb{Z}) \). One finds that \( \bar{H} \) must be conjugate to one of the three groups

\[
\bar{H}_4 = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle,
\] (36)

\[
\bar{H}_6 = \left\langle \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} \right\rangle,
\] (37)

\[
\bar{H}_8 = \left\langle \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \right\rangle,
\] (38)

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

\[
H_j = \chi^{-1}(C(F_a) \times \bar{H}_j), \quad j = 4, 6, 8.
\] (39)
We say that an orbit is type-$a_j$ if $\text{Gal}(\mathbb{E}_i/\mathbb{E}_0)$ is isomorphic to $\mathcal{H}_j$. Of the known cases, orbit 12$b$ is type-$a_4$ while orbits 21$e$, 48$g$ are type-$a_8$. It is an open question whether there exists any type-$a_9$ orbit.

In [19] the following, weaker conjecture was proposed for strongly-centred type-$a$ fiducials:

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

\[
\text{Gal}(\mathbb{E}_i/\mathbb{E}_0) \cong A/S(\Pi),
\]

where

\[
A = \{ rI + sG : r, s \in \mathbb{Z}/d'\mathbb{Z} \text{ and } rI + sG \in \text{GL}(2, \mathbb{Z}/d'\mathbb{Z}) \}
\]

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

To see that this conjecture is indeed weaker, let $\Pi$ be a strongly centred type-$a$ fiducial satisfying conjecture 1. Then $\text{Gal}(\mathbb{E}_i/\mathbb{E}_0) \cong H_j/S(\Pi)$ for some $j$. The fact that $F_a$ is conjugate to the Zauner matrix in dimension $n$ means, in view of lemma 12 in [26],

\[
C(F_a) = \{ rI + sF_a : r, s \in \mathbb{Z}/n'\mathbb{Z} \text{ and } rI + sF_a \in \text{GL}(2, \mathbb{Z}/n'\mathbb{Z}) \}.
\]

Define

\[
G = \frac{2n + 1}{3}(F_a - I)
\]

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

\[
C(F_a) = \{ rI + sG : r, s \in \mathbb{Z}/n'\mathbb{Z} \text{ and } rI + sG \in \text{GL}(2, \mathbb{Z}/n'\mathbb{Z}) \}.
\]

It is straightforward to show that

\[
\mathcal{H}_j = \{ rI + sH_j : r, s \in \mathbb{Z}/3\mathbb{Z} \text{ and } rI + sH_j \in \text{GL}(2, \mathbb{Z}/3\mathbb{Z}) \},
\]

where

\[
H_4 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad H_6 = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}, \quad H_8 = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.
\]

Using the Chinese remainder theorem [37], one finds

\[
\mathcal{H}_j = \{ rI + sH_j : r, s \in \mathbb{Z}/d'\mathbb{Z} \text{ and } rI + sH_j \in \text{GL}(2, \mathbb{Z}/d'\mathbb{Z}) \},
\]

where

\[
H_j = \chi^{-1}(G, H_j).
\]

The fact that

\[
\chi(I + 3H_j) = (I + 3G, I) = \chi(F_a),
\]

means $I + 3H_j = F_a$. So $\Pi$ satisfies conjecture 2. To see that conjecture 2 is strictly weaker than conjecture 1, consider the order 2 subgroup of $\text{GL}(2, \mathbb{Z}/3\mathbb{Z})$;

\[
\mathcal{H}_2 = \{-I\} = \{ rI + sH_2 : r, s \in \mathbb{Z}/3\mathbb{Z} \text{ and } rI + sH_2 \in \text{GL}(2, \mathbb{Z}/3\mathbb{Z}) \},
\]

where $H_2 = -I$. Let $\mathcal{H}_2 = \chi^{-1}\left(\left(G, \mathcal{H}_2\right)\right)$. Then
\[ \mathcal{H}_2 = \{ rl + s\mathcal{H}_2 : r, s \in \mathbb{Z}/d'\mathbb{Z} \text{ and } rl + s\mathcal{H}_2 \in \text{GL}(2, \mathbb{Z}/d'\mathbb{Z}) \} \]  \hspace{1cm} (51)

where
\[ \mathcal{H}_2 = \chi^{-1}(G, \mathcal{H}_2). \] \hspace{1cm} (52)

Moreover, \( I + 3\mathcal{H}_2 = F_a \). So a fiducial for which \( \text{Gal}(E_1/E_0) \cong \mathcal{H}_2/S(\Pi) \) 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 \( \text{GL}(2, \mathbb{Z}/d'\mathbb{Z}) \), which means that \( \mathcal{H}_2 \) is contained in every maximal Abelian subgroup of \( \text{GL}(2, \mathbb{Z}/d'\mathbb{Z}) \) containing \( F_a \). In view of its importance, it may be worth noting that, in addition to equation (51), one also has
\[ \mathcal{H}_2 = \{ rl + sF_a : r, s \in \mathbb{Z}/d'\mathbb{Z} \text{ and } rl + sF_a \in \text{GL}(2, \mathbb{Z}/d'\mathbb{Z}) \}. \] \hspace{1cm} (53)

Indeed, it is easily verified that
\[ \mathcal{H}_2 = \frac{2n+1}{3}F_a + \frac{4n-1}{3}I \] \hspace{1cm} (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 \( F_a = I + 3\mathcal{H}_2 \), this means
\[ \{ rl + s\mathcal{H}_2 : r, s \in \mathbb{Z}/d'\mathbb{Z} \text{ and } rl + s\mathcal{H}_2 \in \text{GL}(2, \mathbb{Z}/d'\mathbb{Z}) \} = \{ rl + sF_a : r, s \in \mathbb{Z}/d'\mathbb{Z} \text{ and } rl + sF_a \in \text{GL}(2, \mathbb{Z}/d'\mathbb{Z}) \}. \] \hspace{1cm} (55)

### 4. Fields and multiplets

It is shown in [27] 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 of 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 \( E_{\text{min}} \) (respectively maximal field, denoted \( E_{\text{max}} \)). Associated with 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:

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 with a given field. One would like to know if this one-to-one correspondence between fields and multiplets persists in higher dimensions.
4. In the dimensions listed, \( E_{\text{min}} \) 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 \( E_{\min} \) of minimal degree over \( \mathbb{Q} \), and a unique field \( E_{\max} \) of maximal degree over \( \mathbb{Q} \). The field \( E_{\min} \) is always the ray class field over \( \mathbb{Q}(\sqrt{D}) \) with conductor \( d' \) and ramification at both infinite places. The field \( E_{\max} \) always contains \( E_{\min} \), and additional fields \( E \), when they exist, always lie between these two:

\[
E_{\min} \subseteq E \subseteq E_{\max}.
\]

### Table 1. Minimal and maximal multiplets for dimensions in which 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 \( E_{\max}/E_{\min} \), where \( E_{\max} \) is the maximal field and \( E_{\min} \) is the minimal one.

| \( d \) | Minimal multiplet | Maximal multiplet | \([E_{\max} : E_{\min}]\) |
|---|---|---|---|
| 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 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.

| \( d \) | Minimal multiplet | Intermediate multiplet (s) | Maximal multiplet | \([E_{\max} : E_{\min}]\) |
|---|---|---|---|---|
| 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 | 35bedg | 16 |
| 39 | 39ij | 39hf, 39gh | 39acde | 6 |
| 48 | 48g | 48e, 48f | 48abcd | 24 |
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 one-to-one correspondence between fields and multiplets. This information is summarized in table 2 and figure 1.

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 $\Pi_N$ is a known high precision numerical fiducial corresponding to an unknown exact fiducial $\Pi_E$ in dimension $d$. Suppose, in addition, that it is somehow known that $Q(\Pi_E, \tau)$ is the minimal SIC-field for dimension $d$. If the conjectures in [27, 28] are correct, $Q(\Pi_E, \tau)$ is then the ray class field over $Q(\sqrt{D})$ with conductor $d'$ and ramification at both infinite places. Using Magma, we can easily calculate a basis for the field over $Q$. Let $b_1, \ldots, b_n$ be such a basis. Then for all $j, k = 0, 1, \ldots, d - 1$ there exist integers $\mu_0(j, k), \mu_1(j, k), \ldots, \mu_n(j, k)$ such that

$$\mu_0(j, k) \langle j \mid \Pi_E \mid k \rangle - \sum_{r=1}^{n} \mu_r(j, k) b_r = 0. \quad (57)$$

For the numerical fiducial, one then has

$$\mu_0(j, k) \langle j \mid \Pi_N \mid k \rangle - \sum_{r=1}^{n} \mu_r(j, k) b_r \approx 0 \quad (58)$$

to a high degree of precision. If the precision is sufficiently great we can use an integer relation algorithm to find the integers $\mu_r(j, k)$, $j$. Substituting these integers in

$$\sum_{r=1}^{n} \frac{\mu_r(j, k)}{\mu_0(j, k)} b_r \quad (59)$$

gives us the exact matrix element $\langle j \mid \Pi_E \mid k \rangle$ for each $j, k$. There are three problems with this ‘brute-force’ approach:

- It requires us to guess which numerical fiducials correspond to an exact fiducial generating the ray-class field.
- We do not currently have a conjecture for $Q(\Pi_E, \tau)$ 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, was actually calculated last).

