

PAPER

SICs and the elements of order three in the Clifford group

To cite this article: Len Bos and Shayne Waldron 2019 *J. Phys. A: Math. Theor.* **52** 105301

View the [article online](#) for updates and enhancements.



IOP | ebooks™

Bringing you innovative digital publishing with leading voices to create your essential collection of books in STEM research.

Start exploring the collection - download the first chapter of every title for free.

SICs and the elements of order three in the Clifford group

Len Bos¹ and Shayne Waldron^{2,3} 

¹ Department of Computer Science, University of Verona, Verona, Italy

² Department of Mathematics, University of Auckland, Private Bag 92019, Auckland, New Zealand

E-mail: waldron@math.auckland.ac.nz

Received 21 September 2018, revised 23 December 2018

Accepted for publication 18 January 2019

Published 8 February 2019



CrossMark

Abstract

For over a decade, there has been intensive work on the numerical and analytic construction of SICs (d^2 equiangular lines in \mathbb{C}^d) as an orbit of the Heisenberg group. The Clifford group, which consists of the unitary matrices which normalise the Heisenberg group, plays a key role in these constructions. All of the known fiducial (generating) vectors for such SICs are eigenvectors of symplectic operations in the Clifford group with canonical order 3. Here we describe the Clifford group and the subgroup of symplectic operations in terms of a natural set of generators. From this, we classify all its elements of canonical order three. In particular, we show (contrary to prior claims) that there are symplectic operations of canonical order 3 for $d \equiv 6 \pmod{9}$, which are not conjugate to the Zauner matrix. It is as yet unknown whether these give rise to SICs.

Keywords: SIC (symmetric informationally complete positive valued operator measure), Clifford group, symplectic operation, quadratic Gauss sum, Heisenberg group

1. Introduction

A set of d^2 unit vectors in \mathbb{C}^d (or the lines they determine) is said to be equiangular if

$$|\langle v_j, v_k \rangle|^2 = \frac{1}{d+1}, \quad j \neq k.$$

In the quantum information theory community, the corresponding rank one orthogonal projections $P_j = v_j v_j^*$ are said to be a symmetric informationally complete positive operator valued measure (SIC or SIC-POVM for short). The existence of a SIC for every dimension d is known as *Zauner's conjecture* or the *SIC problem* [FHS17].

³ Author to whom any correspondence should be addressed.

Since Zauner's thesis in 1999 (see [Zau10]), there has been constant progress on the SIC problem. With one exception (the Hoggar lines in \mathbb{C}^8), all the known SICs appear as the orbit of a single (fiducial) vector/projection under the action of the Heisenberg group (this is sometimes referred to as a strong form of Zauner's conjecture). The search for such a fiducial vector dramatically reduces the number of unknown variables from the order of d^3 to d , and has led to high accuracy numerical SICs [RBKSC04, SG10, Sco17], which in turn has led to analytic SICs [ACFW18] i.e. a proof Zauner's conjecture for various dimensions d .

A key feature of these SIC fiducials is that they are mapped to each other by elements of the Clifford group, i.e. the normaliser of the Heisenberg group in the unitary matrices (see especially Appleby [App05]), and there is a fiducial (on a given Clifford group orbit) which is an eigenvector of a 'symplectic' operation in the Clifford group with canonical order 3. This further reduces the number of unknowns in a SIC fiducial to the order of $\frac{d}{3}$. Here, we consider the structure of the Clifford group, and in particular, its elements of order 3. The main points are:

- We determine the diagonal elements of the Clifford group, and thereby show that it is generated by the Fourier matrix F and a diagonal matrix R (together with generators of the Heisenberg group).
- The generator R above can be replaced by the Zauner matrix Z (of order 3).
- We show that the subgroup of symplectic operations is generated by F and R .
- We give an alternative to the Appleby indexing of the elements of the Clifford group, which is 1–1, in all cases.
- We use our indexing to determine the Clifford operations of order 3, and in particular, those with Clifford trace -1 (canonical order 3). This includes a family for $d \equiv 6 \pmod{9}$, which was previously overlooked.
- We show that for d even there are nontrivial symplectic operations which are not displacement free, i.e. belong to the Heisenberg group.
- We show explicitly how to write the permutation matrices as words in F and R .

The techniques involved include the calculation of certain quadratic Gauss sums, and the analysis of certain binary quadratic forms over \mathbb{Z}_d . Along the way we prove conjecture 4 of [Fla06].

2. The Heisenberg group and Weyl–Heisenberg SICs

Throughout, let ω and μ be the primitive d th and $2d$ th roots of unity

$$\omega := e^{\frac{2\pi i}{d}}, \quad \mu := e^{\frac{2\pi i}{2d}},$$

and take the indices for elements of \mathbb{C}^d and $\mathbb{C}^{d \times d}$ from $\mathbb{Z}_d = \{0, 1, \dots, d-1\}$. Let $S \in \mathbb{C}^{d \times d}$ be the cyclic shift matrix, and $\Omega \in \mathbb{C}^{d \times d}$ be the modulation matrix given by

$$(S)_{jk} := \delta_{j,k+1}, \quad (\Omega)_{jk} := \omega^j \delta_{j,k}. \quad (2.1)$$

The notation $X = S$ and $Z = \Omega$ is commonly used in quantum information theory. These matrices have order d , and satisfy the commutativity relation

$$\Omega^k S^j = \omega^{jk} S^j \Omega^k. \quad (2.2)$$

Thus the group generated by the unitary matrices S and Ω is

$$H := \langle S, \Omega \rangle = \{\omega^r S^j \Omega^k : r, j, k \in \mathbb{Z}_d\}. \quad (2.3)$$

This is called the Heisenberg group⁴ (for \mathbb{Z}_d), as is the group

$$\hat{H} := \{ch : c \in \mathbb{T}, h \in H\} \subset \mathcal{U}(\mathbb{C}^d), \quad \mathbb{T} := \{c \in \mathbb{C} : |c| = 1\}. \quad (2.4)$$

The map $(j, k) \mapsto S^j \Omega^k$ is a faithful irreducible projective representation of $\mathbb{Z}_d \times \mathbb{Z}_d$. In particular, the unitary action of H on \mathbb{C}^d is irreducible, and so $(hv)_{h \in H}$ and $(S^j \Omega^k v)_{j, k \in \mathbb{Z}_d}$ are tight frames for \mathbb{C}^d for any $v \neq 0$ (see [VW05]), i.e.

$$f = \frac{1}{d} \sum_{(j, k) \in \mathbb{Z}_d^2} \langle f, S^j \Omega^k v \rangle S^j \Omega^k v, \quad \forall f \in \mathbb{C}^d.$$

Every SIC is a tight frame. A SIC (equiangular tight frame of d^2 vectors for \mathbb{C}^d) is said to be a Weyl–Heisenberg SIC for \mathbb{C}^d if (up to projective unitary equivalence) it has the form

$$\Phi_v := (S^j \Omega^k v)_{j, k \in \mathbb{Z}_d},$$

where the unit vector $v \in \mathbb{C}^d$ (or the projection $\Pi = vv^*$) is called a fiducial.

A Weyl–Heisenberg SIC for \mathbb{C}^d is generated from a single fiducial vector v by applying S (translation) and Ω (frequency shift). Thus, it is a discrete analogue of a Gabor system (Weyl–Heisenberg frame) with good time–frequency localisation. In this analogy the fiducial vector v corresponds to the *mother wavelet*. From now on, we consider only Weyl–Heisenberg SICs (which we refer to as SICs).

3. The Clifford group

Let $[U] := \{cU : c \in \mathbb{T}\} = \{e^{it}U : t \in \mathbb{R}\}$, so that $[U]$ is the unitary scalar matrices. The normaliser of the Heisenberg group \hat{H} in the group of unitary matrices is called the Clifford group, and it is denoted by $C(d)$. The projective Clifford group is $PC(d) := C(d)/[U]$ (its elements are called Clifford operations).

There is a natural action of $C(d)$ on the SIC fiducial vectors v , and of $PC(d)$ on SIC fiducial projectors $\Pi = vv^*$ given by

$$a \cdot v := av, \quad [a] \cdot \Pi := (av)(av)^* = a\Pi a^{-1}.$$

This maps SICs to SICs, since if $[a] \in PC(d)$ and v is a SIC fiducial vector, then

$$|\langle S^{j_1} \Omega^{k_1} av, S^{j_2} \Omega^{k_2} av \rangle|^2 = |\langle a^{-1} S^{j_1 - j_2} \Omega^{k_1 - k_2} av, v \rangle|^2 = \frac{1}{d+1}, \quad (j_1, k_1) \neq (j_2, k_2),$$

because $a^{-1} S^j \Omega^k a$, $(j, k) \neq (0, 0)$, is a nonscalar element of \hat{H} .

Since $H \subset C(d)$, the action of $C(d)$ on \mathbb{C}^d is irreducible, and its centre is $[I]$. Since

$$S^* = S^T = S^{-1}, \quad \Omega^* = \Omega^{-1}, \quad \Omega^T = \Omega, \quad (3.5)$$

the Heisenberg group and the Clifford group are closed under taking the transpose and Hermitian transpose, and hence also entrywise conjugation $\bar{A} = (A^*)^T$. Therefore entrywise conjugation maps a given Heisenberg SIC fiducial to another. The group generated by entrywise conjugation and $C(d)$ is the extended Clifford group $EC(d)$, and the extended projective Clifford group is $PEC(d) := EC(d)/[I]$ (the nonunitary elements of these groups are called the antiunitaries). These map SICs to SICs. The counting of (Weyl–Heisenberg) SICs is usually done up to projective unitary equivalence and the extended Clifford orbit it lies on (see [Wal18]). In addition to (entrywise) complex conjugation, certain Galois automorphisms of

⁴It is also known as the generalised Pauli or Weyl–Heisenberg group.

the SIC field (the field generated by μ and entries of a fiducial projector Π) have been shown to map SICs to SICs. Counting SICs up to the orbit under the extension of the Clifford group by these (pointwise) automorphisms gives a so called multiplet (union of extended Clifford orbits) [ACFW18].

Elements of the Clifford group include the Fourier matrix F , the diagonal matrix R , and the permutation matrices P_σ , $\sigma \in \mathbb{Z}_d^*$ (the units modulo d), which are given by

$$(F)_{jk} := \frac{1}{\sqrt{d}}\omega^{jk}, \tag{3.6}$$

$$(R)_{jk} := \mu^{j(j+d)}\delta_{jk}, \tag{3.7}$$

$$(P_\sigma)_{jk} := \delta_{j,\sigma k}, \quad \sigma \in \mathbb{Z}_d^*. \tag{3.8}$$

We observe that R is well defined, i.e. the value of $j(j+d)$ depends only on the integer $j \bmod d$. The entry $\mu^{j(j+d)}$ has many alternative descriptions, e.g.

$$\mu^{j(j+d)} = \mu^{j^2}(-1)^j = \mu^{j^2}(-1)^{j^2} = (-\mu)^{j^2} = \mu^{(d+1)j^2}.$$

Indeed, elementary computations (see [Wal18]) give:

Lemma 3.1. *The unitary matrices F, R, P_σ belong to the Clifford group. Indeed*

$$F(S^j\Omega^k)F^{-1} = \omega^{-jk}S^{-k}\Omega^j, \tag{3.9}$$

$$R(S^j\Omega^k)R^{-1} = \mu^{j(j+d)}S^j\Omega^{j+k}, \tag{3.10}$$

$$P_\sigma(S^j\Omega^k)P_\sigma^{-1} = S^{\sigma j}\Omega^{\sigma^{-1}k}, \tag{3.11}$$

where σ^{-1} is the multiplicative inverse of $\sigma \in \mathbb{Z}_d^*$.

The appearance of R can be explained (it was first observed by [BW07] for d odd). It appears in the following direct search for diagonal matrices in the normaliser of \hat{H} .