5.1. Method 1

We describe the method as it applies for a type-$\alpha$ fiducial, and then indicate the modifications needed to deal with a type-$\beta$ fiducial at the end. Define

$$\chi_{E,p} = \Tr(D_p \Pi_E) \quad \chi_{N,p} = \Tr(D_p \Pi_N). \quad (60)$$
Let $C(\Pi_E)$ be the centralizer of the symmetry group $S(\Pi_E)$, and let $O_1 \ldots O_m$ be the orbits of $(\mathbb{Z}/d'\mathbb{Z})^2$ under the action of $C(\Pi_E)$. If $d \neq 0 \mod 3$ (respectively $d = 0 \mod 3$) let $S_{E,j}$ be the set of distinct numbers $\chi_{E,p}$ (respectively $\chi_{E,p}^3$) obtained as $p$ runs over $O_j$, and define

$$Q_{E,j}(x) = \prod_{s \in S_{E,j}} (x - s).$$  \hfill (61)

Of course, we do not know the overlaps $\chi_{E,p}$, so the polynomial $Q_{E,j}(x)$ is also unknown. However, $S(\Pi_E)$, $C(\Pi_E)$ and the orbits $O_1 \ldots O_m$ can all be calculated just from a knowledge of $\Pi_N$. Let $S_{N,j}$ be the set of distinct numbers $\chi_{N,p}$ ($\chi_{E,p}^3$ if $d = 0 \mod 3$) obtained as $p$ runs over $O_j$, and define

---

\footnote{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 $g(\chi_p)$ only equals $\chi_{G,p}$ up to a cube root of unity \cite{26} (where $g$ is any element of $\text{Gal}(E_1/E_0)$), and the coefficients of $Q(x)$ are consequently guaranteed to be in the field $E_0$. Cubing the overlaps obviates this difficulty.}
\[ Q_{N,j}(x) = \prod_{s \in S_{N,j}} (x - s). \] (62)

The known polynomials \( Q_{N,j}(x) \) will then be high precision approximations to the unknown polynomials \( Q_{E,j}(x) \). If the conjecture that Gal\((\mathbb{E}_1/\mathbb{E}_0)\) is isomorphic to \( C(II)/S(II) \) is correct (see equation (25)), then the coefficients of \( Q_{E,j}(x) \) 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), the degree of \( Q_{E,j}(x) \), and consequently the degree of its numerical approximant \( Q_{N,j}(x) \), is also comparatively small. It is consequently possible to use an integer relation algorithm to calculate the coefficients of \( Q_{E,j}(x) \) from those of \( Q_{N,j}(x) \) without knowing the field in advance, and without an impractically high degree of precision and CPU time (using, for instance, the Magma function \texttt{MinimalPolynomial} or the Mathematica function \texttt{RootApproximant})

In practice, it is most efficient to use this method to find the next-to-leading coefficient of the lowest degree polynomial \( Q_{E,j}(x) \) (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 \texttt{IntegerRelation} (in Magma) or \texttt{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 \( Q_{E,j}(x) \) was \( \sim 1 \) s or less in every case. The precision needed was \( 10^5 \) decimal digits or fewer. We then used Magma to construct 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 \( Q_{E,j}(x) \) over this field. If the fiducial was not minimal, we factored the \( Q_{E,j}(x) \) 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 could then be expressed in terms of the generators. This part of the calculation took \( \sim 1 \) day of CPU time. Finally, the exact fiducial was calculated from the overlaps using equation (4).

For a type-\( \alpha \) fiducial, the above procedure needs to be modified slightly. This is because, if conjecture 1 is correct, Gal\((\mathbb{E}_1/\mathbb{E}_0)\) is isomorphic to \( \mathcal{M}/S(\Pi_E) \) for some maximal Abelian subgroup \( \mathcal{M} \) which, unlike \( C(\Pi_E) \) for a type-\( \beta \) fiducial, cannot be determined 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 \( H_2 \), which can be calculated in advance of knowing the exact fiducial from equation (53). The calculation then mirrors the calculation for a type-\( \beta \) fiducial, but using \( H_2 \) instead of \( C(\Pi_E) \). Specifically, let \( \mathcal{O}_1 \ldots \mathcal{O}_m \) be the orbits of \( (\mathbb{Z}/d'^2\mathbb{Z})^2 \) under the action of \( H_2 \), and let \( S_{E,j} \) be the set of distinct numbers \( \chi^{e,p}_j \) obtained as \( p \) runs over \( \mathcal{O}_j \); define \( Q_{E,j}(x) = \prod_{s \in S_{E,j}} (x - s) \). Let

\[
\mathcal{F} : \text{Gal}(\mathbb{E}_1/\mathbb{E}_0) \to \mathcal{M}/S(\Pi_E). \] (63)

Then the coefficients of \( Q_{E,j}(x) \) are in \( \mathbb{F} \), the fixed field of \( \mathcal{F}^{-1}(H_2) \). It follows from the results in section 3 that \( [\mathcal{M} : H_2] \leq 4 \). Consequently, the degree of \( \mathbb{F}/\mathbb{Q} \) is no more than four 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-\( \beta \) fiducial to determine the coefficients of the \( Q_{E,j}(x) \) from their approximants \( Q_{N,j}(x) \), and hence to determine the exact fiducial.

There are two main steps to the method just described. The first step is to find the coefficients of the polynomials \( Q_{E,j}(x) \) using an integer relation algorithm; the second is to factor the polynomials. As we noted above, the first step is fast, taking \( \lesssim 1 \) s 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 calculate the cubed overlaps first and then take the cube root at the end of the calculation.

5.2. Method 2

As before we first describe the 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 \( Q_{E_j} (x) \)—with, however, the difference that even when \( d = 0 \mod 3 \), the numbers \( s \) in equation (62) are the overlaps themselves (as opposed to their cubes). We then use the \textit{Magma} function \texttt{MinimalPolynomial} to obtain exact versions of the coefficients. If \( d \neq 0 \mod 3 \), we take \( E_0 \) 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 \( p = 0 \mod \frac{d}{3} \), and then take the desired strongly centred fiducial to be the one for which the polynomials obtained by applying \texttt{MinimalPolynomial} to the coefficients have lowest degree. If the SIC is minimal, \( E_1 \) can be taken to be the appropriate ray-class field. Otherwise, \( E_1 \) is an extension of this field. We find a set of generators for the extension by factoring some of the polynomials \( Q_{E_j} (x) \). It is crucial to the success of this method that in practice one does not need to factor all the \( Q_{E_j} (x) \). 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 \( Q_{E_j} (x) \) of highest degree, this method would have few if any advantages over Method 1 described above.

Once the fields \( E_0 \) and \( E_1 \) have been determined, we use the conjectured isomorphism of equation (25) to reduce the rest of the calculation to a problem in linear algebra. Let \( b_1, \ldots, b_n \) be a basis for the extension \( E_1 / E_0 \), let \( g_1, \ldots, g_n \) and \( G_1 \langle \Pi_E \rangle, \ldots, G_n \langle \Pi_E \rangle \) be explicit listings of the elements of \( \text{Gal}(E_1 / E_0) \) and \( C(\Pi_E) / S(\Pi_E) \) respectively, and let \( \mathcal{P} \) be the set of permutations \( f \) with the property that

\[
g_j \rightarrow G_{f(j)} \langle \Pi_E \rangle
\]  

is an isomorphism of \( \text{Gal}(E_1 / E_0) \) onto \( C(\Pi_E) / S(\Pi_E) \). Given any overlap \( \text{Tr}(D_p \Pi_E) \)

\[
\sum_{k=1}^{n} s_k b_k = \text{Tr}(D_p \Pi_E) \tag{65}
\]

for some \( s_k \in E_0 \). The conjecture is that for some permutation \( f \in \mathcal{P} \),

\[
g_j (\text{Tr}(D_p \Pi_E)) = \text{Tr}(D_{G_{f(j)} } \Pi_E)
\]  

for all \( j \). If correct, this means

\[
S = B^{-1} V_f
\]

where \( B \) is the matrix

\[
B = \begin{pmatrix}
  g_1(b_1) & g_1(b_2) & \cdots \\
  g_2(b_1) & g_2(b_2) & \cdots \\
  \vdots & \vdots & \ddots
\end{pmatrix}
\]  

(68)
and $S$, $V_f$ are the vectors

$$S = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \end{pmatrix}, \quad V_f = \begin{pmatrix} \text{Tr}(D_{G_{(1)}} p \Pi_E) \\ \text{Tr}(D_{G_{(2)}} p \Pi_E) \\ \vdots \end{pmatrix}. \quad (69)$$

Of course, we do not know the permutation $f$. To find it, we consider in turn each of the permutations in $P$, and use it in conjunction with equation (67) 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 $e_1, \ldots, e_m$ be a basis for $E_0/Q$. We use the Magma function `IntegerRelation` to find integers $l_{j,0}, \ldots, l_{j,m}$ solving the equation

$$l_{j,0}s_j - l_{j,1}e_1 - \cdots - l_{j,m}e_m = 0.$$ 

We find that for one choice of permutation $f$, the norms $\sqrt{l_{j,0}^2 + \cdots + l_{j,m}^2}$ 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 $\text{Gal}(E_1/E_0)$ and $C(\Pi_E)/\mathcal{S}(\Pi_E)$, and

$$S = \sum_{a=1}^m e_a \begin{pmatrix} l_{1,a} \\ l_{2,a} \\ \vdots \end{pmatrix}, \quad (70)$$

to be the exact value of the vector $S$. We then invert equation (67) to obtain the exact value of the overlaps $\text{Tr}(D_{G_{(1)}} p \Pi_E)$. By repeating this procedure, we obtain an exact value for every overlap and use equation (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.

**Acknowledgments**

This research was supported in part by the Australian Research Council via EQuS project number CE11001013. SF acknowledges support from an Australian Research Council Future Fellowship FT130101744.

**Appendix. Results**

We used the method described in section 5 to calculate exact fiducials for $EC(d)$ orbits 17abc, 18ab, 19abcd, 20ab, 21abcde. The fiducials themselves are available online [32]. The purpose of this appendix is to describe the associated fields and Galois groups, and the isomorphism of equation (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 $\Pi_{sc}$ be an exact version of the Scott–Grassl numerical fiducial in such a dimension, and let $\Pi_{sc}$ be the strongly-centred fiducial we have calculated. Then

$$\Pi_{sc} = U \Pi_{sc} U^\dagger \quad (A.1)$$

$U$ is the orthogonal transformation that strongly-centres $\Pi_{sc}$. To find $U$, we choose a basis for $E_0$, and find a basis for $E_0/Q$ that is strongly-centred. We then use the Magma function `IntegerRelation` to find integers $l_{j,0}, \ldots, l_{j,m}$ solving the equation

$$l_{j,0}s_j - l_{j,1}e_1 - \cdots - l_{j,m}e_m = 0.$$ 

We find that for one choice of permutation $f$, the norms $\sqrt{l_{j,0}^2 + \cdots + l_{j,m}^2}$ 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 $\text{Gal}(E_1/E_0)$ and $C(\Pi_E)/\mathcal{S}(\Pi_E)$, and

$$S = \sum_{a=1}^m e_a \begin{pmatrix} l_{1,a} \\ l_{2,a} \\ \vdots \end{pmatrix}, \quad (70)$$

to be the exact value of the vector $S$. We then invert equation (67) to obtain the exact value of the overlaps $\text{Tr}(D_{G_{(1)}} p \Pi_E)$. By repeating this procedure, we obtain an exact value for every overlap and use equation (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.
Table A1. Displacement operators converting Scott–Grassl numerical fiducials to strongly-centred ones in dimensions divisible by 3.

| Orbit | U | Orbit | U | Orbit | U | Orbit | U |
|-------|---|-------|---|-------|---|-------|---|
| 15a   | D_{15,10} | 21bcd | D_{14,17} | 30d | D_{20,20} | 39k | D_{26,0} |
| 15c   | D_{10,5}  | 21e   | D_{7,0}   | 39abcd | D_{26,13} | 39j | D_{26,26} |
| 15bd  | l        | 24abc | D_{8,16}  | 39e   | l      | 39j   | D_{13,13} |
| 18ab  | D_{12,6} | 30ac  | D_{30,10} | 39f   | D_{13,26} | 48adf | l  |
| 21a   | D_{7,14} | 30b   | l        | 39g   | D_{0,13} | 48bc  | D_{16,32} |
|       |          |       |          |       |        |       | 48e   | D_{16,16} |

Table A2. a, r and t generators.

| d   | a     | r_1 | r_2 | r_3 | r_4 | ir_3 | t           | minimal polynomial of t over Q(a, r_1, ..., r_t) |
|-----|-------|-----|-----|-----|-----|------|-------------|-----------------------------------------------|
| 15  | √3    | √3  |     |     |     |      |             | 8x^2 - 2(r_1 - 1)x - (r_1 + 3)                |
| 17  | √7    | √3  | √7  |     |     |      |             | x^8 + 1/3(r_2 - 17)x^6 - 1/3(r_2 - 51)x^4 + 1/72(7r_2 - 34)x^2 - 1/256(4r_2 - 17) |
| 18  | √285  | √3  | √3  |     |     |      |             | 512x^8 - 256x^6 - 1024x^2 + 448x^6 + 672x^3 + 240x^4 + 160x^3 + 40x^2 + 10x + 1 |
| 20  | √337  | √3  | √6  | √3  |     |      |             | x^5 - 5/9r_2r_3(r_4 + 1)x + 5/9(r_4 - 1)     |
| 21  | √11   | √3  | √7  |     |     |      |             | x^5 - 5/9(r_1r_2 - 1)x^2 - 5/9(r_1r_2 + 1)x + 5/9(r_1r_2 + 5) |
| 24  | √11   | √2  | √3  | √3  |     |      |             | 8x^2 - (4 + r_1 + r_2r_2)                   |
| 28  | √29   | √2  | √7  | √3  |     |      |             | 16x^4 - 4r_1(r_2 - 1)x^2 - 4(r_2 + 1)x + r_1(r_2 + 3) |
| 30  | √93   | √3  | √3  |     |     |      |             | 8x^2 - 2r_1(r_2 + 1)x + r_2 + 1            |
| 35  | √2   | √5  | √7  | √3  |     |      |             |                                             |
| 39  | √10   | √20 | √3  |     |     |      |             |                                             |
| 48  | √3   | √2  | √3  | √103|     |      |             |                                             |

where U is the displacement operator specified in table A1.

The multiplet structure for these dimensions is specified in table 2. The maximal field for each dimension is specified in tables A2–A6, using the same notational conventions as in [26] to denote the field generators:

- a denotes D, the square-free part of (d - 3)(d + 1).
- r_1, ..., r_t denote square roots of integers.
- t denotes cos π/d or sin π/d.
- b_1, ..., b_4 denote numbers constructed recursively from Q(a, r_1, ..., r_t, l) by taking sums, products and roots.
- i denotes the square root of -1.

The a, r and t generators are tabulated in table A2; the b generators in tables A3–A5. The minimal polynomials of the cubic b generators are tabulated in table A6. The fields in the tower of equation (14) are tabulated in table A7, for the maximal, minimal and intermediate multiplets in each dimension.
Table A3. \( b \) generators for \( d = 15, 17–19 \).

| \( d \) | \( b_1 \) | \( b_2 \) | \( b_3 \) | \( b_4 \) |
|-------|-------|-------|-------|-------|
| 15    | \( i(-30 + 28a - 6r_1 + 4ar_1 + (-60 + 24a - 12r_1 + 8ar_1)t)\)\( ^\dagger \) | \( 2\text{Re}\left((10 + 30i)\right)^\dagger \) | \( i\sqrt{2a} \) | \( \sqrt{a + 2} \) |
| 17    | \( 32(-1938 + 765a + 462r_2 - 181ar_2 - 2(171 - 72a - 67r_2 + 32ar_2)t + 2(5844 - 2303a - 1404r_2 + 551ar_2)t^2 + 4(173 - 64a - 229r_2 + 112ar_2)t^3 - 8(2592 - 1021a - 624r_2 + 245ar_2)t^4 - 16(-39 + 24a - 113r_2 + 56ar_2)t^5 + 32(348 - 137a - 84r_2 + 33ar_2)t^6 + 512(-2 + a)(1 + r_2)t^7)\)\( ^\dagger \) | \( 2\text{Re}\left((17(44 + 3i\sqrt{21}))\right)^\dagger \) | \( 2\text{Re}\left((\frac{1}{2}(1 + i\sqrt{3}))\right)^\dagger \) |
| 18    | \( 32i((a + 15)(r_1 + 5))^\dagger \) | \( 2\text{Re}\left((-11 + i\sqrt{35})\right)^\dagger \) | \( 2\text{Re}\left((38(13 + 3i\sqrt{3}))\right)^\dagger \) | \( 2\text{Re}\left((\frac{1}{2}(1 + i\sqrt{3}))\right)^\dagger \) |
| 19    | \( i(2a + 1)^\dagger \) | | | |
Table A4. $b$ generators for $d = 20, 21, 24, 28.$

| $d$   | $b_1$                              | $b_2$                                | $b_3$                               | $b_4$                              |
|-------|------------------------------------|--------------------------------------|-------------------------------------|------------------------------------|
| 20    | $i((a + 17)(r_1 + 17))^\frac{1}{2}$ | $i((-33 + 66a - 22r_1 + 33ar_1 - (11 + 8a + 15ar_1)b_1)^\frac{1}{2}$ | $\left(\frac{1}{3}(4(-4 - 9a + i\sqrt{465 - 72a}))\right)^{\frac{1}{2}}$ | $\text{Re}\left(\frac{1}{3}(4(-4 - 9a + i\sqrt{465 - 72a})\right)^{\frac{1}{2}}$ |
| 21    | $(9 + 4r_1)^\frac{1}{2}$           | $i\sqrt{a - 3}$                      | $\text{Re}\left((1 - i\sqrt{9})\right)^{\frac{1}{2}}$ | $\text{Re}\left((1 + i\sqrt{9})\right)^{\frac{1}{2}}$ |
| 24    | $i\sqrt{a + 1}$                    | $\sqrt{(4 + r_1)(3 + r_2)}$         | $\text{Re}\left((1 + i\sqrt{9})\right)^{\frac{1}{2}}$ | $\text{Re}\left((189 + 21i\sqrt{87})\right)^{\frac{1}{2}}$ |
| 28    | $i\sqrt{a + 5}$                    | $\text{Re}\left((1 + i\sqrt{9})\right)^{\frac{1}{2}}$ | $\text{Re}\left((189 + 21i\sqrt{87})\right)^{\frac{1}{2}}$ | $\text{Re}\left((189 + 21i\sqrt{87})\right)^{\frac{1}{2}}$ |
Table A5. \( b \) generators for \( d = 30, 35, 39, 48. \)

| \( d \) | \( b_1 \) | \( b_2 \) | \( b_3 \) | \( b_4 \) | \( b_5 \) | \( b_6 \) |
|-------|-------|-------|-------|-------|-------|-------|
| 30    | \( \frac{1}{2}(4(-5r_1r_2 + (4a - 23)r_3) + t + 2((-4a + 21)r_2 - 8a + 111))^{\frac{1}{2}} \) | \( 2\text{Re}((1 + 2i\sqrt{3}t)^{\frac{1}{2}}) \) | \( 2\text{Re}\left((4 + b_2 + i\sqrt{48 - 8b_2 - b_2^2})^{\frac{1}{2}}\right) \) | \( 2\text{Re}\left((70 + 10i\sqrt{3})^{\frac{1}{2}}\right) \) | \( \frac{1}{2}\sqrt{2a + 18} \) | \( \frac{1}{2}\sqrt{245a - 7r_2b_3 - 49ar_1} \) |
| 35    | \( i\sqrt{2a + 1} \) | \( \sqrt{2r_2 + 78} \) | \( \sqrt{14(r_1 + 5)} \) | \( \text{Re}\left((28 + 84i\sqrt{3})^{\frac{1}{2}}\right) \) | \( \sqrt{3 - r_3} \) | \( \text{Re}\left((-676 + 10140i\sqrt{3})^{\frac{1}{2}}\right) \) |
| 39    | \( \sqrt{3r_1 + 18} \) | \( \sqrt{18r_2 - 78} \) | \( \sqrt{(4a + 15)(r_1 + 5)} \) | \( \text{Re}\left((2a - 5)(r_1 - 2)b_3 - (8a - 35) \right) \) | \( \text{Re}\left((r_1 - 10)^{\frac{1}{2}}\right) \) | \( \sqrt{(5(a + 1) - (3a - 5)r_3)b_4 - 2(a + 5)r_3} \) |
| 48    | \( i\sqrt{a - 1} \) | \( \sqrt{6 + r_1r_2} \) | \( \sqrt{6 - 2r_1r_2 + (r_2 - r_1)b_2} \) | \( \sqrt{2r_3 + 42} \) | \( \sqrt{3 - a} \) | \( \sqrt{210(3 - a)} \) |

\( a, b \) and \( r \) are as defined in Eq. (1) and the appendix.
Complex conjugation is given by $\bar{a} = a$, and it therefore completely specifies the Galois group for every multiplet in dimension $d$. For each generator $g$, and are chosen so that

\begin{align*}
\text{Gal}(\mathbb{E}/\mathbb{Q}) &= \langle g_1 \rangle \oplus \cdots \oplus \langle g_m \rangle \oplus \langle \bar{g}_1 \rangle \quad \text{(A.2)}
\end{align*}

(1) $g_a$ is an order 2 extension of the non-trivial element of $\text{Gal}(\mathbb{E}_c/\mathbb{Q})$.