Proposition 3.1. *The subgroup of diagonal unitary matrices in $C(d)$ is generated by the unitary scalar matrices, Ω , and the matrix R .*

Proof. Suppose that $\Lambda = \text{diag}(\lambda_j)$ normalises \hat{H} , and $\lambda_d := \lambda_0$. Then

$$\Lambda S \Lambda^{-1} = \begin{pmatrix} 0 & 0 & \dots & \frac{\lambda_d}{\lambda_{d-1}} \\ \frac{\lambda_1}{\lambda_0} & 0 & \dots & 0 \\ 0 & \frac{\lambda_2}{\lambda_1} & \dots & 0 \\ \vdots & & & \vdots \end{pmatrix} = c S \Omega^k, \quad \text{i.e.} \quad \frac{\lambda_{j+1}}{\lambda_j} = c \omega^{jk}, \quad \forall j,$$

where $c \in \mathbb{C}$, $k \in \mathbb{Z}$. Solving this recurrence gives

$$\lambda_j = \lambda_0 c^j \omega^{\frac{1}{2}j(j-1)k} = \lambda_0 c^j \mu^{j(j-1)k} = \lambda_0 \mu^{j(j+d)k} (c\mu^{-k(d+1)})^j.$$

Since $\lambda_d = \lambda_0$, this gives

$$(c\mu^{-k(d+1)})^d = (c\mu^{-k(d+1)})^0 = 1 \implies c\mu^{-k(d+1)} = \omega^m,$$

and so $\Lambda = \lambda_0 R^k \Omega^m$. □

We will see (theorem 4.1) that R along with F and H generate the Clifford group. To this end, we now consider the structure of $C(d)$, by using a variation of the arguments of [App05]. Let

$$U_{(j,k)} := S^j \Omega^k, \quad (j, k) \in \mathbb{Z}_d^2. \quad (3.12)$$

If $a \in C(d)$, then

$$aU_\lambda a^{-1} = z_a(\lambda)U_{\psi_a(\lambda)}, \quad \forall \lambda \in \mathbb{Z}_d^2, \quad (3.13)$$

which defines functions $\psi_a : \mathbb{Z}_d^2 \rightarrow \mathbb{Z}_d^2$ and $z_a : \mathbb{Z}_d^2 \rightarrow \mathbb{T}$, since no U_λ is a scalar multiple of another. For example, (3.9) and (3.10) give

$$\psi_F \begin{pmatrix} j \\ k \end{pmatrix} = \begin{pmatrix} -k \\ j \end{pmatrix}, \quad z_F \begin{pmatrix} j \\ k \end{pmatrix} = \omega^{-jk}, \quad \psi_R \begin{pmatrix} j \\ k \end{pmatrix} = \begin{pmatrix} j \\ j+k \end{pmatrix}, \quad z_R \begin{pmatrix} j \\ k \end{pmatrix} = \mu^{j(j+d)}.$$

We now show the elements of the Clifford group factored by \hat{H} can be indexed by the elements of $SL_2(\mathbb{Z}_d)$. For a 2×2 matrix A , we define a symmetric matrix σ_A by

$$\sigma_A := \begin{pmatrix} \alpha\gamma & \beta\gamma \\ \beta\gamma & \beta\delta \end{pmatrix}, \quad A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}. \quad (3.14)$$

The map $A \mapsto \sigma_A$ is not 1-1, e.g. $\sigma_A = 0$ for all diagonal matrices.

Lemma 3.2. *Let ψ_a and z_a be given by (3.13). Then the map*

$$\psi : C(d) \rightarrow SL_2(\mathbb{Z}_d) : a \mapsto \psi_a \quad (3.15)$$

is a group homomorphism with kernel \hat{H} , and z_a satisfies

$$z_a(p+q) = \omega^{p^T \sigma_A q} z_a(p) z_a(q), \quad p, q \in \mathbb{Z}_d^2 \quad (3.16)$$

where $A = \psi_a$ and σ_A is given by (3.14).

Proof. By (2.2), we have $U_p U_q = \omega^{p_2 q_1} U_{p+q}$ and so

$$\omega^{p_2 q_1} (aU_{p+q} a^{-1}) = aU_p U_q a^{-1} = (aU_p a^{-1})(aU_q a^{-1}),$$

which gives

$$\begin{aligned} \omega^{p_2 q_1} z_a(p+q) U_{\psi_a(p+q)} &= z_a(p) U_{\psi_a(p)} z_a(q) U_{\psi_a(q)} \\ &= z_a(p) z_a(q) \omega^{\psi_a(p)_2 \psi_a(q)_1} U_{\psi_a(p) + \psi_a(q)} \end{aligned}$$

and hence

$$\psi_a(p+q) = \psi_a(p) + \psi_a(q), \quad (3.17)$$

$$\omega^{p_2 q_1} z_a(p+q) = z_a(p) z_a(q) \omega^{\psi_a(p)_2 \psi_a(q)_1}. \quad (3.18)$$

For $p = p_1 e_1 + p_2 e_2 \in \mathbb{Z}_d^2$, from (3.17) we obtain

$$\psi_a(p) = p_1 \psi_a(e_1) + p_2 \psi_a(e_2) = [\psi_a(e_1), \psi_a(e_2)] p,$$

i.e. ψ_a can be represented by the 2×2 matrix $[\psi_a(e_1), \psi_a(e_2)]$.

Let $[p', q'] = [\psi_a(p), \psi_a(q)] = \psi[p, q]$, so that $\det([p', q']) = \det(\psi_a) \det([p, q])$. Since the quotient $z_a(p)z_a(q)/z_a(p+q)$ is symmetric in p and q , (3.18) gives

$$\begin{aligned} \omega^{p_2q_1 - p_2'q_1'} = \omega^{q_2p_1 - q_2'p_1'} &\implies p_1'q_2' - q_1'p_2' = p_1q_2 - q_1p_2 \\ &\implies \det([p', q']) = \det([p, q]), \\ &\implies \det(\psi_a) = 1, \end{aligned} \quad (3.19)$$

i.e. $\psi_a \in SL_2(\mathbb{Z}_d)$. Using this, (3.18) can be written as (3.16).

Since $(ab)U_\lambda(ab)^{-1} = a(bU_\lambda b^{-1})a^{-1}$, we have

$$z_a(\lambda)U_{\psi_{ab}(\lambda)} = a(z_b(\lambda)U_{\psi_b(\lambda)})a^{-1} = z_b(\lambda)z_a(\psi_b(\lambda))U_{\psi_a(\psi_b(\lambda))}, \quad (3.20)$$

so that $\psi_{ab}(\lambda) = \psi_a(\psi_b(\lambda))$, i.e. $a \mapsto \psi_a$ is a homomorphism.

We now find the kernel of ψ . By (2.2), $\hat{H} \subset \ker \psi$. Suppose $\psi_a = I$, so that $aSa^{-1} = z_a(1, 0)S$ and $a\Omega a^{-1} = z_a(0, 1)\Omega$. Since $S^d = \Omega^d = I$, this implies that $z_a(1, 0)$ and $z_a(0, 1)$ are d th roots of unity, say

$$aSa^{-1} = \omega^\alpha S, \quad a\Omega a^{-1} = \omega^\beta \Omega. \quad (3.21)$$

If $a \in \hat{H}$, then (3.21) implies that a is a scalar multiple of $S^{-\beta}\Omega^\alpha$. Hence, we consider the unitary matrix $b = (S^{-\beta}\Omega^\alpha)^{-1}a$. By (3.21) and repeated application of (2.2), we have that

$$\begin{aligned} b(S^j\Omega^k)b^{-1} &= \Omega^{-\alpha}S^\beta(aSa^{-1})^j(a\Omega a^{-1})^kS^{-\beta}\Omega^\alpha \\ &= \Omega^{-\alpha}S^\beta(\omega^\alpha S)^j(\omega^\beta \Omega)^kS^{-\beta}\Omega^\alpha = S^j\Omega^k. \end{aligned}$$

Since b commutes with the basis $(S^j\Omega^k)_{j,k \in \mathbb{Z}_d}$ for $\mathbb{C}^{d \times d}$, Schur's lemma implies that b must be a (unit) scalar matrix cI , and hence $a = cS^{-\beta}\Omega^\alpha \in \hat{H}$. \square

The order of $SL_2(\mathbb{Z}_d)$ is known to be (see [Gun62] theorem 3, chapter I)

$$|SL_2(\mathbb{Z}_d)| = d^3 \prod_{p|d} \left(1 - \frac{1}{p^2}\right), \quad (p \text{ the prime factors of } d).$$

Hence, by lemma 3.2, the number of Clifford operations is

$$|\text{PC}(d)| = \left| \frac{\mathbf{C}(d)}{[I]} \right| = \left| \frac{\hat{H}}{[I]} \right| \left| \frac{\mathbf{C}(d)}{\hat{H}} \right| = d^2 |SL_2(\mathbb{Z}_d)| = d^5 \prod_{p|d} \left(1 - \frac{1}{p^2}\right).$$

Example 3.1. From lemma 3.1, we have the following $\psi_a \in SL_2(\mathbb{Z}_d)$,

$$\psi_F = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \psi_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \psi_{P_\sigma} = \begin{pmatrix} \sigma^{-1} & 0 \\ 0 & \sigma \end{pmatrix}. \quad (3.22)$$

Example 3.2. If $h = cS^a\Omega^b \in \hat{H}$, then $\psi_h = I$ and $z_h(j, k) = \omega^{bj-ak}$ (a character), since (2.2) gives

$$hU_{(j,k)}h^{-1} = S^a\Omega^b S^j\Omega^k\Omega^{-b}S^{-a} = S^a(\omega^{bj}S^j\Omega^b)\Omega^{k-b}S^{-a} = \omega^{bj-ak}S^j\Omega^k = \omega^{jb-ak}U_{(j,k)}.$$

A function z_a satisfying (3.16) is called a second degree character of \mathbb{Z}_n^2 associated to the bicharacter

$$B : \mathbb{Z}_n^2 \times \mathbb{Z}_n^2 \rightarrow \mathbb{T}, \quad B(p, q) := \omega^{p^T \sigma_A q},$$

given by σ_A (see [Rei89]). A continuous map $B : G \times G \rightarrow \mathbb{T}$ is a bicharacter of a locally compact abelian group G if for any fixed choice of one argument the resulting function $G \rightarrow \mathbb{T}$ is a character. All the second degree characters associated to a given bicharacter can be obtained from one by multiplying it by the characters.

Using a variation of the above argument, in FHK⁺08 it is shown that if

$$\hat{H} \rightarrow \hat{H} : cU_\lambda \mapsto cz(\lambda)U_{A\lambda}, \quad c \in \mathbb{T}, \quad z : \mathbb{Z}_d \rightarrow \mathbb{T}, \quad A \in GL_2(\mathbb{Z}_d), \tag{3.23}$$

is an automorphism of \hat{H} , then $A \in SL_2(\mathbb{Z}_d)$ and z is a second degree character (given by σ_A). For $a \in C(d)$, the map $cU_\lambda \mapsto a(cU_\lambda)a^{-1} = cz_a(\lambda)U_{A\lambda}$, $A = \psi_a$, is an automorphism of \hat{H} . The elements of $C(d)$ are termed metaplectic operations, and they are said to ‘intertwine the automorphisms of \hat{H} ’.

4. Generators for the Clifford group

It turns out that the matrices ψ_F and ψ_R of (3.22) generate $SL_2(\mathbb{Z}_d)$, and hence we obtain the following generators for the Clifford group.

Theorem 4.1 (Generators for the Clifford group). *The homomorphism*

$$\psi : C(d) \rightarrow SL_2(\mathbb{Z}_d) : a \mapsto \psi_a$$

maps F and R to generators for $SL_2(\mathbb{Z}_d)$, and hence is onto. Therefore $C(d)$ is generated by the unitary scalar matrices, and S, Ω, F, R .

Proof. By lemma 3.2, the kernel of $a \mapsto \psi_a$ is \hat{H} . Since \hat{H} is generated by the unitary scalar matrices and S, Ω , it suffices to show that $SL_2(\mathbb{Z}_d)$ is generated by

$$\psi_F = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \psi_R = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}. \tag{4.24}$$

It is well known that these matrices generate $SL_2(\mathbb{Z})$. Since the map of taking the entries of $A \in SL_2(\mathbb{Z})$ modulo d is a homomorphism onto $SL_2(\mathbb{Z}_d)$, they generate $SL_2(\mathbb{Z}_d)$. \square

This result appears in [Far14], where the generator F is referred to as the *QFT (discrete quantum Fourier transform) gate*, and R as the *phase-shift gate*. There it is proved using the Pauli–Euclid–Gottesman lemma, which says that there is a Clifford operation conjugating $S^j \Omega^k$ to $\Omega^{\gcd(j,k)}$.

We call the subgroup of the Clifford group $C(d)$ generated by F, R (and the scalars) the symplectic unitaries

$$C_{Sp}(d) := \langle F, R, [I] \rangle,$$

and the elements of $C_{Sp}(d)/[I]$ the symplectic operations. We will show that this is equivalent to the definition of [AYAZ13] that an element of the Clifford group is a symplectic unitary if it has an Appleby index of the form $[A, 0]$. Elements of the Heisenberg group \hat{H} (or $\hat{H}/[I]$) are referred to as Heisenberg operations, (Weyl) displacements or time–frequency shifts. It follows from theorem 4.1, that

Every Clifford operation is the product of a symplectic operation and a displacement.

For d even, an elementary calculation gives

$$\Omega^{\frac{d}{2}} = R^d, \quad S^{\frac{d}{2}} = F^{-1}\Omega^{\frac{d}{2}}F = F^{-1}R^dF, \quad S^{\frac{d}{2}}\Omega^{\frac{d}{2}} = F^{-1}R^dFR^d. \quad (4.25)$$

Thus there are nontrivial symplectic operations which are also displacements⁵. It turns out that (4.25) are the only ones (see corollary 7.1). This makes the description of the Clifford group more technical for d even (here R has order $2d$).

5. Indexing the Clifford operations

We now show that each Clifford operation is uniquely determined by the pair (ψ_a, z_a) . Define a semidirect product $SL_2(\mathbb{Z}_d) \ltimes \mathbb{T}^{\mathbb{Z}_d^2}$ via the multiplication

$$(A, z_A)(B, z_B) := (AB, (z_A \circ B)z_B), \quad (5.26)$$

where functions $\mathbb{Z}_d^2 \rightarrow \mathbb{T}$ are multiplied pointwise.