(2) $g_1, \ldots, g_m, \bar{g}_1$ fix $\mathbb{E}_c$. In particular, they are mutually commuting. Moreover,

(3) $\bar{g}_1$ is the non-trivial element of $\text{Gal}(\mathbb{E}/\mathbb{E}_c)$.

(4) Complex conjugation is given by $g_r = g_a \bar{g}_1 g_a$ (see equation (15)).

For each generator $h$, Box 1 also tabulates the order of $h$, and $g_a h g_a$. In view of equation (A.2) 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 $EC(d)$ orbits in a multiplet. Finally, we tabulate the $G$ matrices defined

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|c|}
\hline
\text{Table A6. Minimal polynomials for cubic $b$ generators.} \\
\hline
\text{d} & \text{Generator} & \text{In terms of radicals} & \text{Minimal polynomial} \\
\hline
15 & $b_2$ & $2\text{Re}\left((10 + 30i)^\frac{1}{2}\right)$ & $x^3 - 30x - 20$ \\
17 & $b_2$ & $2\text{Re}\left((17(44 + 3i\sqrt{21}))^\frac{1}{2}\right)$ & $x^3 - 255x - 1496$ \\
18 & $b_2$ & $2\text{Re}\left((-11 + i\sqrt{95})^\frac{1}{2}\right)$ & $x^3 - 18x + 22$ \\
& $b_3$ & $2\text{Re}\left((\frac{1}{2}(1 + i\sqrt{95}))^\frac{1}{2}\right)$ & $x^3 - 18x - 3$ \\
19 & $b_2$ & $\text{Re}\left((38(13 + 3i\sqrt{5}))^\frac{1}{2}\right)$ & $x^3 - 228x - 988$ \\
20 & $b_2$ & $2\text{Re}\left((10(19 + 9i\sqrt{15}))^\frac{1}{2}\right)$ & $x^3 - 300x - 380$ \\
21 & $b_4$ & $\text{Re}\left((4(-4 - 9a + i\sqrt{465} - 72a))^\frac{1}{2}\right)$ & $x^3 - 21x + 9a + 4$ \\
24 & $b_3$ & $4\text{Re}\left((1 + i\sqrt{7})^\frac{1}{2}\right)$ & $x^3 - 24x - 16$ \\
28 & $b_3$ & $2\text{Re}\left((189 + 21i\sqrt{57})^\frac{1}{2}\right)$ & $x^3 - 126x - 378$ \\
30 & $b_2$ & $2\text{Re}\left((1 + 2i\sqrt{3})^\frac{1}{2}\right)$ & $x^3 - 15x - 2$ \\
& $b_3$ & $2\text{Re}\left((4 + b_2 + i\sqrt{48 - 8b_2 - b_2^2})^\frac{1}{2}\right)$ & $x^3 - 12x - 2b_2 - 8$ \\
& $b_4$ & $2\text{Re}\left((70 + 10i\sqrt{3})^\frac{1}{2}\right)$ & $x^3 - 60x - 140$ \\
35 & $b_2$ & $2\text{Re}\left((280 + 210i\sqrt{3})^\frac{1}{2}\right)$ & $x^3 - 210x - 560$ \\
& $b_4$ & $\text{Re}\left((28 + 84i\sqrt{3})^\frac{1}{2}\right)$ & $x^3 - 21x - 7$ \\
39 & $b_5$ & $\text{Re}\left((-676 + 10i40\sqrt{3})^\frac{1}{2}\right)$ & $x^3 - 507x + 169$ \\
& $b_6$ & $\text{Re}\left((180 - 4a + i\sqrt{6753} + 90a)^\frac{1}{2}\right)$ & $x^3 - 39x + a - 45$ \\
48 & $b_6$ & $2\text{Re}\left((7 + i\sqrt{13})^\frac{1}{2}\right)$ & $x^3 - 12x - 14$ \\
\hline
\end{tabular}
\end{table}
Table A7. 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 \( c = (r_2(a_1 + r_3 + 2a + 1)b_3 + 42r_1 + 70)b_5b_6 \).

| multiplet | \( E_0 \) | \( E_1 \) | \( E \) | deg(\( E/Q \)) |
|-----------|-----------|-----------|-----------|-------------|
| 15ac      | \( \mathbb{Q}(a, b_3) \) | \( \mathbb{E}_0(r_1, t, b_1, b_2, b_3) \) | \( E_1(i) \) | 384         |
| 15b       | \( \mathbb{Q}(a) \)     | \( \mathbb{E}_0(r_1, t, b_1, b_2, b_3) \) | \( E_1(i) \) | 192         |
| 15d       | \( \mathbb{Q}(a) \)     | \( \mathbb{E}_0(r_1, t, b_1, b_2) \)    | \( E_1(i) \) | 96          |
| 17ab      | \( \mathbb{Q}(a, r_1) \) | \( \mathbb{E}_0(r_2, t, b_1, b_2) \)    | \( E_1(i) \) | 768         |
| 17c       | \( \mathbb{Q}(a) \)     | \( \mathbb{E}_0(r_2, t, b_1, b_2) \)    | \( E_1(i) \) | 384         |
| 18ab      | \( \mathbb{Q}(a, r_1) \) | \( \mathbb{E}_0(r_2, t, b_1, b_2, b_3) \) | \( E_1(i) \) | 864         |
| 19bc      | \( \mathbb{Q}(a, r_2) \) | \( \mathbb{E}_0(r_1, t, b_1, b_2) \)    | \( E(i) \)  | 864         |
| 19a       | \( \mathbb{Q}(a) \)     | \( \mathbb{E}_0(r_1, t, b_1, b_2) \)    | \( E(i) \)  | 432         |
| 19d       | \( \mathbb{Q}(a) \)     | \( \mathbb{E}_0(t, b_1, b_2) \)        | \( E(ir_1) \)| 216         |
| 19e       | \( \mathbb{Q}(a) \)     | \( \mathbb{E}_0(t, b_1) \)              | \( E(ir_1) \)| 72          |
| 20ab      | \( \mathbb{Q}(a, r_1) \) | \( \mathbb{E}_0(r_2, r_3, r_4, t, b_1, b_2, b_3) \) | \( E_1(i) \) | 1536        |
| 21abcd    | \( \mathbb{Q}(a, r_1, b_1) \) | \( \mathbb{E}_0(r_2, t, b_2, b_3, b_4) \) | \( E_1(i) \) | 1152        |
| 21e       | \( \mathbb{Q}(a) \)     | \( \mathbb{E}_0(r_1, r_2, t, b_1, b_2, b_3) \) | \( E_1(i) \) | 384         |
| 24ab      | \( \mathbb{Q}(a, r_3) \) | \( \mathbb{E}_0(r_1, r_2, t, b_1, b_2, b_3, b_4) \) | \( E_1(i) \) | 1536        |
| 24c       | \( \mathbb{Q}(a) \)     | \( \mathbb{E}_0(r_1, r_2, t, b_1, b_2, b_3) \) | \( E_1(i) \) | 384         |
| 28ab      | \( \mathbb{Q}(a, r_3) \) | \( \mathbb{E}_0(r_1, r_2, t, b_1, b_2, b_3, b_4) \) | \( E_1(i) \) | 2304        |
| 28c       | \( \mathbb{Q}(a) \)     | \( \mathbb{E}_0(r_1, r_2, t, b_1, b_2, b_3) \) | \( E_1(i) \) | 576         |
| 30abc     | \( \mathbb{Q}(a, b_2) \) | \( \mathbb{E}_0(r_1, r_2, t, b_1, b_2, b_3, b_4, b_5) \) | \( E_1(i) \) | 3456        |
| 30d       | \( \mathbb{Q}(a) \)     | \( \mathbb{E}_0(r_1, r_2, t, b_1, b_2, b_3, b_4, b_5) \) | \( E_1(i) \) | 1152        |
| 35bcdg    | \( \mathbb{Q}(a, r_3, b_3) \) | \( \mathbb{E}_0(r_1, r_2, b_1, b_2, b_3, b_4, b_5, b_6) \) | \( E_1(i) \) | 4608        |
| 35af      | \( \mathbb{Q}(a, r_3) \) | \( \mathbb{E}_0(r_1, r_2, b_1, b_2, b_3, b_4, b_5b_6) \) | \( E_1(i) \) | 2304        |
| 35e       | \( \mathbb{Q}(a) \)     | \( \mathbb{E}_0(r_1, r_2, r_3, b_1, b_2, b_3, b_4, c) \) | \( E_1(i) \) | 1152        |
| 35h       | \( \mathbb{Q}(a) \)     | \( \mathbb{E}_0(r_1, r_2, b_1, b_2, b_3, b_4, b_6) \) | \( E_1(i) \) | 1152        |
| 35i       | \( \mathbb{Q}(a) \)     | \( \mathbb{E}_0(r_1, r_2, b_1, b_2, b_3, b_4) \) | \( E_1(i) \) | 576         |
| 35j       | \( \mathbb{Q}(a) \)     | \( \mathbb{E}_0(r_1, b_1, b_2, b_3, b_4) \) | \( E_1(i) \) | 288         |
| 39acde    | \( \mathbb{Q}(a, r_1, b_1) \) | \( \mathbb{E}_0(r_2, b_3, b_4, b_5, b_6, b_7) \) | \( E(ir_1) \)| 4608        |
| 39bf      | \( \mathbb{Q}(a, r_1) \) | \( \mathbb{E}_0(r_2, b_3, b_4, b_5, b_6, b_7) \) | \( E(ir_1) \)| 2304        |
| 39gh      | \( \mathbb{Q}(a, r_1) \) | \( \mathbb{E}_0(r_2, b_3, b_4, b_5, b_6, b_7) \) | \( E(ir_1) \)| 1536        |
| 39ij      | \( \mathbb{Q}(a, r_1) \) | \( \mathbb{E}_0(r_2, b_3, b_4, b_5, b_6, b_7) \) | \( E(ir_3) \)| 768         |
| 48abcd    | \( \mathbb{Q}(a, r_3, b_4) \) | \( \mathbb{E}_0(r_1, r_2, t, b_1, b_2, b_3, b_5, b_6) \) | \( E_1(i) \) | 12288       |
| 48e       | \( \mathbb{Q}(a) \)     | \( \mathbb{E}_0(r_1, r_2, r_3, t, b_1, b_2, b_3, b_4, b_5) \) | \( E_1(i) \) | 4096        |
| 48f       | \( \mathbb{Q}(a) \)     | \( \mathbb{E}_0(r_1, r_2, t, b_1, b_2, b_3, b_6) \) | \( E_1(i) \) | 1536        |
| 48g       | \( \mathbb{Q}(a) \)     | \( \mathbb{E}_0(r_1, r_2, t, b_1, b_2, b_3, b_4) \) | \( E_1(i) \) | 512         |