Corollary 5.1. *With the multiplication (5.26), the map*

$$\mathbb{C}(d) \rightarrow SL_2(\mathbb{Z}_d) \ltimes \mathbb{T}^{\mathbb{Z}_d^2} : a \mapsto (\psi_a, z_a) \quad (5.27)$$

is a homomorphism with kernel $[I]$. Thus every Clifford operation $[a] \in \mathbb{C}(d)/[I]$ has a unique index (ψ_a, z_a) , and these satisfy

$$\psi_{ab} = \psi_a\psi_b, \quad z_{ab} = (z_a \circ \psi_b)z_b, \quad (5.28)$$

$$\psi_{a^*} = \psi_{a^{-1}} = \psi_a^{-1}, \quad z_{a^*} = z_{a^{-1}} = \overline{z_a} \circ \psi_{a^*}, \quad (5.29)$$

$$\psi_{\overline{a}} = J\psi_aJ, \quad z_{\overline{a}} = \overline{z_a} \circ J, \quad J := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (5.30)$$

Further, if $\psi_a = \psi_b$, then z_a/z_b is a character.

Proof. It is easy to check $SL_2(\mathbb{Z}_d) \ltimes \mathbb{T}^{\mathbb{Z}_d^2}$ is a group with the multiplication (5.26), identity $(I, 1)$, and inverse $(A, z_A)^{-1} = (A^{-1}, \overline{z_A^{-1}} \circ A^{-1})$. By (3.20), we have

$$\psi_{ab} = \psi_a\psi_b, \quad z_{ab} = (z_a \circ \psi_b)z_b,$$

i.e. the map $a \mapsto (\psi_a, z_a)$ is a homomorphism. Thus (5.28) holds, as does (5.29) by the calculation $(\psi_{a^{-1}}, z_{a^{-1}}) = (\psi_a, z_a)^{-1} = (\psi_a^{-1}, \overline{z_a^{-1}} \circ \psi_a^{-1})$. and (5.30), since $\overline{U_\lambda} = U_{J\lambda}$ gives

$$\overline{a}U_\lambda\overline{a}^{-1} = \overline{aU_{J\lambda}a^{-1}} = \overline{z_a(\lambda)U_{AJ\lambda}} = \overline{z_a}(\lambda)U_{JAJ\lambda}.$$

Now suppose that a is in the kernel, i.e. $\psi_a = I$, $z_a = 1$. By lemma 3.2, we have $a = cS^j\Omega^k \in \hat{H}$. Using (2.2), we therefore obtain (see example 3.2)

$$aS^{p_1}\Omega^{p_2}a^{-1} = S^j\Omega^kS^{p_1}\Omega^{p_2}\Omega^{-k}S^{-j} = \omega^{kp_1-jp_2}S^{p_1}\Omega^{p_2},$$

so that $z_a(p) = \omega^{kp_1-jp_2} = 1, \forall p \in \mathbb{Z}_d^2$. Thus $j = k = 0$ and $a = cI \in [I]$, as supposed.

For $\psi_a = \psi_b = A$, it follows from (3.16) or (3.18) that z_a/z_b is a character. □

⁵Subgroups of the symplectic unitaries are sometimes said to be *displacement free*.

Example 5.1. For $a = RF$, from (3.22) and lemma 3.1, we calculate

$$\psi_{RF} = \psi_R \psi_F = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},$$

$$z_{RF} = (z_R \circ \psi_F) z_F \implies z_{RF}(j, k) = \mu^{(-k)(-k+d)} \omega^{-jk} = \mu^{k(k+d)+2jk}.$$

We call the subgroup of $SL_2(\mathbb{Z}_d) \times \mathbb{T}^{\mathbb{Z}_d^2}$ given by

$$\text{Ind}(d) := \{(\psi_a, z_a) : a \in \mathbf{C}(d)\}$$

the index group of the Clifford operations, and the index map is the isomorphism

$$\mathbf{C}(d)/[I] \rightarrow \text{Ind}(d) : [a] \mapsto (\psi_a, z_a). \tag{5.31}$$

In view of the multiplication

$$z_{ah} = (z_a \circ \psi_h) z_h = z_a z_h, \quad h \in \hat{H}.$$

Example 3.2 (that all characters of \mathbb{Z}_d^2 have the form $z_h, h \in \hat{H}$), and the fact that $a \mapsto \psi_a$ is onto $SL_2(\mathbb{Z}_d)$ (theorem 4.1), the elements of $\text{Ind}(d)$ consist of all pairs (A, z) , where $A \in SL_2(\mathbb{Z}_d)$ and z is a second degree character given by σ_A . In other words:

Corollary 5.2. *The automorphisms of the Heisenberg group of the form (3.23) are given by conjugation by Clifford operations.*

Proof. All the possible automorphisms of this type have z a second degree character given by σ_A , where $A \in SL_2(\mathbb{Z}_d)$, i.e. $(A, z) \in \text{Ind}(d)$. If a is a Clifford operation with this index, then conjugation by a gives such an automorphism of \hat{H} . \square

6. Appleby indexing

If d is odd, then $-\mu = \omega^{\frac{d+1}{2}}$, and it follows from (3.16) that

$$z_a(p) = (-\mu)^{p^T \sigma_{AP}} \hat{z}_a(p), \quad \forall p \in \mathbb{Z}_d^2, \tag{6.32}$$

where $A = \psi_a$, and \hat{z}_a is a character. If d is even, then the factor $(-\mu)^{p^T \sigma_{AP}}$ above is not well defined. To obtain an analogue of (6.32), one must ‘lift’ A to a $B \in SL_2(\mathbb{Z}_{2d}^2)$. This ‘doubling’ works, but the corresponding (Appleby) index $[B, \chi]$ is not unique. We now give the details, as in [App05], using corollary 5.1 to streamline the proof.

Define displacement operators by

$$\hat{D}_p := (-\mu)^{p_1 p_2} S^{p_1} \Omega^{p_2}, \quad p \in \mathbb{Z}^2. \tag{6.33}$$

These satisfy $\det(\hat{D}_p) = 1$,

$$\hat{D}_p^{-1} = \hat{D}_{-p}, \quad \hat{D}_p \hat{D}_q = (-\mu)^{\langle\langle p, q \rangle\rangle} \hat{D}_{p+q} = \omega^{\langle\langle p, q \rangle\rangle} \hat{D}_q \hat{D}_p, \tag{6.34}$$

and

$$\hat{D}_{p+dq} = \begin{cases} \hat{D}_p, & d \text{ odd;} \\ (-1)^{\langle\langle p, q \rangle\rangle} \hat{D}_p, & d \text{ even,} \end{cases} \tag{6.35}$$

where $\langle\langle \cdot, \cdot \rangle\rangle$ denotes the *symplectic form*

$$\langle\langle p, q \rangle\rangle := p_2q_1 - p_1q_2 = p^T \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} q,$$

which has the property

$$\langle\langle Ap, Aq \rangle\rangle = \det(A)\langle\langle p, q \rangle\rangle, \quad \forall p, q. \quad (6.36)$$

It follows from (6.35) that \hat{D}_p depends only on $p \bmod d'$, where

$$d' := \begin{cases} d, & d \text{ odd;} \\ 2d, & d \text{ even.} \end{cases}$$

The appearance of d' in the description of $C(d)$ is due to the fact that R has order d' . The *overlaps* $\chi_p^\Pi := \text{trace}(\Pi \hat{D}_p)$, $p \in \mathbb{Z}_{d'}^2$, for a SIC fiducial $\Pi = vv^*$ play a crucial role in describing the Galois symmetries of a SIC.

We now generalise (6.32), to show that for each $[a] \in C(d)/[I]$ there exists a $B \in SL_2(\mathbb{Z}_{d'})$ and $\chi \in \mathbb{Z}_{d'}^2$, such that

$$a\hat{D}_p a^{-1} = \omega^{\langle\langle \chi, Bp \rangle\rangle} \hat{D}_{Bp}, \quad \forall p \in \mathbb{Z}_{d'}^2.$$

Here $\langle\langle \chi, Bp \rangle\rangle$ is interpreted as $\langle\langle \chi, Ap \rangle\rangle$, $A := B \bmod d$, when d is even. We will write the pair (B, χ) as $[B, \chi]$, and call it an *Appleby index*.

Theorem 6.1. *Define a semidirect product $SL_2(\mathbb{Z}_{d'}) \ltimes \mathbb{Z}_d^2$ via the multiplication*

$$[B_1, \chi_1][B_2, \chi_2] := [B_1 B_2, \chi_1 + A_1 \chi_2], \quad A_1 := B_1 \bmod d. \quad (6.37)$$

There exists a unique surjective homomorphism onto the Clifford operations

$$f : SL_2(\mathbb{Z}_{d'}) \ltimes \mathbb{Z}_d^2 \rightarrow C(d)/[I], \quad (6.38)$$

with the property that for $[a] = f([B, \chi])$

$$a\hat{D}_p a^{-1} = \omega^{\langle\langle \chi, Bp \rangle\rangle} \hat{D}_{Bp}, \quad \forall p \in \mathbb{Z}_{d'}^2, \quad (6.39)$$

i.e.

$$A := \psi_a = B \bmod d, \quad z_a(p) = \omega^{\langle\langle \chi, Ap \rangle\rangle} (-\mu)^{p^T \sigma_{BP}}, \quad \forall p \in \mathbb{Z}_d^2. \quad (6.40)$$

This f is an isomorphism for d odd (i.e. $d' = d$), and for d even it has kernel

$$\ker f = \left\{ \left[\begin{pmatrix} 1 + rd & sd \\ td & 1 + rd \end{pmatrix}, \begin{pmatrix} s\frac{d}{2} \\ t\frac{d}{2} \end{pmatrix} \right] : r, s, t \in \{0, 1\} \right\}. \quad (6.41)$$

Proof. If $a \in C(d)$ satisfies (6.39), then (6.40) follows. Here $p^T \sigma_{BP}$ is calculated modulo $2d$, and its value only depends on $p \bmod d$. In view of the isomorphism (5.31), f is uniquely defined, and it suffices to show that

$$\theta : SL_2(\mathbb{Z}_{d'}) \ltimes \mathbb{Z}_d^2 \rightarrow \text{Ind}(d) : [B, \chi] \mapsto (A, z_a),$$

given by (6.40) is a surjective homomorphism.

We now show it is a homomorphism (as a map to $SL_2(\mathbb{Z}_d) \times \mathbb{T}^{\mathbb{Z}_d^2}$). Now

$$\theta([B_1, \chi_1][B_2, \chi_2]) = \theta([B_1 B_2, \chi_1 + A_1 \chi_2]) = (A_1 A_2, z_{a_1 a_2}),$$

$$A_j := B_j \bmod d, \quad z_{a_1 a_2}(p) := \omega^{\langle \chi_1 + A_1 \chi_2, A_1 A_2 p \rangle} (-\mu)^{p^T \sigma_{B_1 B_2} p},$$

and

$$\theta([B_1, \chi_1])\theta([B_2, \chi_2]) = (A_1, z_{a_1})(A_2, z_{a_2}) = (A_1 A_2, (z_{a_1} \circ A_2)z_{a_2}),$$

$$((z_{a_1} \circ A_2)z_{a_2})(p) = \omega^{\langle \chi_1, A_1 A_2 p \rangle} (-\mu)^{(B_2 p)^T \sigma_{B_1 B_2} p} \omega^{\langle \chi_2, A_2 p \rangle} (-\mu)^{p^T \sigma_{B_2} p},$$

so that θ is a homomorphism provided that

$$\langle \chi_1 + A_1 \chi_2, A_1 A_2 p \rangle = \langle \chi_1, A_1 A_2 p \rangle + \langle \chi_2, A_2 p \rangle,$$

$$p^T \sigma_{B_1 B_2} p = (B_2 p)^T \sigma_{B_1 B_2} p + p^T \sigma_{B_2} p.$$

The first follows since (6.36) gives

$$\langle \chi_2, A_2 p \rangle = \langle A_1 \chi_2, A_1 A_2 p \rangle,$$

and the second follows by the identity

$$\sigma_{B_1 B_2} = B_2^T \sigma_{B_1 B_2} + \det(B_1) \sigma_{B_2}.$$

We calculate (as in examples 3.1 and 3.2)

$$\theta\left(\left[\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, 0\right]\right) = (\psi_F, z_F), \quad \theta\left(\left[\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, 0\right]\right) = (\psi_R, z_R), \quad (6.42)$$

and

$$\theta\left(\left[\begin{pmatrix} \alpha \\ \beta \end{pmatrix}, 1\right]\right) = (z_{S^{\alpha\Omega\beta}}, \psi_{S^{\alpha\Omega\beta}}), \quad (6.43)$$

so that θ maps generators for $SL_2(\mathbb{Z}_{d'}) \times \mathbb{Z}_d^2$ to generators for $\text{Ind}(d)$, and hence is a surjective homomorphism.

Finally, we determine $\ker f = \ker \theta$. By (6.40), we have $[B, \chi] \in \ker f$ if

$$A := \psi_a = B \bmod d = I, \quad z_a(p) = \omega^{\langle \chi, A p \rangle} (-\mu)^{p^T \sigma_B p} = 1, \quad \forall p.$$

For d odd, $d' = d$, and so $B = I$ and $z_a(p) = \omega^{\chi_2 p_1 - \chi_1 p_2} = 1, \forall p$. Thus $[B, \chi] = [I, 0]$, and f is an isomorphism. For d even, $B \bmod d = I$ gives

$$B = \begin{pmatrix} 1 + rd & sd \\ td & 1 + ud \end{pmatrix}, \quad r, s, t, u \in \{0, 1\},$$

and the condition $\det(B) = 1$ gives

$$\det(B) = (1 + rd)(1 + ud) - std^2 \equiv 1 + (r + u)d \pmod{d'} \implies r = u,$$

so that

$$B = \begin{pmatrix} 1 + rd & sd \\ td & 1 + rd \end{pmatrix}, \quad \sigma_B = \begin{pmatrix} td(1 + rd) & tdsd \\ sdt & sd(1 + rd) \end{pmatrix} \equiv \begin{pmatrix} td & 0 \\ 0 & sd \end{pmatrix} \pmod{d'}.$$

Hence $z_a(p) = \omega^{\langle\langle\chi,p\rangle\rangle} (-\mu)^{p^T \sigma_B p} = \omega^{\chi_2 p_1 - \chi_1 p_2} (-\mu)^{tdp_1^2 + sdp_2^2} = 1$, which gives

$$\omega^{\chi_1 p_2 - \chi_2 p_1} = (-1)^{p_1^2 + s p_2^2} = (-1)^{p_1 + s p_2} \omega^{\frac{d}{2}(tp_1 + sp_2)}, \quad \forall p.$$

Thus, $\chi_1 = \frac{d}{2}s$, $\chi_2 = -\frac{d}{2}t = \frac{d}{2}t$, and we obtain (6.41). □

Each Clifford operation has an Appleby index $[B, \chi] \in SL_2(\mathbb{Z}_{d'}) \times \mathbb{Z}_d^2$.

- This is unique for d odd.
- There are eight choices (each differing by an element of $\ker f$) for d even.
- Appleby indices for $F, R, S^\alpha \Omega^\beta$ are given by (6.42) and (6.43).

Example 6.1. By (3.11), the index for the permutation matrix $P_\sigma, \sigma \in \mathbb{Z}_d^*$, is

$$(\psi_{P_\sigma}, z_{P_\sigma}) = (P_\sigma, 1),$$

and it has an Appleby index $[P_\sigma, 0]$, where $\sigma \in \mathbb{Z}_{d'}$, i.e. σ^{-1} is calculated modulo $2d$ when d is even (see proposition 8.1). For example, when $d = 8$ ($d' = 16$), the permutation matrix

$$P_3 = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} \text{ has eight Appleby indices } [B, \chi]$$

$$\left[\begin{pmatrix} 1 + 8r & 8s \\ 8t & 1 + 8r \end{pmatrix}, \begin{pmatrix} 4s \\ 4t \end{pmatrix} \right] \left[\begin{pmatrix} 3 & 0 \\ 0 & 11 \end{pmatrix}, 0 \right] = \left[\begin{pmatrix} 3 + 8r & 8s \\ 8t & 11 + 8r \end{pmatrix}, \begin{pmatrix} 4s \\ 4t \end{pmatrix} \right], \quad r, s, t \in \{0, 1\}.$$

Two of these have $\chi = 0$ (and B diagonal).

7. Symplectic unitaries

By (4.25), for d even, there are nontrivial *symplectic unitaries* (those generated by F, R and the scalars) which are in the Heisenberg group [App05]. We now characterise these.

Let m_d be the surjective homomorphism

$$m_d : SL_2(\mathbb{Z}_{d'}) \rightarrow SL_2(\mathbb{Z}_d) : B \mapsto A := B \pmod{d},$$

which is the identity for d odd, and for d even has kernel (see theorem 6.1)

$$K := \left\{ \begin{pmatrix} 1 + rd & sd \\ td & 1 + rd \end{pmatrix} : r, s, t \in \{0, 1\} \right\}, \quad |K| = 8. \quad (7.44)$$

Corollary 7.1. *A matrix $a \in C(d)$ is a symplectic unitary if and only if it has an Appleby index of the form $[B, 0]$. Indeed, the map*

$$\alpha : SL_2(\mathbb{Z}_{d'}) \rightarrow C_{Sp}(d)/[I] : B \mapsto f([B, 0]) \quad (7.45)$$

is a surjective homomorphism, which is an isomorphism for d odd. When d is even, $\ker \alpha = \{I, (d + 1)I\}$, and hence the only nontrivial Heisenberg operations which are symplectic are given by

$$S^{\frac{d}{2}}, \Omega^{\frac{d}{2}}, S^{\frac{d}{2}}\Omega^{\frac{d}{2}} \quad (d \text{ even}).$$

Proof. By (6.37), we have

$$[B_1 B_2, 0] = [B_1, 0][B_2, 0],$$

and so α is a homomorphism. It is onto, since by (6.42), its image contains

$$\alpha\left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right) = [F], \quad \alpha\left(\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right) = [R], \tag{7.46}$$

which are generators for $C_{Sp}(d)/[I]$. Since ψ has kernel \hat{H} (lemma 3.2), it induces a well defined homomorphism $\hat{\psi} : C_{Sp}(d)/[I] \rightarrow SL_2(\mathbb{Z}_d)$, with

$$\hat{\psi}([F]) = \psi(F) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \hat{\psi}([R]) = \psi(R) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}. \tag{7.47}$$

By (7.46) and (7.47), we conclude that

$$m_d = \hat{\psi} \circ \alpha,$$

since it holds for the generators (4.24) of $SL_2(\mathbb{Z}_{d'})$. The kernel of $\hat{\psi}$ consists of the symplectic operations which are also Heisenberg operations, i.e.

$$\ker \hat{\psi} = C_{Sp}(d)/[I] \cap \hat{H}/[I].$$

For d odd, m_d is an isomorphism, so that $\ker \hat{\psi} = \{[I]\}$. For d even,

$$m_d = \hat{\psi} \circ \alpha \implies |\ker \hat{\psi}| |\ker \alpha| = |\ker m_d| = |K| = 8,$$

and (6.35) gives

$$\hat{D}_{(d+1)p} = (-1)^{\langle p,p \rangle} \hat{D}_p = \hat{D}_{Ip} \implies (d + 1)I \in \ker \alpha \implies |\ker \alpha| \geq 2.$$

In view of (4.25), we must have

$$\ker \alpha = \{I, (d + 1)I\}, \quad \ker \hat{\psi} = \{[I], [S^{\frac{d}{2}}], [\Omega^{\frac{d}{2}}], [S^{\frac{d}{2}}\Omega^{\frac{d}{2}}]\},$$

as claimed. □

Thus, each symplectic operation $[a]$ has an Appleby index of the form $[B, 0]$, and

- This is unique for d odd.
- There are two choices $([B, 0]$ and $[(d + 1)B, 0]$ for d even.

We call $B \in SL_2(\mathbb{Z}_{d'})$ a symplectic index for $[a] \in C_{Sp}(d)/[I]$.

The following commutative diagram summarises corollary 7.1.

$$\begin{array}{ccc} SL_2(\mathbb{Z}_{d'}) & \xrightarrow{\alpha} & C_{Sp}(d)/[I] \\ & \searrow m_d & \downarrow \hat{\psi} \\ & & SL_2(\mathbb{Z}_d) \end{array} \tag{7.48}$$

In particular, we have the following 1–1 indexing of the symplectic operations

$$\frac{C_{Sp}(d)}{[I]} \cong \begin{cases} SL_2(\mathbb{Z}_d), & d \text{ odd;} \\ \frac{SL_2(\mathbb{Z}_{2d})}{\langle (d+1)I \rangle}, & d \text{ even.} \end{cases}$$

The matrices in $SL_2(\mathbb{Z}_{d'})$ are said to be *symplectic*. If a is a symplectic unitary, with symplectic index B , then (6.39) gives

$$a\hat{D}_p a^{-1} = \hat{D}_{Bp}, \quad \forall p(\in \mathbb{Z}_{d'}),$$

i.e. the conjugation action of a on the displacement \hat{D}_p is given by multiplication of p by the symplectic matrix B . This is the origin of the term *symplectic unitary*.

The group $C_{Sp}(d)$ of symplectic unitaries is *not irreducible* for $d > 2$, since its centre contains the nondiagonal matrix

$$P_{-1} = F^2.$$

Calculations in $C_{Sp}(d)/[I]$ can be done in the finite group generated by F and R .

8. Permutation matrices

Here we show that the permutation matrices are a subgroup of the symplectic unitaries (as we define them), i.e. each permutation matrix is a word in F , R and the scalar matrices.

Proposition 8.1. *The permutation matrices P_b , $b \in \mathbb{Z}_d^*$, are symplectic. Indeed, with $1 \leq b < d$, we have*

$$P_b = (c_{b,d})^{-1} R^{b^{-1}} F R^b F R^{b^{-1}} F, \tag{8.49}$$

where b^{-1} is the inverse of b in \mathbb{Z}_d^* , and $c_{b,d} = c_{b^{-1},d}$ is the Gauss sum

$$c_{b,d} := \frac{1}{\sqrt{d}} \sum_{j \in \mathbb{Z}_d} \mu^{bj(j+d)} = \frac{1}{2\sqrt{d}} G(b(d+1), 2d).$$

Proof. Let $B = \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix} \in SL_2(\mathbb{Z}_{d'})$. Then $\sigma_B = 0$, and so (3.11) gives

$$A := \psi_{P_b} = B \text{ mod } d, \quad z_{P_b}(p) = 1 = \omega^{\langle (0,Ap) \rangle} (-\mu)^{p^T \sigma_{Bp}}, \quad \forall p \in \mathbb{Z}_d^2.$$

By theorem 6.1, this implies that $[B, 0]$ is an Appleby index for P_b , which is therefore a symplectic unitary, with symplectic index B . Now B can be factored

$$B = \begin{pmatrix} b & \\ & b^{-1} \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & -b^{-1} \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -b \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -b^{-1} \end{pmatrix}. \tag{8.50}$$

In view of (6.42), a symplectic index for $R^b F$ is given by

$$\begin{pmatrix} 0 & -1 \\ 1 & -b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^b \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

and so applying the homomorphism α of corollary 7.1 to (8.50) gives (8.49), for some scalar $c_{b,d}$, to be determined. From (3.6) and (3.7), we have

$$(R^b F)_{jk} = \frac{1}{\sqrt{d}} \mu^{bj(j+d)+2jk}. \tag{8.51}$$

Hence, equating the $(0, 0)$ -entries of $c_{b,d} P_b (R^{b^{-1}} F)^{-1} = R^b F R^{b^{-1}} F$, gives

$$\frac{1}{\sqrt{d}} c_{b,d} = \sum_{j \in \mathbb{Z}_d} (R^b F)_{0j} (R^{b^{-1}} F)_{j0} = \frac{1}{d} \sum_{j \in \mathbb{Z}_d} \mu^{b^{-1}j(j+d)}.$$

We recall that $\mu^{j(j+d)}$ depends only on j modulo d , and $\mu^{jd} = \mu^{d^2}$, so that

$$c_{b,d} = \frac{1}{2} \frac{1}{\sqrt{d}} \sum_{j=0}^{2d-1} \mu^{b^{-1}j(j+d)} = \frac{1}{2\sqrt{d}} \sum_{j=0}^{2d-1} \mu^{b^{-1}(d+1)j^2} = \frac{1}{2\sqrt{d}} G(b^{-1}(d+1), 2d).$$

Evaluating the $(0, 0)$ -entries of (8.49), using (8.51), gives

$$c_{b,d} = \frac{1}{d\sqrt{d}} \sum_{j \in \mathbb{Z}_d} \sum_{k \in \mathbb{Z}_d} \mu^{bj(j+d)+2jk+b^{-1}k(k+d)} = c_{b^{-1},d}.$$

□

If the b^{-1} is computed as the inverse in \mathbb{Z}_d^* for d even, then the formula (8.49) only gives P_b up to multiplication by the symplectic Heisenberg operations (4.25). The permutation matrices $\{P_\sigma\}_{\sigma \in \mathbb{Z}_d^*}$ are a subgroup of the symplectic unitaries, since the map $\mathbb{Z}_d^* \rightarrow \text{CSp}(d) : \sigma \rightarrow P_\sigma$ is a group homomorphism, by the calculation

$$(P_{\sigma_1 \sigma_2})_{jk} = \sum_r (P_{\sigma_1})_{jr} (P_{\sigma_2})_{rk} = \delta_{j, \sigma_1 r} \delta_{r, \sigma_2 k} = \sigma_{j, \sigma_1 \sigma_2 k} = (P_{\sigma_1 \sigma_2})_{jk}.$$

The formulas for evaluating Gauss sums imply that $c_{b,d}$ is an 8th root of unity, e.g. if b has odd order, then $c_{b,d} = (\sqrt{i})^{1-d}$.

Example 8.1. When $b = 1$, (8.49) gives

$$(RF)^3 = c_{1,d} P_1 = e^{-\frac{2\pi i}{8}(d-1)} I.$$

Thus $[RF]$ is a symplectic operation of order three.