by equation (21). In dimension \( d \), let \( dx, dy \) be two \( \text{EC}(d) \) orbits such that generator \( g_j \) takes \( dx \) to \( dy \), and let \( \Pi_1, \Pi_2 \) be the exact fiducials on these orbits given in [32]. Then

\[
g_j(\text{Tr}(D\Pi_1)) = \text{Tr}(Dg_j\Pi_1)
\]  

(A.3)

where \( G_{ij} \) are the matrices tabulated in box 3. We only tabulate the matrices for cases where the action is non-trivial, so that \( g_j(\Pi_1) \neq \Pi_1 \). The \( F \) matrices in equation (20) can then be obtained by inverting equation (22).
### Dimension 15

1. \[
\begin{array}{cccccccccc}
\ h & a & r_1 & t & b_1 & b_2 & b_3 & b_4 & i & \text{Order} & g_u h_{g_u^{-1}} \\
\ g_u & -a & r_1 & t & b_1 & b_2 & b_3 & b_4 & -i & 2 & g_u \\
\ g_1 & a & r_1 & r_1 & b_1 & b_2 & b_3 & -b_4 & i & 2 & g_1 \\
\ g_2 & a & -r_1 & t' & b_1' & b_2' & b_3 & b_4 & i & 24 & g_2 \\
\ g_3 & a & r_1 & t & b_1 & b_2 & -b_3 & b_4 & i & 2 & g_3 \\
\ \bar{g}_1 & a & r_1 & t & b_1 & b_2 & b_3 & b_4 & -i & 2 & g_c = \bar{g}_1^2 \bar{g}_3 \bar{g}_1 \\
\end{array}
\]

\[ t' = \cos \frac{5\pi}{12} \]

\[ b_1' = \sqrt{30 + 28a + 6r_1 + 4ar_1 + (60 + 24a + 12r_1 + 8ar_1)i} \]

\[ b_1' = i\sqrt{16a + (60 - 32a - 36r_1 + 16ar_1)i} \]

\[ b_2' = 2 \text{Re} \left( e^{i\pi/4} (10 + 30i) \right) \]

\[ b_3' = \sqrt{2a} \]

\[ b_4' = -a + 2 \]

2. Orbit Gal(\mathbb{E}/\mathbb{Q}) \quad \text{Gal(\mathbb{E}/\mathbb{E}_0)}

- 15ac \quad \langle g_u, g_1, g_2, g_3, g_1 \rangle \quad \langle g_2, g_3, g_1 \rangle
g_1 \text{ interchanges } 15a, 15c \text{ and restricts to the identity on } 15b, 15d; g_3 \text{ restricts to the identity on } 15d

- 15b \quad \langle g_u, g_2, g_3, g_1 \rangle \quad \langle g_2, g_3, g_1 \rangle

- 15d \quad \langle g_u, g_2, g_1 \rangle \quad \langle g_2, g_1 \rangle

3. \[
\begin{array}{cccccc}
G_{a1} = G_{a1} & G_{a2} = G_{a2} & G_{a3} = G_{a2} & G_{a3} = G_{a3} = G_{a3} \\
(0 & 1 & 1 & 0) & (1 & 12 & 3 & 14) & (0 & 4 & 11 & 4)
\end{array}
\]

### Dimension 17

1. \[
\begin{array}{cccccccccc}
\ h & a & r_1 & r_2 & t & b_1 & b_2 & i & \text{Order} & g_u h_{g_u^{-1}} \\
\ g_u & -a & r_1 & r_2 & t & b_1 & b_2 & i & 2 & g_u \\
\ g_1 & a & -r_1 & r_2 & t & b_1 & b_2 & i & 2 & g_1 \\
\ g_2 & a & r_1 & -r_2 & t' & b_1' & b_2' & i & 96 & g_2^17 \bar{g}_1 \\
\ g_3 & a & r_1 & r_2 & t & b_1 & b_2 & -i & 2 & g_c = \bar{g}_2^4 \bar{g}_1 \\
\end{array}
\]

\[ t' = \sin \frac{5\pi}{12} \]

\[ b_1' = 32 \left( 1938 + 765a - 462r_2 - 181ar_2 - 2(-171 - 72a + 67r_2 + 32ar_2)i - 5844 - 2303a + 1404r_2 + 551ar_2)i^2 + 8(-173 - 64a + 229r_2 + 112ar_2)i^3 + 8(-2592 - 1021a + 624r_2 + 245ar_2)i^4 - 16(39 + 24a + 113r_2 + 58ar_2)i^5 + 32(-348 - 157a + 84r_2 + 33ar_2)i^6 + 512(2 + a)(1 + r_2)i^7 \right) \]

\[ b_1' = 32(1(-204 + 119a + 60r_2 - 33ar_2) - 8(-39 + 20a - 3r_2)i + 16(-81 + 25a - 39r_2 + 17ar_2)i^2 + 4(-491 + 240a - 51r_2)i^3 + 8(-600 - 211a - 216r_2 + 91ar_2)i^4 - 16(-234 + 112a - 27r_2)i^5 + 96(-36 + 13a - 12r_2 + 5ar_2)i^6 + 256(-9 + 4a - r_2)i^7) \]

\[ b_2' = 2 \text{Re} \left( e^{i\pi/4} (1744 + 3i\sqrt{17}) \right) \]
2. Orbit Gal\(\mathbb{E}/\mathbb{Q}\) Gal\(\mathbb{E}/\mathbb{E}_0\) \(g_1\) interchanges orbits 17a, 17b and restricts to the identity on 17c.

\[
17ab \quad \langle g_a, g_1, g_2, g_1 \rangle \quad \langle g_2, g_1 \rangle \\
17c \quad \langle g_a, g_2, g_1 \rangle \quad \langle g_2, g_1 \rangle
\]

3. 

| \(G_{a1}\) | \(G_{b1}\) | \(G_{a2}\) | \(G_{b2}\) | \(G_{c2}\) |
|---|---|---|---|---|
| \((2, 7)\) | \((15, 10)\) | \((1, 11)\) | \((6, 16)\) | \((1, 11)\) |

Dimension 18

1. \(h\) \(t\) \(r_1\) \(r_2\) \(b_1\) \(b_2\) \(b_3\) \(i\) Order \(g_a h g_a^{-1}\) \(r' = \cos \frac{11\pi}{18}\)

\[
g_a = a - r_1 \quad b_1' = b_2 \quad b_2' = b_3 \quad b_3' = i \quad g_a = g_a \\
g_1 = a - r_1 \quad b_1' = b_2 \quad b_2' = b_3 \quad b_3' = i \quad g_1 = g_1 \\
g_2 = a \quad r_1 = -r_1 \quad b_1 = b_2 - b_3 \quad b_3 = i \quad g_2 = g_2 \\
g_3 = a \quad r_1 = -r_1 \quad b_1 = b_2 - b_3 \quad b_3 = i \quad g_3 = g_3 \\
g_1 = a \quad r_1 = r_2 \quad t = b_1 - b_2 - b_3 \quad i = 2 \quad g_c = g_1^3 g_1
\]

2. Orbit Gal\(\mathbb{E}/\mathbb{Q}\) Gal\(\mathbb{E}/\mathbb{E}_0\) \(g_1\) interchanges orbits 18a, 18b.

\[
18ab \quad \langle g_a, g_1, g_2, g_3, g_1 \rangle \quad \langle g_1, g_2, g_3, g_1 \rangle
\]

3. 

| \(G_{a1}\) | \(G_{b1}\) | \(G_{a2}\) | \(G_{b2}\) | \(G_{c3}, G_{b3}\) |
|---|---|---|---|---|
| \((1, 8)\) | \((4, 3)\) | \((9, 17)\) | \((1, 9)\) | \((0, 5)\) |
| \((9, 35)\) | \((7, 32)\) | \((19, 26)\) | \((27, 10)\) | \((31, 5)\) |
Dimension 19

1. \[
\begin{array}{cccccccc}
  h & a & r_1 & r_2 & t & b_1 & b_2 & ir_1 & \text{Order} \\
  g_a & -a & r_1 & r_2 & t & b_1' & b_2 & ir_1 & 2 & g_a \\
  g_1 & a & r_1 & -r_2 & t & b_1 & b_2 & ir_1 & 2 & g_1 \\
  g_2 & a & r_1 & r_2 & t' & -b_1 & b_2 & ir_1 & 18 & g_2 \\
  g_3 & a & r_1 & r_2 & t & b_1 & b_2' & ir_1 & 3 & g_3 \\
  g_4 & a & -r_1 & r_2 & t & b_1 & b_2 & ir_1 & 2 & g_4 \\
  \bar{g}_1 & a & r_1 & r_2 & t & b_1 & b_2 & -ir_1 & 2 & \bar{g}_1 = g_9^1 \\
\end{array}
\]

\[ t' = \cos \frac{\pi}{19} \]

\[ b'_1 = (2a - 1)^{\frac{1}{2}} \]

\[ b'_2 = 2 \text{Re} \left( e^{\frac{\pi}{3} (38(13 + 3i\sqrt{5}))^{\frac{1}{4}}} \right) \]

2. Orbit  \begin{array}{ccc}
  \text{Gal}(\mathbb{E}/\mathbb{Q}) & \text{Gal}(\mathbb{E}/\mathbb{E}_0) \\
  19bc & \langle g_a, g_1, g_2, g_3, g_4, g_1 \rangle & \langle g_2, g_3, g_4, g_1 \rangle \\
  19a & \langle g_a, g_2, g_3, g_4, g_1 \rangle & \langle g_2, g_3, g_4, g_1 \rangle \\
  19d & \langle g_a, g_2, g_3, g_1 \rangle & \langle g_2, g_3, g_1 \rangle \\
  19e & \langle g_a, g_2, g_1 \rangle & \langle g_2, g_1 \rangle \\
\end{array}

\[ g_1 \] 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. \[ G_{a3} \quad G_{e3} \quad \bar{G}_{a2}, G_{a1}, G_{d2}, G_{d1} \quad G_{a3}, G_{e3} \quad G_{d3} \quad G_{a4} \quad G_{d4}, G_{a4} \]

\[
\begin{pmatrix}
2 & 5 \\
14 & ?
\end{pmatrix}
\begin{pmatrix}
5 & 2 \\
? & 14
\end{pmatrix}
\begin{pmatrix}
15 & 0 \\
0 & 15
\end{pmatrix}
\begin{pmatrix}
7 & 14 \\
5 & 2
\end{pmatrix}
\begin{pmatrix}
2 & 5 \\
14 & 7
\end{pmatrix}
\begin{pmatrix}
7 & 14 \\
5 & 2
\end{pmatrix}
\begin{pmatrix}
10 & 14 \\
5 & 5
\end{pmatrix}
\begin{pmatrix}
5 & 5 \\
14 & 10
\end{pmatrix}
\]
### Dimension 20

| 1. | h | a | r₁ | r₂ | r₃ | r₄ | t | b₁ | b₂ | b₃ | i | Order | $g_{ab}h_{Re}^{-1}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $g_a$ | $-a$ | r₁ | r₂ | r₃ | r₄ | t | $b'_1$ | $b'_2$ | $b'_3$ | i | 2 | $g_a$ |
| $g_1$ | a | $-r_1$ | r₂ | r₃ | r₄ | t | $b''_1$ | $b''_2$ | $b''_3$ | i | 4 | $g_1^3$ |
| $g_2$ | a | r₁ | r₂ | r₃ | $-r_4$ | t' | $b'_1$ | $b'_2$ | $b'_3$ | i | 24 | $g_2^1$ |
| $g_3$ | a | r₁ | r₂ | r₃ | $-r_4$ | t'' | $b'_1$ | $b'_2$ | $b'_3$ | i | 2 | $g_3^1$ |
| $g_4$ | a | r₁ | r₂ | r₃ | r₄ | t | $b'_1$ | $b'_2$ | $b'_3$ | $-i$ | 2 | $g_e = g_4^1$ |

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

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

$$b'_1 = ((a - 17)(17 + r_1))^\frac{1}{2}$$

$$b'_2 = i((a + 17)(17 - r_1))^\frac{1}{2}$$

$$b'_3 = \Re(10e^{\frac{3i\pi}{2}}(19 + 19\sqrt{19}))$$

$$b'_4 = \left(i\left((-a + 18)r_1r_4 + (-7a + 21)r_3 - (2a + 15)r_2 + 3a)r_4 - 3(-a + 18)r_2 + 195\right)^\frac{1}{2}$$

$$b''_i = -\left(i\left((-a + 39)r_3r_4 + (7a + 21)r_3 + (2a + 15)r_2 - 3a)r_4 - 3(a + 18)r_2 + 195\right)^\frac{1}{2}$$

### Orbit

| 2. | Orbit | $\text{Gal}(E/Q)$ | $\text{Gal}(E/E_0)$ | $g_1$ interchanges orbits 20a, 20b. |
|---|---|---|---|---|
| 20ab | $\langle g_a, g_1, g_2, g_3, g_4, \bar{g}_1 \rangle$ | $\langle g_1, g_2, g_3, g_4, \bar{g}_1 \rangle$ | $\langle g_1, g_2, g_3, g_4, \bar{g}_1 \rangle$ |

### Table

| 3. | $G_{a1}$ | $G_{b1}$ | $G_{a2}, G_{b2}$ | $G_{a3}, G_{b3}$ | $G_{a4}, G_{b4}$ |
|---|---|---|---|---|---|
| | (1 24) | (15 24) | (1 32) | (10 31) | (1 20) |
| | (16 25) | (16 39) | (8 33) | (9 1) | (20 21) |
Dimension 21

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

$\theta' = \cos \frac{10a}{\pi}$

$\theta'' = \cos \frac{11a}{\pi}$

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

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

$g_1$ 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.
Dimension 24

1. 

| $h$ | $a$ | $r_1$ | $r_2$ | $r_3$ | $t$ | $b_1$ | $b_2$ | $b_3$ | $b_4$ | i | Order $g_ag_a^{-1}$ |
|-----|-----|------|------|------|----|------|------|------|------|---|-------------------|
| $g_a$ | $-a$ | $r_1$ | $r_2$ | $r_3$ | $t$ | $b_1'$ | $b_2$ | $b_3$ | $b_4'$ | i | 2 | $g_a$ |
| $g_1$ | $a$ | $r_1$ | $r_2$ | $-r_3$ | $t$ | $b_1$ | $b_2$ | $b_3$ | $b_4'$ | i | 4 | $g_3^2b_1$ |
| $g_2$ | $a$ | $r_1$ | $-r_2$ | $r_3$ | $t'$ | $b_1'$ | $b_2'$ | $b_3$ | $b_4'$ | i | 12 | $g_3^2g_4$ |
| $g_3$ | $a$ | $-r_1$ | $r_2$ | $r_3$ | $t''$ | $b_1'$ | $b_2'$ | $b_3$ | $b_4'$ | i | 4 | $g_3^2g_3$ |
| $g_4$ | $a$ | $r_1$ | $r_2$ | $r_3$ | $t$ | $-b_1$ | $b_2$ | $b_3$ | $b_4$ | i | 2 | $g_4$ |
| $g_1$ | $a$ | $r_1$ | $r_2$ | $r_3$ | $t$ | $b_1$ | $b_2$ | $b_3$ | $b_4$ | $-i$ | 2 | $g_c = g_3^2g_4g_1$ |

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

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

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

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

$b_3' = \sqrt{(4 - r_1)(3 + r_2)}$

$b_4' = 4Re(e^{2\pi i} (1 + i\sqrt{7})^i)$

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

$b_6' = i\sqrt{(a + 1)(-r_3 + 5)}$

2. 

| Orbit | $\text{Gal}(E/Q)$ | $\text{Gal}(E/E_0)$ |
|-------|------------------|-------------------|
| $24ab$ | $(g_a, g_1, g_2, g_3, g_4, g_1)$ | $(g_3, g_2, g_3, g_4, g_1)$ |
| $24c$ | $(g_a, g_2, g_3, g_4, g_1)$ | $(g_2, g_3, g_4, g_1)$ |

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

3. 

| $G_{e_1}$ | $G_{e_2}$ | $G_{e_3}$ | $G_{e_4} = G_{e_2}$ | $G_{e_5}$ | $G_{e_6} = G_{e_3}$ | $G_{e_7} = G_{e_4}$ | $G_{e_8}$ |
|-----------|-----------|-----------|-----------------|-----------|-----------------|-----------------|-----------|
| 9 23      | 3 5       | 11 46     | 2 37            | 17 36     | 5 12            | 5 24            | 0 25      |
| 32 39     | 8 45      | 2 9       | 11 39           | 12 5      | 36 17           | 24 29           | 23 25     |
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 | $g_1'$ |
| $g_2$ | $a$ | $-r_1$ | $r_2$ | $r_3$ | $t'$ | $b_1$ | $b_2$ | $b_3$ | $b_4$ | $i$ | 6 | $g_2$ |
| $g_3$ | $a$ | $r_1$ | $r_2$ | $r_3$ | $t$ | $b_1$ | $-b_2$ | $b_3$ | $b_4$ | $i$ | 6 | $g_3'$ |
| $g_4$ | $a$ | $r_1$ | $-r_2$ | $r_3$ | $t''$ | $b_1$ | $b_2$ | $b_3$ | $b_4$ | $i$ | 2 | $g_4'$ |
| $g_5$ | $a$ | $r_1$ | $r_2$ | $r_3$ | $t$ | $-b_1$ | $-b_2$ | $b_3$ | $b_4$ | $i$ | 2 | $g_5'$ |
| $\bar{g}_1$ | $a$ | $r_1$ | $r_2$ | $r_3$ | $t$ | $b_1$ | $b_2$ | $b_3$ | $b_4$ | $i$ | 2 | $\bar{g}_1'$ |

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

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

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

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

$b_3' = 2 \text{Re} \left( e^{i \pi/4} (189 + 21i\sqrt{87}) \right)$

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

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

2.  

| Orbit | $\text{Gal}(E/Q)$ | $\text{Gal}(E/E_0)$ |
|-------|-----------------|-----------------|
| $28ab$ | $\langle g_a, g_1, g_2, g_3, g_4, g_5, b_{arg_1} \rangle$ | $\langle g_1', g_2, g_3, g_4, g_5, g_1 \rangle$ |
| $28c$ | $\langle g_a, g_2, g_3, g_4, g_5, g_1 \rangle$ | $\langle g_2, g_3, g_4, g_5, g_1 \rangle$ |

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

3.  