The symplectic unitary of order three (as a matrix), given by

$$Z := \zeta^{d-1} RF, \quad \zeta := e^{\frac{2\pi i}{24}}, \quad \psi_Z = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},$$

is called the Zauner matrix. This matrix plays a central role in the construction of SICs, since the majority of the known SICs are can be obtained as eigenvectors of Z . The Zauner matrix satisfies

$$R^{-1} Z R = \bar{Z}^2, \quad R^{-1} Z^2 R = \bar{Z}, \tag{8.52}$$

$$Z(S^j \Omega^k) Z^{-1} = \mu^{k(k-2j+d)} S^{-k} \Omega^{j-k}, \tag{8.53}$$

and by (5.28) and (5.30)

$$\psi_Z = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \quad \psi_{Z^2} = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \quad \psi_{\bar{Z}} = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \quad \psi_{\bar{Z}^2} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}.$$

In view of its definition, Z can substitute for either F or R as the generators for the Clifford group given by theorem 4.1. Since the antilinear map of entrywise complex conjugation

$$C : \mathbb{C}^d \rightarrow \mathbb{C}^d : z \mapsto \bar{z}$$

maps SIC fiducials to SIC fiducials (as does the Clifford group), it is natural to consider the extended Clifford group $\text{EC}(d)$, which is generated by C and the Clifford group. Thus we have the following cute corollary of theorem 4.1.

Corollary 8.1. *The extended Clifford group is generated by \hat{H} , and*

$$C \text{ (order 2), } \quad Z \text{ (order 3), } \quad F \text{ (order 4).}$$

In addition to being symplectic and of order three, Z has *Clifford trace*

$$\text{trace}(\psi_Z) = -1 \in \mathbb{Z}_d.$$

We now give a complete characterisation of all such symplectic unitaries.

9. The symplectic unitaries of order three

The Clifford trace is the map

$$\text{tr}_C : \mathbb{C}(d) \rightarrow \mathbb{Z}_d : a \mapsto \text{trace}(\psi_a).$$

Since $a \mapsto \psi_a$ is a homomorphism with kernel \hat{H} (lemma 3.2), this satisfies

$$\text{tr}_C(ab) = \text{tr}_C(ba), \quad \forall a, b \in \mathbb{C}(d), \quad (9.54)$$

$$\text{tr}_C(ah) = \text{tr}_C(a), \quad \forall a \in \mathbb{C}(d), \forall h \in \hat{H}. \quad (9.55)$$

In particular, the Clifford trace of any conjugate of Z or $Z^{-1} = Z^2$ is -1 , e.g.

$$\text{tr}_C(gZg^{-1}) = \text{tr}_C(Zg^{-1}g) = \text{tr}_C(Z) = \text{trace}(\psi_Z) = -1,$$

and the Clifford trace is well defined on the Clifford operations, i.e.

$$\text{tr}_C([a]) := \text{tr}_C(a), \quad \forall [a] \in \text{PC}(d).$$

The order of a Clifford operation is related to its Clifford trace, since

$$A^2 = \text{trace}(A)A - I, \quad \forall A \in \text{SL}_2(\mathbb{Z}_d). \quad (9.56)$$

Lemma 9.1. *A nonidentity extended Clifford operation $[a] \in \text{EC}(d)/[I]$ with index (A, z_a) and Clifford trace $t = \text{trace}(A)$ has order 3 if and only if*

$$(t^2 - 1)A = (t + 1)I, \quad z_a((t + 1)Ap) = \omega^{(t+1)p^T M_A p}, \quad \forall p \in \mathbb{Z}_d^2, \quad (9.57)$$

where $M_A = \begin{pmatrix} \gamma(\alpha^3 + 2\alpha^2\delta + \alpha\delta^2 - 2\alpha - \delta) & \beta\gamma(\alpha + \delta - 1)(\alpha + \delta + 1) \\ \beta\gamma(\alpha + \delta - 1)(\alpha + \delta + 1) & \beta(\delta^3 + 2\alpha\delta^2 + \alpha^2\delta - 2\delta - \alpha) \end{pmatrix}$, $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$.

Proof. Since a product of three antiunitaries is not a unitary matrix, we have that $a \in \mathbb{C}(d)$. In view of the isomorphism (5.31), $[a]$ has order 3 if and only if

$$(A, z_a)^3 = (A^3, (z_a \circ A^2)(z_a \circ A)z_a) = (I, 1).$$

From (9.56), we obtain

$$A^3 = A(tA - I) = t(tA - I) - A = (t^2 - 1)A - tI,$$

so that the condition $A^3 = I$ can be written as the first condition of (9.57).

We now consider the condition $(z_a \circ A^2)(z_a \circ A)z_a = 1$. By (3.16), we calculate

$$\begin{aligned} z_a(p)z_a(Ap)z_a(A^2p) &= \omega^{-p^T \sigma_A(Ap)} z_a(p + Ap)z_a(A^2p) \\ &= \omega^{-p^T \sigma_A(Ap)} \omega^{-(p+Ap)^T \sigma_A(A^2p)} z_a(p + Ap + A^2p) \\ &= \omega^{-p^T (\sigma_A A + \sigma_A A^2 + A^T \sigma_A A^2)} z_a(p + Ap + A^2p). \end{aligned}$$

By (9.56), we have

$$I + A + A^2 = I + A + tA - I = (1 + t)A.$$

Using $\det(A) = \alpha\delta - \beta\gamma = 1$, a calculation gives

$$\begin{aligned} &\sigma_A A + \sigma_A A^2 + A^T \sigma_A A^2 \\ &= (\alpha + \delta + 1) \begin{pmatrix} \gamma(\alpha^3 + 2\alpha^2\delta + \alpha\delta^2 - 2\alpha - \delta) & \beta\gamma(\alpha + \delta - 1)(\alpha + \delta + 1) \\ \beta\gamma(\alpha + \delta - 1)(\alpha + \delta + 1) & \beta(\delta^3 + 2\alpha\delta^2 + \alpha^2\delta - 2\delta - \alpha) \end{pmatrix}. \end{aligned}$$

Thus we may rewrite the condition $(z_a \circ A^2)(z_a \circ A)z_a = 1$, to obtain the result. □

Example 9.1. Since $z_a(0) = 1, \forall a \in \text{EC}(d)$, and $\text{tr}_C(I) = 2 = -1$ if and only if $d = 3$, we have that if $a \in C(d)$ has Clifford trace -1 and $d \neq 3$, then $[a]$ has order 3.

Taking the trace of $(t^2 - 1)A = (t + 1)I$, shows that a Clifford operation of order 3 has Clifford trace t satisfying

$$(t - 2)(t + 1)^2 = 0. \tag{9.58}$$

For d a prime, the Clifford operators of order 3 must have Clifford trace -1 .

Proposition 9.1. *Suppose that $d \neq 3$ and $a \in C(d)$. Then*

1. *If a has Clifford trace -1 , then $[a]$ has order 3.*
2. *If d is prime, then $[a]$ has order 3 if and only if a has Clifford trace -1 .*

Proof. Since we have already proved 1, it suffices to prove for $d \neq 3$ prime and $[a]$ of order 3 that the Clifford trace $t = \text{tr}_C(a)$ is -1 . We recall that t is a root of (9.58).

If $t \neq -1$, then $t + 1$ is a unit (all nonzero elements of \mathbb{Z}_d are units for d prime), so that $t = 2$. But, if $t = 2$, then (9.57) gives $3A = 3I$, and hence $A = I$ ($3 \in \mathbb{Z}_d^*$ for $d \neq 3$ prime), so that $a \in \hat{H}$ (by lemma 3.2). Since $(S^j \Omega^k)^3 = \omega^3 S^{3j} \Omega^{3k}$ and S, Ω have order d , the order of $[a]$ cannot be 3 (since 3 does not divide d). Thus $t = \text{tr}_C(a) - 1$ (when $[a]$ has order 3 and $d \neq 3$ is prime). □

A Clifford operation of order 3 is said to be canonical order 3 if it has Clifford trace -1 (see [App05]), e.g. the Zauner matrix Z and W_1, W_2 (theorem 9.1) are canonical order 3.

Example 9.2. It follows from (9.54) and (9.55) that left or right multiplication of a canonical order 3 Clifford operation by a displacement operation gives another canonical order 3 operation, e.g. $[h_1 Z h_2]$ is canonical order 3 for any $h_1, h_2 \in \hat{H}$.

There are Clifford operations of order 3 with Clifford trace 2.

Example 9.3. If 3 divides d , then the symplectic unitary $R^{\frac{d'}{3}}$ (and its inverse) has order 3 and Clifford trace

$$\text{tr}_C(R^{\frac{d'}{3}}) = \text{trace}\left(\begin{pmatrix} 1 & 0 \\ \frac{d'}{3} & 1 \end{pmatrix}\right) = 2,$$

as do the Weyl displacement operators $S^{\frac{d'}{3}}, \Omega^{\frac{d'}{3}}, S^{\frac{d'}{3}}\Omega^{\frac{d'}{3}}$.

There are Clifford operations of order 3 with Clifford trace $t \neq -1, 2$, i.e. for which (9.58) holds with $t - 2$ and $t + 1$ not units in \mathbb{Z}_d .

Example 9.4. For $d = 10$, $SL_2(\mathbb{Z}_{10})$ has a single conjugacy class of elements of order 3 and trace 4 and 7. These have representatives

$$A = \begin{pmatrix} 3 & 2 \\ 6 & 1 \end{pmatrix} \quad (\text{trace } 4), \quad B = \begin{pmatrix} 6 & 5 \\ 5 & 1 \end{pmatrix} \quad (\text{trace } 7).$$

These can be lifted to symplectic indices which give symplectic unitaries of order 3 and Clifford trace 4 and 7, e.g. $a = R^{10}FR^8F^{-1}R^6, b = R^{10}FR^5F^{-1}R^{15}$.

The main technical result of the paper is the following lemma. This is essentially a proof the Conjecture 4 of [Fla06] on the number of conjugacy classes (d is replaced by $2d$ for d even), which was proved for d prime.

Lemma 9.2. *Suppose that $d \geq 2$, and let*

$$z := \psi_Z = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \quad z^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \tag{9.59}$$

$$m_1 := \begin{pmatrix} 1 & 3 \\ \frac{d-3}{3} & -2 \end{pmatrix}, \quad d \equiv 3 \pmod{9}, \tag{9.60}$$

$$m_2 := \begin{pmatrix} 1 & 3 \\ \frac{2d-3}{3} & -2 \end{pmatrix}, \quad d \equiv 6 \pmod{9}. \tag{9.61}$$

Then the conjugacy classes of elements of order 3 and trace -1 in $SL_2(\mathbb{Z}_d)$ have representatives

$$\{z\}, \quad d \not\equiv 0 \pmod{3}, \tag{9.62}$$

$$\{z, z^2\}, \quad d \equiv 0 \pmod{9} \text{ or } d = 3, \tag{9.63}$$

$$\{z, z^2, m_1\}, \quad d \equiv 3 \pmod{9}, \quad d \neq 3, \tag{9.64}$$

$$\{z, z^2, m_2\}, \quad d \equiv 6 \pmod{9}. \tag{9.65}$$

By the Chinese remainder theorem, it is sufficient to prove this for d a prime power. The proof is given in the appendix. It is elementary, but long, since each case involves the solution of a binary quadratic equation.

We also need the following technical lemmas.

Lemma 9.3. *Let $\varphi : G \rightarrow H$ be a homomorphism of G onto H , with $|\ker \varphi| = 2^k$. If $h \in H$ has order 3, then there is an element $g \in G$ of order 3 with $\varphi(g) = h$.*

Proof. By the first isomorphism theorem for groups, we may assume that $H = G/K$, where $K = \ker \varphi$. Suppose that $h = aK \in G/K$ has order 3, i.e. $a^3 = x \in K$, where $a \notin K$. By Bézout’s identity (the Euclidean algorithm) choose integers α, β with $1 = -3\alpha + 2^k\beta$. Let $g = ax^\alpha \in \langle a \rangle$. Then $\varphi(g) = ax^\alpha K = aK$, and

$$g^3 = (ax^\alpha)^3 = a^3 x^{3\alpha} = x^{3\alpha+1} = x^{2^k\beta} = 1. \quad \square$$

Lemma 9.4. *For d even, $SL_2(\mathbb{Z}_{2d})$ has no elements of order 3 and trace $d - 1$.*

Proof. If $A \in SL_2(\mathbb{Z}_{2d})$ has order 3, and $t = \text{trace}(A)$, then, by (9.56), we have

$$A^3 = A(tA - I) = t(tA - I) - A = (t^2 - 1)A - tI = I \implies (t^2 - 1)A = (t + 1)I.$$

For $t = d - 1$, this gives $(d^2 - 2d)A = 0 = dI \pmod{2d}$, which not possible. □

We now characterise all symplectic unitaries of canonical order 3.