| $G_{a_{1}}$ | $G_{a_{2}}$ | $G_{a_{3}} = G_{a_{2}}$ | $G_{a_{4}}$ | $G_{a_{5}} = G_{a_{4}}$ | $G_{a_{6}} = G_{a_{5}}$ | $G_{a_{7}} = G_{a_{6}}$ | $G_{a_{8}} = G_{a_{7}}$ |
|-----------|-----------|-----------------|-----------|-----------------|-----------------|-----------------|-----------------|
| (17 50)   | (6 11)    | (27 29)         | (13 30)   | (26 43)         | (37 7 1)        | (49 8)         | (14 42)        |
| (0 29)    | (27 29)   | (26 43)         | (37 7 1)   | (49 8)         | (14 42)        | (17 50)        | (0 29)         |
### Dimension 30

| h | a | r₁ | r₂ | t | b₁ | b₂ | b₃ | b₄ | b₅ | i | Order | gₐh⁻¹_a | t' = \cos \frac{2\pi}{3} |
|---|---|----|----|---|----|----|----|----|----|---|--------|-----------|------------------|
| gₐ | -a | r₁ | r₂ | t | b₁ | b₂ | b₃ | b₄ | b₅ | i | 2 | gₐ | \( b₁' = -\frac{1}{2} \sqrt{4(-5r₁r₂-(4a+23)r₁)t+2((4a+21)r₂+8a+111)} \) |
| g₁ | a | r₁ | r₂ | t | b₁ | b₂ | b₃ | b₄ | b₅ | i | 9 | g₁ | \( b₁'' = \frac{1}{2} \sqrt{4(5r₁r₂+(4a-23)r₁)t'+2((4a-21)r₂-8a+111)} \) |
| g₂ | a | r₁ | -r₂ | t' | b₁'' | b₂ | b₃ | b₄ | b₅ | i | 8 | g₂ | \( b₂' = 2 \text{Re} \left( e^{\frac{2\pi}{3}} (1+2i\sqrt{3}) \right) \) |
| g₃ | a | r₁ | r₂ | t | b₁ | b₂ | b₃ | b₄ | b₅ | i | 3 | g₃ | \( b₃' = 2 \text{Re} \left( e^{\frac{2\pi}{3}} (4+b₄'+i\sqrt{48-8b₄'-b₄''}) \right) \) |
| g₄ | a | -r₁ | r₂ | -t | b₁ | b₂ | b₃ | b₄ | b₅ | i | 2 | g₄g₅ | \( b₄' = 2 \text{Re} \left( e^{\frac{2\pi}{3}} (70+10i\sqrt{3}) \right) \) |
| g₅ | a | r₁ | r₂ | t | b₁ | b₂ | b₃ | b₄ | -b₅ | i | 2 | g₅ | \( b₅' = -\frac{1}{2} \sqrt{2a-18} \) |
| g₁ | a | r₁ | r₂ | t | b₁ | b₂ | b₃ | b₄ | b₅ | -i | 2 | g₄g₁ | |

### 2. Orbit 

| Orbit | \( \text{Gal}(E/Q) \) | \( \text{Gal}(E/E₀) \) |
|-------|-------------------------|-------------------------|
| 30abc | \{gₐ, g₁, g₂, g₃, g₄, g₅, g₆\} | \{g₁, g₂, g₃, g₄, g₅, g₆\} |
| 30d   | \{gₐ, g₁, g₂, g₃, g₄, g₅, g₆\} | \{g₁, g₂, g₃, g₄, g₅, g₆\} |

\( g₁ \) cycles orbits 30abc in the order 30a → 30b → 30c → 30a, and restricts to an order 3 automorphism on 30d.

### 3. 

| \( G_{a₁} \) | \( G_{a₂} \) | \( G_{b₁} \) | \( G_{b₂} \) | \( G_{a₁} = G_{b₁} \) | \( G_{a₂} = G_{b₂} \) |
|------------|------------|------------|------------|----------------|----------------|
| (15, 49)  | (9, 56)    | (21, 40)   | (13, 24)   | (1, 20)        | (36, 37)        |
| \( G_{a₁} = G_{b₂} \) | \( G_{a₁} = G_{b₁} \) | \( G_{a₂} = G_{b₁} \) | \( G_{a₂} = G_{b₂} \) |
| (11, 25)  | (35, 36)   | (5, 19)    | (1, 48)    | (1, 30)        | (1, 3)          |
| \( G_{a₁} = G_{b₂} \) | \( G_{a₁} = G_{b₁} \) | \( G_{a₂} = G_{b₁} \) | \( G_{a₂} = G_{b₂} \) |

g₁ cycles orbits 30abc in the order 30a → 30b → 30c → 30a, and restricts to an order 3 automorphism on 30d.
Dimension 35

| $h$ | $a$ | $r_1$ | $r_2$ | $r_3$ | $b_1$ | $b_2$ | $b_3$ | $b_4$ | $b_5$ | $b_6$ | 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 | $g_1$ |
| $g_2$ | $a$ | $-r_1$ | $r_2$ | $r_3$ | $b_1$ | $b_2$ | $b'_3$ | $b_4$ | $b_5$ | $b_6'$ | $i$ | 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 | $g_3$ |
| $g_4$ | $a$ | $r_1$ | $-r_2$ | $r_3$ | $b_1$ | $b_2$ | $-b_3$ | $b_4$ | $b_5$ | $b_6$ | $i$ | 2 | $g_3^3 g_4$ |
| $g_1$ | $a$ | $r_1$ | $r_2$ | $r_3$ | $b_1$ | $b_2$ | $b_3$ | $b_4$ | $b_5$ | $b_6$ | $-i$ | $2$ | $g_c = g_2^{12} g_3^{8} g_1$ |

$g_1$ cycles orbits $35bcdg$ in the order $35b \rightarrow 35c \rightarrow 35d \rightarrow 35g \rightarrow 35b$ and interchanges orbits $35af$; it satisfies the relations $g_1^2 = g_1^{12}$ on $35af$, $g_1 = g_2^6 g_4 g_1$ on $35e$; it restricts to the identity on $35h$, $35i$, $35j$. $g_2$ satisfies the relations $g_2^2 = e$ on $35i$ (where $e$ is the identity) and $g_2^6 = g_4 g_1$ on $35j$.
|   | $G_{a1}$ | $G_{a2}$ | $G_{a3}$ | $G_{a4}$ | $G_{a5}$ | $G_{a6}$ | $G_{a7}$ | $G_{a8}$ | $G_{a9}$ | $G_{a10}$ |
|---|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|
| 1 | $r_1$ | $r_2$ | $b_1$ | $b_2$ | $b_3$ | $b_4$ | $b_5$ | $b_6$ | $b_7$ | $\tau_3$ |
| $g_a$ | $-a$ | $r_1$ | $r_2$ | $b_1$ | $b_2$ | $b_3$ | $b_4$ | $b_5$ | $b_6$ | $b_7$ | $\tau_3$ | 2 |
| $g_1$ | $a$ | $-r_1$ | $r_2$ | $b_1$ | $b_2$ | $b_3$ | $b_4$ | $b_5$ | $b_6$ | $b_7$ | $\tau_3$ | 8 |
| $g_2$ | $a$ | $r_1$ | $r_2$ | $-b_1$ | $b_2$ | $b_3$ | $b_4$ | $b_5$ | $b_6$ | $b_7$ | $\tau_3$ | 2 |
| $g_3$ | $a$ | $r_1$ | $r_2$ | $b_1$ | $b_2$ | $b_3$ | $b_4$ | $b_5$ | $b_6$ | $b_7$ | $\tau_3$ | 4 |
| $g_4$ | $a$ | $r_1$ | $r_2$ | $b_1$ | $b_2$ | $b_3$ | $b_4$ | $b_5$ | $b_6$ | $b_7$ | $\tau_3$ | 3 |
| $g_5$ | $a$ | $r_1$ | $r_2$ | $b_1$ | $b_2$ | $b_3$ | $b_4$ | $b_5$ | $b_6$ | $b_7$ | $\tau_3$ | 3 |
| $g_6$ | $a$ | $r_1$ | $r_2$ | $b_1$ | $b_2$ | $b_3$ | $b_4$ | $b_5$ | $b_6$ | $-b_7$ | $\tau_3$ | 2 |
| $\bar{g}_1$ | $a$ | $r_1$ | $r_2$ | $b_1$ | $b_2$ | $b_3$ | $b_4$ | $b_5$ | $b_6$ | $-b_7$ | $-\tau_3$ | 2 |

Dimension 39

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

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

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

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

$$b_5' = \sqrt{-2b_3 - 5)(r_1 + 2)b_3 - (8a - 35)(10 + r_1)}$$

$$b_6' = \text{Re}(e^{\frac{\pi}{4}(676 + 1014i\sqrt{3})})$$

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

$$b_7' = \sqrt{6a + 3}$$
2. Orbit $\text{Gal}(E/Q)$ $\text{Gal}(E/E_0)$

| $39acde$ | $\langle g_a, g_3, g_2, g_4, g_5, g_6, g_1 \rangle$ | $\langle g_1^{2}, g_3, g_4, g_5, g_6, g_1 \rangle$ |
| $39bf$ | $\langle g_a, g_1, g_3, g_4, g_5, g_6, g_1 \rangle$ | $\langle g_1^{2}, g_3, g_4, g_5, g_6, g_1 \rangle$ |
| $39gh$ | $\langle g_a, g_1, g_2, g_3, g_4, g_5, g_6, g_1 \rangle$ | $\langle g_1^{2}, g_2, g_3, g_4, g_5, g_6, g_1 \rangle$ |
| $39ij$ | $\langle g_a, g_1, g_3, g_4, g_6, g_1 \rangle$ | $\langle g_1^{2}, g_3, g_4, g_6, g_1 \rangle$ |

$g_1$ interchanges the pairs $39ac$, $39cd$, $39bf$, $39gh$ 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.|
| $G_{a1}$ | $G_{b1}$ | $G_{a2}$ | $G_{b2}$ | $G_{a3}$ | $G_{b3}$ | $G_{a4}$ | $G_{b4}$ | $G_{a5}$ | $G_{b5}$ | $G_{a6}$ | $G_{b6}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $\begin{pmatrix} 12 & 14 \\ 25 & 26 \end{pmatrix}$ | $\begin{pmatrix} 0 & 25 \\ 14 & 25 \end{pmatrix}$ | $\begin{pmatrix} 10 & 32 \\ 3 & 29 \end{pmatrix}$ | $\begin{pmatrix} 13 & 27 \\ 1 & 26 \end{pmatrix}$ | $\begin{pmatrix} 3 & 7 \\ 32 & 10 \end{pmatrix}$ | $\begin{pmatrix} 6 & 10 \\ 26 & 29 \end{pmatrix}$ | $\begin{pmatrix} 16 & 33 \\ 29 & 13 \end{pmatrix}$ | $\begin{pmatrix} 2 & 3 \\ 38 & 38 \end{pmatrix}$ | $\begin{pmatrix} 0 & 7 \\ 28 & 6 \end{pmatrix}$ | $\begin{pmatrix} 4 & 21 \\ 4 & 21 \end{pmatrix}$ |
| $G_{a2}$ | $G_{b2}$ | $G_{a3}$ | $G_{b3}$ | $G_{a4}$ | $G_{b4}$ | $G_{a5}$ | $G_{b5}$ | $G_{a6}$ | $G_{b6}$ |
| $\begin{pmatrix} 19 & 23 \\ 16 & 3 \end{pmatrix}$ | $\begin{pmatrix} 3 & 16 \\ 23 & 19 \end{pmatrix}$ | $\begin{pmatrix} 1 & 12 \\ 13 & 38 \end{pmatrix}$ | $\begin{pmatrix} 7 & 7 \\ 15 & 26 \end{pmatrix}$ | $\begin{pmatrix} 20 & 7 \\ 15 & 13 \end{pmatrix}$ | $\begin{pmatrix} 21 & 25 \\ 14 & 7 \end{pmatrix}$ | $\begin{pmatrix} 7 & 14 \\ 25 & 21 \end{pmatrix}$ | $\begin{pmatrix} 11 & 18 \\ 33 & 32 \end{pmatrix}$ | $\begin{pmatrix} 9 & 28 \\ 34 & 33 \end{pmatrix}$ |
| $G_{a4}$ | $G_{b4}$ | $G_{a5}$ | $G_{b5}$ | $G_{a6}$ | $G_{b6}$ |
| $\begin{pmatrix} 4 & 9 \\ 30 & 13 \end{pmatrix}$ | $\begin{pmatrix} 13 & 30 \\ 9 & 4 \end{pmatrix}$ | $\begin{pmatrix} 22 & 0 \\ 0 & 22 \end{pmatrix}$ | $\begin{pmatrix} 0 & 2 \\ 8 & 24 \end{pmatrix}$ | $\begin{pmatrix} 12 & 14 \\ 25 & 26 \end{pmatrix}$ | $\begin{pmatrix} 25 & 27 \\ 12 & 13 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 \\ 38 & 1 \end{pmatrix}$ | $\begin{pmatrix} 2 & 3 \\ 12 & 38 \end{pmatrix}$ | $\begin{pmatrix} 0 & 7 \\ 28 & 6 \end{pmatrix}$ |
### Dimension 48

1. \[ h \ a \ r_1 \ r_2 \ r_3 \ t \ b_1 \ b_2 \ b_3 \ b_4 \ b_5 \ b_6 \ i \ \text{Order of } g_{a_{b'i'}} = \frac{12\pi}{7} \]
   \[ r' = \cos \frac{12\pi}{7}, \quad r'' = \cos \frac{12\pi}{47} \]

2. \[ g_{a_{b'i'}} = \sqrt{5 - (3a - 5)b_1^2 + 2(a + 5)r_3 + 210(3 + a)} \]
   \[ g_{b'i'} = \sqrt{5 - 1} \]

3. \[ \text{Cycle structure for } g_{a_{b'i'}}: \quad g_1 \text{ cycles } 48abcd \text{ in the order } 48a \to 48d \to 48b \to 48c \to 48a \text{ and restricts to the identity on } 48f, 48g. \]

\[ G_{a_{b'i'}} = G_{a_{b'i'}} = G_{a_{b'i'}} = G_{a_{b'i'}} = G_{a_{b'i'}} = G_{a_{b'i'}} = G_{a_{b'i'}} \]

\[ (17 \ 37) \quad (11 \ 31) \quad (25 \ 93) \quad (4 \ 47) \quad (15 \ 17) \quad (31 \ 33) \quad (95 \ 0) \]
ORCID iDs
Marcus Appleby
https://orcid.org/0000-0001-9225-4064
Steven Flammia
https://orcid.org/0000-0002-3975-0226

References

[1] Zauner G 1999 Quantendesigns. Grundzüge einer nichtkommutativen designtheorie PhD Thesis University of Vienna
Zauner G 2011 Quantum designs: foundations of a noncommutative design theory Int. J. Quantum Inf. 9 445–508 (published in english translation)
[2] Renes J M, Blume-Kohout R, Scott A J and Caves C M 2004 Symmetric informationally complete quantum measurements J. Math. Phys. 45 2171–80
[3] Fuchs C A and Sasaki M 2003 Squeezing quantum information through a classical channel: measuring the quantumness of a set of quantum states Quantum Inf. Comput. 3 377–404
[4] Řeháček J, Englert B-G and Kaszlikowski D 2004 Minimal qubit tomography Phys. Rev. A 70 052321
[5] Englert B-G, Kaszlikowski D, Ng H K, Chua W K, Řeháček J and Anders J 2004 Efficient and robust quantum key distribution with minimal state tomography (arXiv:quant-ph/0412075)
[6] Scott A J 2006 Tight informationally complete quantum measurements J. Phys. A: Math. Gen. 39 13507–30
[7] Durt T, Kurtzweiler C, Lamas-Linares A and Ling A 2008 Wigner tomography of two-qubit states and quantum cryptography Phys. Rev. A 78 042338
[8] Zhu H and Englert B-G 2011 Quantum state tomography with fully symmetric measurements and product measurements Phys. Rev. A 84 022327
[9] Zhu H 2016 Quasiprobability representations of quantum mechanics with minimal negativity Phys. Rev. Lett. 117 120404
[10] Fuchs C A and Schack R 2013 Quantum-bayesian coherence Rev. Mod. Phys. 85 1693–715
[11] Howard S D, Calderbank A R and Moran W 2006 The finite Heisenberg–Weyl groups in radar and communications EURASIP J. Appl. Signal Process. 2006 1–11
[12] Malikiosis R-D 2018 Spark deficient Gabor frames Pacific J. Math. 294 159–80
[13] Scott A J and Grassl M 2010 Symmetric informationally complete positive-operator-valued measures: a new computer study J. Math. Phys. 51 042203
[14] Scott A J 2017 SICs: extending the list of solutions (arXiv:1703.03993)
[15] Fuchs C A, Hoang M C and Stacey B C 2017 The SIC question: history and state of play Axioms 6 21
[16] Grassl M and Scott A J 2017 Fibonacci–Lucas SIC-POVMs J. Math. Phys. 58 122201
[17] Grassl M and Scott A J (unpublished)
[18] Appleby D M 2005 Symmetric informationally complete-positive operator valued measures and the extended Clifford group J. Math. Phys. 46 052107
[19] Appleby D M, Bengtsson I, Brierley S, Grassl M, Gross D and Larsson J-Å 2012 The monomial representations of the Clifford group Quantum Inf. Comput. 12 404–31
[20] Appleby D M, Bengtsson I, Brierley S, Ericsson A, Grassl M and Larsson J-Å 2014 Systems of imprimitivity for the Clifford group Quantum Inf. Comput. 14 339–60
[21] Hoggar S G 1998 64 lines from a quaternionic polytope Geometriae Dedicata 69 287–9
[22] Zhu H 2015 Super-symmetric informationally complete measurements Ann. Phys., NY 362 311–26
[23] Stacey B C 2017 Sporadic SICs and the normed division algebras Found. Phys. 47 1060–4
[24] Marcus D A 1977 Number Fields (New York: Springer)
[25] Cohn H 1978 A Classical Invitation to Algebraic Numbers and Class Fields (with two appendices by Olga Taussky) (New York: Springer)
[26] Appleby D M, Yadsan-Appleby H and Zauner G 2013 Galois automorphisms of a symmetric measurement Quantum Inf. Comput. 13 672–720
[27] Appleby M, Flammia S, McConnell G and Yard J 2016 Generating ray class fields of real quadratic fields via complex equiangular lines (arXiv:1604.06098)
[28] Appleby M, Flammia S, McConnell G and Yard J 2017 SICs and algebraic number theory Found. Phys. 47 1042–59

39
[29] Appleby M, Bengtsson I, Dumitru I and Flammia S 2017 Dimension towers of SICs. I. Aligned SICs and embedded tight frames J. Math. Phys. 58 112201
[30] Bailey D H, Borwein J M, Calkin N J, Girgensohn R, Luke D R and Moll V H 2007 Experimental Mathematics in Action (Wellesley, MA: A K Peters)
[31] Ferguson H, Bailey D and Arno S 1999 Analysis of PSLQ, an integer relation finding algorithm Math. Comput. 68 351–69
[32] Exact SIC fiducial vectors www.physics.usyd.edu.au/~sflammia/SIC
[33] Knill E 1996 Group representations, error bases and quantum codes (arXiv:quant-ph/9608049)
[34] Klappenecker A A and Rötteler M 2002 Beyond stabilizer codes. I. Nice error bases IEEE Trans. Inf. Theory 48 2392–5
[35] Appleby D M 2009 Properties of the extended Clifford group with applications to SIC-POVMs and MUBs (arXiv:0909.5233)
[36] Appleby D M, Bengtsson I and Dang H B 2015 Galois unitaries, mutually unbiased bases, and MUB-balanced states Quantum Inf. Comput. 15 1261–94
[37] Ireland K and Rosen M 1990 A Classical Introduction to Modern Number Theory (Graduate Texts in Mathematics vol 84) 2nd edn (New York: Springer)