Theorem 9.1 (Characterisation). *The symplectic operations of canonical order 3 are conjugate in $C_{Sp}(d)/[I]$ to $[a]$, where $a \in C_{Sp}(d)$ is one of the following*

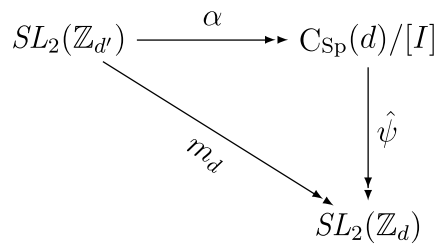
$$\begin{aligned} & \{Z\}, \quad d \not\equiv 0 \pmod{3}, \\ & \{Z, Z^2\}, \quad d \equiv 0 \pmod{9} \text{ or } d = 3, \\ & \{Z, Z^2, W_1\}, \quad d \equiv 3 \pmod{9}, d \neq 3, \\ & \{Z, Z^2, W_2\}, \quad d \equiv 6 \pmod{9}, \end{aligned}$$

where

$$\begin{aligned} Z &:= e^{\frac{2\pi i}{2d}(d-1)} R F^{-1}, \\ W_a &:= (-1)^{d-1} R^{\frac{2d}{3}a} F^{-1} R^3 F R, \end{aligned} \tag{9.66}$$

have order 3 in $C_{Sp}(d)$.

Proof. The key idea is to apply the fact that group homomorphisms map conjugacy classes to conjugacy classes to the commutative diagram (7.48) of section 7, i.e.



We observe that

- The kernel of $\hat{\psi}$ has order 1 or 4 (d odd or even), and so the conjugacy classes of elements of order 3 and Clifford trace -1 in $C_{Sp}(d)/[I]$ map onto the conjugacy classes of elements of order 3 and trace -1 in $SL_2(\mathbb{Z}_d)$ (by lemma 9.3).

- The kernel of α has 1 or 2 (d odd or even), and so each conjugacy class of an element of order 3 and Clifford trace -1 in $C_{Sp}(d)/[I]$ is the image under α of the conjugacy class of an element of order 3 in $SL_2(\mathbb{Z}_{d'})$ (by lemma 9.3) and of trace -1 (by lemma 9.4).

Thus the conjugacy classes of elements of order 3 and trace -1 in $SL_2(\mathbb{Z}_{d'})$ map onto the conjugacy classes of elements of canonical order 3 in $C_{Sp}(d)/[I]$, which in turn map onto the conjugacy classes of elements of order 3 and trace -1 in $SL_2(\mathbb{Z}_d)$. A count of the conjugacy classes in $SL_2(\mathbb{Z}_{d'})$ and $SL_2(\mathbb{Z}_d)$ (for d even) shows that these maps are 1-1, i.e. representatives of the conjugacy classes of elements of order 3 and trace -1 in $SL_2(\mathbb{Z}_{d'})$ give symplectic indices for representatives of the conjugacy classes of the symplectic operations of canonical order 3.

We now use lemma 9.2 to calculate these symplectic indices (and show the injectivity asserted above) for the various cases.

For $d \not\equiv 0 \pmod{3}$, we have $2d \not\equiv 0 \pmod{3}$, and so there is a single conjugacy class with symplectic index z .

For $d \equiv 0 \pmod{9}$, $d \neq 3$, we have $2d \equiv 0 \pmod{9}$, and so there are two conjugacy classes given by the symplectic indices z, z^2 . For $d = 3$, we have $d' = d$, and there are two conjugacy classes given by the symplectic indices z, z^2 .

For $d \equiv 3 \pmod{9}$, $d \neq 3$, we have $2d \equiv 6 \pmod{9}$, so that there are three conjugacy classes given by the symplectic indices z, z^2 , and

$$\begin{pmatrix} 1 & 3 \\ \frac{d-3}{3} & -2 \end{pmatrix} \in SL_2(\mathbb{Z}_d) \quad (d \text{ odd}), \quad \begin{pmatrix} 1 & 3 \\ \frac{2(2d)-3}{3} & -2 \end{pmatrix} \in SL_2(\mathbb{Z}_{2d}) \quad (d \text{ even}).$$

The second formula gives the first for d odd, and so works in both cases.

For $d \equiv 6 \pmod{9}$, we have $2d \equiv 3 \pmod{9}$, so that there are three conjugacy classes given by the symplectic indices z, z^2 , and

$$\begin{pmatrix} 1 & 3 \\ \frac{2d-3}{3} & -2 \end{pmatrix} \in SL_2(\mathbb{Z}_d) \quad (d \text{ odd}), \quad \begin{pmatrix} 1 & 3 \\ \frac{2d-3}{3} & -2 \end{pmatrix} \in SL_2(\mathbb{Z}_{2d}) \quad (d \text{ even}).$$

In the last two cases, the third conjugacy class is given by the symplectic indices m_1 and m_2 (respectively), where

$$m_j := \begin{pmatrix} 1 & 3 \\ \frac{4dj-3}{3} & -2 \end{pmatrix} \in SL_2(\mathbb{Z}_{d'}).$$

and m_j^2 is conjugate to m_j (since otherwise there would be four conjugacy classes). For convenience of presentation, we take the representative with symplectic index

$$w_j := m_j^2 = \begin{pmatrix} -2 & -3 \\ 1 + \frac{2d}{3}j & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{\frac{2d}{3}j} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^3 \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

By taking the symplectic operations corresponding to the representatives z, z^2, w_1, w_2 in the above conjugacy classes, i.e. Z, Z^2, W_1, W_2 , we obtain representatives for the conjugacy classes of canonical order 3 symplectic operations. The normalisation of W_a in its definition (9.66) ensures that it has order 3. \square

From the above proof, we have:

Table 1. The index (ψ_a, z_a) and an Appleby index $[B, \chi]$ for various Clifford operations.

a	ψ_a	$z_a(j,k)$	$[B, \chi]$
$S^\alpha \Omega^\beta$	I	$\omega^{\beta j - \alpha k}$	$[I, \begin{pmatrix} \alpha \\ \beta \end{pmatrix}]$
F	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	ω^{-jk}	$[\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, 0]$
R	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	$\mu^{j(j+d)}$	$[\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, 0]$
P_σ	$\begin{pmatrix} \sigma & 0 \\ 0 & \sigma^{-1} \end{pmatrix}$	1	$[\begin{pmatrix} \sigma & 0 \\ 0 & \sigma^{-1} \end{pmatrix}, 0]$

The conjugacy classes of order 3 and trace -1 elements in $SL(\mathbb{Z}_{d'})$ are in 1–1 correspondence with the conjugacy classes of canonical order 3 symplectic operations.

The canonical order 3 symplectic operations Z (the Zauner matrix) and $M_1 = W_1^2$ appear as symmetries of the Scott–Grassl SICs [SG10], where they are denoted by the symplectic indices F_z and F_a , i.e.

$$B_z = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = (d+1)F_z, \quad B_{m_1} = \begin{pmatrix} d+1 & 3 \\ \frac{d-3}{3} & d-2 \end{pmatrix} = (d+1)F_a.$$

As yet, no numerical SIC fiducials have been found that are eigenvectors of W_2 (see [ABDF17, AB18] for discussion). We propose the name of a ghost SIC for such SIC.

10. Conjugates of the canonical order 3 symplectic unitaries

We now use theorem 9.1 to determine when the conjugate of Z or W_1 (or W_2 for that matter) by a symplectic operation is a monomial matrix of the form $R^\alpha P_\sigma$. Since the permutation matrices in $C(d)$ are symplectic (see section 8), there exists a permutation matrix $P_\sigma \in C(d)$, $\sigma \in \mathbb{Z}_d^*$ of canonical order 3 if and only if

$$P_\sigma^3 = P_{\sigma^3} = I, \quad \text{tr}_C(P_\sigma) = \sigma + \sigma^{-1} = -1,$$

i.e. the existence of an integer σ (for $d \neq 3$) with

$$\sigma^3 \equiv 1 \pmod{d}, \quad \sigma^2 + \sigma + 1 \equiv 0 \pmod{d}. \tag{10.67}$$

For such a σ , we have $\begin{pmatrix} \sigma & 0 \\ \alpha & \sigma^{-1} \end{pmatrix}^3 = \begin{pmatrix} \sigma^3 & 0 \\ \alpha(1 + \sigma + \sigma^2) & \sigma^{-3} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, so that:

If σ satisfies (10.67), then $[R^\alpha P_\sigma]$ is a canonical order 3 symplectic operation.

By Chinese remainder theorem, one has (see [App05]) that the condition (10.67) is equivalent to d satisfying:

- (i) d has at least one prime divisor $\equiv 1 \pmod{3}$.
- (ii) d has no prime divisors $\equiv 2 \pmod{3}$ (so that d is odd).
- (iii) d is not divisible by 9.

The first few d satisfying these conditions are

$$d = 7, 13, 19, 21, 31, 37, 39, 43, 49, 57, 61, 67, 73, 79, 91, 93, 97, \dots$$

By theorem 9.1, the monomial operation $[R^\alpha P_\sigma]$ is conjugate (via a symplectic operation) to one of $[Z], [Z]^2, [W_1], [W_2]$.

- For d not a multiple of 3 ($d \not\equiv 0 \pmod{3}$), i.e.

$$d = 7, 13, 19, 31, 37, 43, 49, 61, 67, 73, 79, 91, 97, \dots$$

there is single conjugacy class, and so all $[R^\alpha P_\sigma]$ are conjugate to $[Z]$.

- For d a multiple of 3, i.e.

$$d = 21, 39, 57, 93, 111, 129, 147, 183, 201, 219, 237, \dots$$

we have $\frac{d}{3} \equiv 1 \pmod{3}$, i.e. $d \equiv 3 \pmod{9}$, and so the conjugacy classes are given by $[Z], [Z]^2, [W_1]$.

For a σ satisfying $\sigma^3 = 1, 1 + \sigma + \sigma^2$, the symplectic index calculations

$$gzg^{-1} = \begin{pmatrix} \sigma & 0 \\ 1 & \sigma^2 \end{pmatrix}, \quad gz^2g^{-1} = \begin{pmatrix} \sigma^2 & 0 \\ -1 & \sigma \end{pmatrix}, \quad g := \begin{pmatrix} 1 & \sigma \\ 0 & 1 \end{pmatrix}, \quad z = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},$$

give the following:

For any d , if σ satisfies (10.67), then

1. The monomial operation $[RP_\sigma]$ is a symplectic conjugate of $[Z]$.
2. The monomial operation $[R^{-1}P_\sigma]$ is a symplectic conjugate of $[Z^2]$.

Whenever d is a multiple of 3, i.e. $d \equiv 3 \pmod{9}$, it appears (for the d listed above) that $[P_\sigma]$ is always a symplectic conjugate of $[M_1]$.

Example 10.1. For $d = 21$, no symplectic conjugate of Z is a permutation matrix, but many conjugates are monomial, e.g. the symplectic index calculation

$$\begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 4 & 0 \\ 1 & 16 \end{pmatrix},$$

together with table 1, gives

$$gZg^{-1} = \omega^7 R^{16} P_4, \quad g := F^{-1} R^{-4} F.$$

Acknowledgment

We would like to thank Andrew Scott, Marcus Appleby, Markus Grassl and Steve Flammia for many helpful discussions related to the canonical order three unitaries.

Appendix

Proof of lemma 9.2. We first show that it suffices to consider the case of d a prime power. Let $d = \prod_{j=1}^m p_j^{r_j}$ be a product of powers of distinct primes. If $a, b \in SL_2(\mathbb{Z}_d)$ are conjugate:

$a = bgb^{-1}$, $g \in SL_2(\mathbb{Z}_d)$, then they are conjugate in $SL_2(\mathbb{Z}_{p_j^{r_j}})$, i.e.

$$ag_j \equiv g_j b \pmod{p_j^{r_j}}, \quad 1 \leq j \leq m, \tag{A.1}$$

where $g_j \equiv g \pmod{p_j^{r_j}}$ and $g_j \in SL_2(\mathbb{Z}_{p_j^{r_j}})$. Conversely, suppose that a and b are conjugate in $SL_2(\mathbb{Z}_{p_j^{r_j}})$ via $g_j \in SL_2(\mathbb{Z}_{p_j^{r_j}})$, $1 \leq j \leq m$. Then by the Chinese remainder theorem, there is a $g \in \mathbb{Z}^{2 \times 2}$ with $g \equiv g_j \pmod{p_j^{r_j}}$, so that (A.1) gives

$$ag \equiv gb \pmod{d} = \prod_{j=1}^m p_j^{r_j}.$$

Similarly, $\det(g) \equiv \det(g_j) \equiv 1 \pmod{p_j^{r_j}}$, gives $\det(g) \equiv 1 \pmod{d}$. Thus a and b are conjugate in $SL_2(\mathbb{Z}_d)$.

Hence we assume now that $d = p^r$, p a prime and begin with the easiest case:

Case 1. $p \neq 3$, i.e. d is not divisible by 3.

Here we claim that there is one single conjugacy class, i.e. if $a, b \in SL_2(\mathbb{Z}_d)$ with $\text{tr}(a) \equiv \text{tr}(b) \equiv -1 \pmod{d}$, then a is conjugate to b . Since

$$z = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \in SL_2(\mathbb{Z}_d)$$

with $\text{tr}(z) \equiv -1 \pmod{d}$, alternatively we may express this by saying that if $a \in SL_2(\mathbb{Z}_d)$ with $\text{tr}(a) \equiv -1 \pmod{d}$, then a is conjugate to z , i.e. $\exists g \in SL_2(\mathbb{Z}_d)$ such that

$$a \equiv gzg^{-1} \iff ag \equiv gz \pmod{d}.$$

It turns out that the existence of such a g reduces to the existence of a solution of an associated binary quadratic equation.

Lemma A.1. *Suppose that $d \in \mathbb{Z}_{\geq 2}$ (including the divisible by 3 case) and that*

$$a = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z}_d) \text{ with } \text{tr}(a) \equiv -1 \pmod{d}. \text{ Then there exists } g \in SL_2(\mathbb{Z}_d) \text{ such that}$$

$$a \equiv gzg^{-1} \pmod{d}$$

iff

$$g = [x; ax], \quad x \in \mathbb{Z}_d^2$$

such that

$$Q_a(x_1, x_2) := \gamma x_1^2 + (\delta - \alpha)x_1 x_2 - \beta x_2^2 \equiv +1 \pmod{d}. \tag{A.2}$$

Proof of lemma Writing $g = [x; y]$ with columns $x, y \in \mathbb{Z}_d^2$,

$$\begin{aligned} gz \equiv ag &\iff [x; y] \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \equiv a[x; y] \\ &\iff [y; -x - y] \equiv [ax; ay] \\ &\iff y \equiv ax \text{ and } ay \equiv -x - y. \end{aligned}$$

But $y \equiv ax$ implies that

$$ay \equiv a^2x \equiv -(a + I_2)x \equiv -ax - x \equiv -y - x.$$

Hence $gz \equiv ag \iff g \equiv [x; Ax]$ for an $x \in \mathbb{Z}_d^2$. Here we have used the fact that, by the modular form of the Cayley–Hamilton theorem,

$$a^2 - \text{tr}(a)a + \det(a)I_2 \equiv 0 \pmod{d}$$

so that, by our assumptions on a ,

$$a^2 \equiv \text{tr}(a)a - \det(a)I_2 \equiv -a - I_2.$$

Now, for g to be in $SL_2(\mathbb{Z}_d)$ we require that $\det(g) \equiv +1 \pmod{d}$. But for $g = [x; ax]$,

$$\begin{aligned} \det(g) &= \det \begin{pmatrix} x_1 & \alpha x_1 + \beta x_2 \\ x_2 & \gamma x_1 + \delta x_2 \end{pmatrix} \\ &= \gamma x_1^2 + (\delta - \alpha)x_1x_2 - \beta x_2^2 =: Q_a(x_1, x_2). \end{aligned} \quad \square$$

We therefore proceed to analyze the solutions of the binary quadratic equation (A.2). We begin with an important subcase.

Lemma A.2. *Suppose that $p > 2$ is a prime and that $a, b, c \in \mathbb{Z}$ are units modulo p (i.e. not multiples of p). Then*

$$ax^2 + by^2 \equiv c$$

has a solution modulo p^r for all $r \geq 1$.

Proof of lemma. We use induction on r . The $r = 1$ case is actually a ‘well-known’ consequence of the Chevalley–Warning theorem (see [IR90]); we give the details for the sake of completeness.

Homogenize the equation to

$$ax^2 + by^2 - cz^2 \equiv 0$$

giving a homogeneous quadratic equation in three variables. The Chevalley–Warning theorem then implies that there is a non-trivial integer solution (x_0, y_0, z_0) such that

$$ax_0^2 + by_0^2 - cz_0^2 \equiv 0 \pmod{p}.$$

If $z_0 \not\equiv 0 \pmod{p}$ it is a unit and we get

$$a(x_0z_0^{-1})^2 + b(y_0z_0^{-1})^2 \equiv c \pmod{p},$$

i.e. $x = x_0z_0^{-1}$, $y = y_0z_0^{-1}$ is a sought for solution. Otherwise, if $z_0 \equiv 0 \pmod{p}$ then we must have $x_0 \not\equiv 0$ and $y_0 \not\equiv 0$ and

$$\begin{aligned} ax_0^2 + by_0^2 &\equiv 0 \pmod{p} \\ \implies x_0^2 + (ba^{-1})y_0^2 &\equiv 0 \\ \implies ba^{-1} &\equiv -(x_0y_0^{-1})^2, \end{aligned}$$

i.e. $-ba^{-1} = t^2$, $t = x_0y_0^{-1}$. Thus our original equation $ax^2 + by^2 \equiv c$ reduces to

$$x^2 - t^2y^2 \equiv ca^{-1}$$

$$\iff (x - ty)(x + ty) \equiv ca^{-1}$$

which is solved, for example, by any solution of the linear system

$$x + ty \equiv ca^{-1}$$

$$x - ty \equiv 1,$$

and in particular by $x = 2^{-1}(ca^{-1} + 1)$, $y = 2^{-1}t^{-1}(ca^{-1} - 1)$.

Continuing by induction, suppose that we have a solution (x_0, y_0) modulo p^r . We will show that then we also have one modulo p^{r+1} . To see this, note first that

$$x_0 + \alpha p^r, y_0 + \beta p^r, \quad \alpha, \beta \in \mathbb{Z}$$

are also solutions modulo p^r . We claim that one of these is also a solution modulo p^{r+1} . Substituting into our equation, we have (using the fact that $p^{2r} \equiv 0 \pmod{p^{r+1}}$)

$$a(x_0 + \alpha p^r)^2 + b(y_0 + \beta p^r)^2 \equiv c \pmod{p^{r+1}}$$

$$\iff a(x_0^2 + 2x_0\alpha p^r + \alpha^2 p^{2r}) + b(y_0^2 + 2y_0\beta p^r + \beta^2 p^{2r}) \equiv c \pmod{p^{r+1}}$$

$$\iff ax_0^2 + by_0^2 + p^r(2ax_0\alpha + 2by_0\beta) + 0 \equiv c \pmod{p^{r+1}}$$

$$\iff (ax_0^2 + by_0^2 - c) + p^r((2ax_0\alpha + 2by_0\beta) + 0) \equiv c \pmod{p^{r+1}}.$$

But, by assumption, (x_0, y_0) is a solution modulo p^r and so

$$ax_0^2 + by_0^2 - c = kp^r$$

for some $k \in \mathbb{Z}$.

Consequently, we see that $(x_0 + \alpha p^r, y_0 + \beta p^r)$ is a solution modulo p^{r+1} iff

$$p^r(k + (2ax_0)\alpha + (2by_0)\beta) \equiv 0 \pmod{p^{r+1}}$$

$$\iff (k + (2ax_0)\alpha + (2by_0)\beta) \equiv 0 \pmod{p}.$$

But, as c is not a multiple of p by assumption, at least one of x_0, y_0 is also not a multiple of p and as $p > 2$, 2 is a unit, it follows that the linear Diophantine equation $(k + (2ax_0)\alpha + (2by_0)\beta) \equiv 0 \pmod{p}$ for (α, β) has at least one coefficient a unit modulo p^{r+1} and therefore has a solution. \square

Lemma A.3. *Suppose that $p > 2$ is a prime and that for $a, b, c \in \mathbb{Z}$,*

$$Q(x, y) := ax^2 + bxy + cy^2$$

is a Binary Quadratic Form with discriminant

$$\Delta := b^2 - 4ac \not\equiv 0 \pmod{p}.$$

Let $u \in \mathbb{Z}$ be a unit modulo p . Then for every $r \geq 1$, the equation

$$Q(x, y) \equiv u \pmod{p^r}$$

has a solution.

Proof of lemma. First suppose that one of $a, c \not\equiv 0 \pmod p$. By symmetry we may assume that it is $a \not\equiv 0 \pmod p$. Then modulo p^r ,

$$\begin{aligned} Q(x, y) &\equiv u \\ \iff 4aQ(x, y) &\equiv 4au \quad (\text{as both } a \text{ and } 4 \text{ are units}) \\ \iff 4ax^2 + 4abxy + 4acy^2 &\equiv 4au \\ \iff (2ax + by)^2 - \{b^2 - 4ac\}y^2 &\equiv 4au \\ \iff (2ax + by)^2 - \Delta y^2 &\equiv 4au. \end{aligned}$$

Setting $x' = 2ax + by$ we have

$$(x')^2 - \Delta y^2 \equiv 4au \pmod{p^r}$$

and by lemma A.2 there is a solution (x'_0, y_0) which leads to the solution

$$x = x_0 = 2^{-1}a^{-1}\{x'_0 - by_0\}, \quad y = y_0$$

to $Q(x, y) \equiv u \pmod{p^r}$.

If, on the other hand, $a \equiv c \equiv 0 \pmod p$ then as, by assumption, $\Delta \not\equiv 0 \pmod p$, we must have $b \not\equiv 0 \pmod p$. We need in this case to prove our claim by induction on r .

If $r = 1$ then our equation reduces to

$$bxy = u \pmod p$$

which has a solution (among others), $x = 1, y = ub^{-1}, \pmod p$.

Hence suppose that there is a solution (x_0, y_0) modulo p^r . We must show that then there is also a solution modulo p^{r+1} . Indeed, just as in the previous lemma, we search for such a solution among

$$x = x_0 + \alpha p^r, \quad y = y_0 + \beta p^r, \quad \alpha, \beta \in \mathbb{Z}.$$

Then modulo p^{r+1} ,

$$\begin{aligned} Q(x_0 + \alpha p^r, y_0 + \beta p^r) &\equiv u \\ \iff (ax_0^2 + bx_0y_0 + cy_0^2 - u) + p^r(2ax_0\alpha + bx_0\beta + by_0\alpha + 2cy_0\beta) &\equiv 0 \\ \iff (ax_0^2 + bx_0y_0 + cy_0^2 - u) + p^rb(x_0\beta + y_0\alpha) &\equiv 0 \end{aligned}$$

as $ap^r \equiv cp^r \equiv 0 \pmod{p^{r+1}}$ since, by assumption in this case a and c are multiples of p . But as (x_0, y_0) is a solution modulo p^r there must exist a $k \in \mathbb{Z}$ such that

$$ax_0^2 + bx_0y_0 + cy_0^2 - u = kp^r.$$

Therefore, cancelling p^r from both sides, we arrive at the condition

$$k + b(x_0\beta + y_0\alpha) \equiv 0 \pmod p.$$

This linear Diophantine equation has a solution for (α, β) as, in this case, b is a unit and the fact that u is a unit implies that not both x_0 and y_0 can be multiples of p . \square

We will use the above to prove

Lemma A.4. For $a = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z}_d)$, $d = p^r$, p a prime other than 3, $r \geq 1$, with $\text{tr}(a) = \alpha + \delta \equiv -1 \pmod{d}$, there is a solution of the quadratic equation (A.2), i.e. of

$$Q_a(x_1, x_2) = \gamma x_1^2 + (\delta - \alpha)x_1x_2 - \beta x_2^2 \equiv +1 \pmod{d}.$$

Consequently a is conjugate to z modulo p^r .

Proof of lemma. First suppose that $p > 3$. First note that the discriminant of Q_a is

$$\begin{aligned} \Delta &= (\delta - \alpha)^2 + 4\beta\gamma \\ &= (\delta + \alpha)^2 - 4(\alpha\delta - \beta\gamma) \\ &= (\text{tr}(a))^2 - 4\det(a) \\ &= (-1)^2 - 4 \times 1 \\ &= -3 \not\equiv 0 \pmod{p}. \end{aligned}$$

Since $u = 1$ is a unit, we have from lemma A.3 that there exists a solution to $Q_a(x_1, x_2) \equiv +1 \pmod{p^r}$.

The case $p = 2$, $d = 2^r$ is somewhat different as then 2 is not a unit and lemma A.3 is not applicable. Nevertheless, also in this case $Q_a(x_1, x_2) \equiv +1 \pmod{2^r}$ has a solution.

To see this note that the units modulo 2^r are precisely the odd integers $\leq d - 1$. Now, $\text{tr}(a) = \alpha + \delta \equiv -1 \pmod{2^r}$ implies that $\alpha + \delta$ is odd and hence one of α, δ is odd and the other is even. Consequently the product $\alpha\delta$ is even. Further, $\det(a)\alpha\delta - \beta\gamma \equiv 1 \pmod{2^r}$ and so $\alpha\delta - \beta\gamma$ is odd with $\alpha\delta$ even. Hence $\beta\gamma$ is odd and indeed both β and γ are odd, i.e. are units.

We claim that there is a solution of the form $Q_a(x_1, 1) \equiv +1 \pmod{2^r}$, i.e. with $x_2 = 1$. In fact, modulo 2^r ,

$$\begin{aligned} Q_a(x_1, 1) &\equiv +1 \\ \iff \gamma x_1^2 + (\delta - \alpha)x_1 - \beta &\equiv +1 \\ \iff x_1^2 + \gamma^{-1}(\delta - \alpha)x_1 &\equiv \gamma^{-1}(1 + \beta). \end{aligned}$$

Note that as one of α, δ is odd and the other even, $\delta - \alpha$ is odd and hence a unit. Further γ is odd and hence so is γ^{-1} . Consequently $\gamma^{-1}(\delta - \alpha)$ is odd. Moreover, β is odd and so $1 + \beta$ and $\gamma^{-1}(1 + \beta)$ are both even.

Consider now the univariate polynomial $P(x) := x^2 + ax$ with $a \in \mathbb{Z}$, odd. We claim that $P(x)$ maps the set of odd integers $\{x \in \mathbb{Z}_d : x \text{ odd}\}$ one-to-one and onto the set of even integers $\{x \in \mathbb{Z}_d : x \text{ even}\}$. Indeed, $P(x) = x^2 + ax = x(x + a)$. Hence if x is odd then $x + a$ is even and $P(x)$ is even. To see that the mapping is one-to-one, suppose that $x, y \in \mathbb{Z}_d$ are both odd. Then modulo $d = 2^r$,

$$\begin{aligned} P(x) &\equiv P(y) \\ \iff x^2 + ax &\equiv y^2 + ay \\ \iff x^2 - y^2 + a(x - y) &\equiv 0 \\ \iff (x - y)(x + y + a) &\equiv 0. \end{aligned}$$

But x, y both odd and a also odd implies that $x + y + a$ is odd and hence a unit modulo 2^f . Consequently we may divide by $x + y + a$ to obtain that $P(x) \equiv P(y)$ iff $x - y \equiv 0$, i.e. $x \equiv y$ and we have shown that the mapping is one-to-one.

To see that it is also onto just note that the cardinality of the domain $\#\{x \in \mathbb{Z}_d : x \text{ odd}\} = d/2$ as does the cardinality of the image $\#\{x \in \mathbb{Z}_d : x \text{ even}\} = d/2$.

Thus with $a = \gamma^{-1}(\delta - \alpha)$ it follows that there is an $x_1 \in \mathbb{Z}_d$ such that $P(x_1) = \gamma^{-1}(1 + \beta)$ and we are done. \square

In summary, we have shown so far that for any d a product of primes other than 3, i.e. for any d not divisible by 3, every $a \in SL_2(\mathbb{Z}_d)$ with $\text{tr}(a) \equiv -1 \pmod d$, is conjugate to $z = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$.

We now consider the cases when d is divisible by 3 beginning with

Case 2. $d = 3$

We claim that there are three conjugacy classes:

1. Those conjugate to z : $C_z := \left\{ \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \right\}$
2. Those conjugate to z^2 : $C_{z^2} := \left\{ \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \right\} = C_z^T$
3. Those conjugate to I_2 : $C_I := \{I_2\}$.

We begin with the lemma for z^2 analogous to lemma A.1 for z .

Lemma A.5. Suppose that $d \geq 2$ and that $a = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z}_d)$ with $\text{tr}(a) \equiv -1 \pmod d$.

Then there exists a $g \in SL_2(\mathbb{Z}_d)$ such that

$$a = gz^2g^{-1}$$

iff $g = [Ay; y]$ for some $y \in \mathbb{Z}_d^2$ such that

$$Q_a(y_1, y_2) = \gamma y_1^2 + (\delta - \alpha)y_1y_2 - \beta y_2^2 \equiv -1 \pmod d.$$

Proof of lemma. Writing, as before, $g = [x; y]$ with columns $x, y \in \mathbb{Z}_d^2$,

$$\begin{aligned} gz^2 \equiv ag &\iff [x; y] \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \equiv a[x; y] = [ax; ay] \\ &\iff [-x - y; x] \equiv [ax; ay] \\ &\iff x \equiv ay \text{ and } -x - y \equiv ax. \end{aligned}$$

But $x \equiv ay$ implies that

$$\begin{aligned} ax &\equiv a^2y \\ &\equiv -(a + I_2)y \\ &\equiv -ay - y \\ &\equiv -x - y. \end{aligned}$$

Hence $gz^2 \equiv ag$ iff $g = [ay; y]$ for some $y \in \mathbb{Z}_d^2$.

Now, for such g ,

$$\begin{aligned} \det(g) &= \det \begin{pmatrix} \alpha y_1 + \beta y_2 & y_1 \\ \gamma y_1 + \delta y_2 & y_2 \end{pmatrix} \\ &= \beta y_2^2 + (\alpha - \delta)y_1 y_2 - \gamma y_1^2 \\ &= -Q_a(y_1, y_2). \end{aligned}$$

Hence $\det(g) \equiv +1 \pmod{d}$ iff $Q_a(y_1, y_2) \equiv -1 \pmod{d}$. □

Now if $a \equiv I_2$ then obviously $a \in C_I$. We claim that if $a \not\equiv I_2$ then there is either a solution of

$$Q_a(y_1, y_2) \equiv +1 \pmod{3}$$

or else of

$$Q_a(y_1, y_2) \equiv -1 \pmod{3}$$

but not both. To see this note that if β and γ are both $0 \pmod{3}$ then a is diagonal and it is easily verified that the only diagonal $a \in SL_2(\mathbb{Z}_3)$ with $\text{tr}(a) \equiv -1$ is $a = I_2$. Hence at least one of β, γ are not $0 \pmod{3}$.

Now, if $\gamma \equiv 1$, then $Q_a(y_1, y_2) \equiv +1$ has the solution $y_1 = 1, y_2 = 0$. If $\gamma \equiv -1$, then $Q_a(y_1, y_2) \equiv -1$ has the solution $y_1 = 1, y_2 = 0$. Otherwise, if $\gamma \equiv 0$ and hence $\beta \not\equiv 0$, $Q_a(0, 1) \equiv -1$ if $\beta \equiv +1$ while $Q_a(0, 1) \equiv +1$ if $\beta \equiv -1$.

We now verify that we can not have solutions to *both* $Q_a(y_1, y_2) \equiv \pm 1$, or in other words, z and z^2 are *not* conjugate. Indeed, by lemma A.1 z^2 is conjugate to z iff there is a solution of

$$Q_{z^2}(x_1, x_2) \equiv +1 \pmod{3}.$$

But $Q_{z^2}(x_1, x_2) = -x_1^2 + x_1 x_2 - x_2^2$ so, modulo 3,

$$\begin{aligned} Q_{z^2}(x_1, x_2) &\equiv +1 \\ \iff x_1^2 - x_1 x_2 + x_2^2 &\equiv -1 \\ \iff x_1^2 + 2x_1 x_2 + x_2^2 &\equiv -1 \\ \iff (x_1 + x_2)^2 &\equiv -1. \end{aligned}$$

But -1 is not a perfect square modulo 3 and so this is not possible.

For $d = 3$ there are only 9 different $a \in SL_2(\mathbb{Z}_3)$ with $\text{tr}(a) \equiv -1$ and hence it is a trivial matter to list the conjugacy classes.

Case 3. $d = 3^r, r \geq 2$. We claim that here there are two conjugacy classes:

1. Those conjugate to z : $\{a \in SL_2(\mathbb{Z}_d) : (a \pmod{3}) \in C_z\}$
2. Those conjugate to z^2 : $\{a \in SL_2(\mathbb{Z}_d) : (a \pmod{3}) \in C_{z^2}\}$

The class $\{a \in SL_2(\mathbb{Z}_d) : (a \pmod{3}) = I_2\}$ is not present. Indeed, if $a \equiv I_2 \pmod{3}$, then

$$a = \begin{pmatrix} 1 + 3x & 3y \\ 3z1 + 3w & \end{pmatrix}$$

for some $x, y, z, w \in \mathbb{Z}$.

Then $\text{tr}(a) = 2 + 3(x + w)$ and

$$\det(a) = (1 + 3x)(1 + 3w) - 9yz = 1 + 3(x + w) \pmod{9}.$$

If $\text{tr}(a) \equiv -1 \pmod{3^r}, r \geq 2$, then $\text{tr}(a) \equiv -1 \pmod{9}$ and similarly $\det(a) \equiv +1 \pmod{9}$. Hence we must have

$$2 + 3(x + w) \equiv -1 \pmod{9}$$

and $1 + 3(x + w) \equiv +1 \pmod{9}$.

Subtracting the two gives $1 \equiv -2 \pmod{9}$ which is clearly not possible.

Supposing therefore that $a \not\equiv I_2 \pmod{3}$, it is easy to check by comparing with the lists of C_z and $C_{z^2} \pmod{3}$, that one of $\beta, \gamma \not\equiv 0 \pmod{3}$. By symmetry we may suppose that it is $\gamma \not\equiv 0$.

We claim that there is either a solution of

$$Q_a(x_1, x_2) \equiv +1 \pmod{3^r}$$

or $Q_a(x_1, x_2) \equiv -1 \pmod{3^r}$

but not both.

The $r = 1$ case gives a solution $(x_1, x_2) = (1, 0) \pmod{3}$ for

$$Q_a(x_1, x_2) \equiv +1 \pmod{3} \quad \text{in case } \gamma \equiv +1 \pmod{3}$$

and

$$Q_a(x_1, x_2) \equiv -1 \pmod{3} \quad \text{in case } \gamma \equiv -1 \pmod{3}.$$

This persists for $r \geq 2$, i.e. there is a solution $(x_1, x_2) = (1, 0) \pmod{3}$ for

$$Q_a(x_1, x_2) \equiv +1 \pmod{3^r} \quad \text{in case } \gamma \equiv +1 \pmod{3}$$

and

$$Q_a(x_1, x_2) \equiv -1 \pmod{3^r} \quad \text{in case } \gamma \equiv -1 \pmod{3}.$$

To see this we proceed by induction on r and assume that we have such a solution mod 3^r ; we will show that there is also one mod 3^{r+1} . Indeed,

$$(x_1 + u3^r, v3^r), \quad u, v \in \mathbb{Z}$$

are all solutions mod 3^r . Then setting $\bar{\gamma} := \gamma \pmod{3}$, we have

$$Q_a(x_1 + u3^r, v3^r) \equiv \bar{\gamma} \pmod{3^{r+1}}$$

$$\iff \gamma(x_1 + u3^r)^2 + (\delta - \alpha)(x_1 + u3^r)(v3^r) - \beta(v3^r)^2 \equiv \bar{\gamma} \pmod{3^{r+1}}$$

$$\iff \gamma(x_1^2 + 2ux_13^r) + (\delta - \alpha)(x_1v3^r) \equiv \bar{\gamma} \pmod{3^{r+1}}$$

$$\iff (\gamma x_1^2 - \bar{\gamma}) + 3^r(2\gamma x_1 u + (\delta - \alpha)x_1 v) \equiv 0 \pmod{3^{r+1}}.$$

But, as $(x_1, 0)$ is a solution mod 3^r (by assumption),

$$\gamma x_1^2 - \bar{\gamma} = k3^r$$

for some $k \in \mathbb{Z}$.

Thus

$$3^r\{k + (2\gamma x_1)u + ((\delta - \alpha)x_1)v\} \equiv 0 \pmod{3^{r+1}}$$

iff

$$k + (2\gamma x_1)u + ((\delta - \alpha)x_1)v \equiv 0 \pmod{3}$$

iff

$$k + (2\gamma)u + ((\delta - \alpha)v) \equiv 0 \pmod{3}$$

as $x_1 \equiv 1 \pmod{3}$. But this has the solution

$$\begin{aligned}
v &= 0, \\
u &= (2\gamma)^{-1}(-k) \pmod{3} \\
&\equiv (-\gamma)^{-1} \pmod{3} \\
&\equiv \gamma^{-1}k \pmod{3} \\
&\equiv \gamma k \pmod{3},
\end{aligned}$$

i.e. we have the solution

$$(x_1 + (k\gamma)3^r, 0) \pmod{3^{r+1}}.$$

The conjugacy classes are distinct as conjugacy modulo 3^{r+1} implies conjugacy modulo 3.

ORCID iDs

Shayne Waldron  <https://orcid.org/0000-0001-5612-2371>

References

- [AB18] Appleby M and Bengtsson I 2018 Simplified exact SICs (arXiv:[1811.00947](https://arxiv.org/abs/1811.00947))
- [ABDF17] 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
- [ACFW18] Appleby M, Chien T-Y, Flammia S and Waldron S 2018 Constructing exact symmetric informationally complete measurements from numerical solutions *J. Phys. A: Math. Theor.* **51** 165302
- [App05] Appleby D M 2005 Symmetric informationally complete-positive operator valued measures and the extended Clifford group *J. Math. Phys.* **46** 052107
- [AYAZ13] Appleby D M, Yadsan-Appleby H and Zauner G 2013 Galois automorphisms of a symmetric measurement *Quantum Inf. Comput.* **13** 672–720
- [BW07] Bos L and Waldron S 2007 Some remarks on Heisenberg frames and sets of equiangular lines *New Zealand J. Math.* **36** 113–37
- [Far14] Farinholt J M 2014 An ideal characterization of the Clifford operators *J. Phys. A: Math. Theor.* **47** 305303
- [FHK⁺08] Feichtinger H G, Hazewinkel M, Kaiblinger N, Matusiak E and Neuhauser M 2008 Metaplectic operators on \mathbb{C}^n *Q. J. Math.* **59** 15–28
- [FHS17] Fuchs C A, Hoang M C and Stacey B C 2017 The sic question: history and state of play *Axioms* **6** 21
- [Fla06] Flammia S T 2006 On SIC-POVMs in prime dimensions *J. Phys. A: Math. Gen.* **39** 13483–93
- [Gun62] Gunning R C 1962 *Lectures on Modular Forms (Annals of Mathematics Studies vol 48)* ed A Brumer (Princeton, NJ: Princeton University Press)
- [IR90] Ireland K and Rosen M 1990 *A Classical Introduction to Modern Number Theory (Graduate Texts in Mathematics vol 84)* 2nd edn (New York: Springer)
- [RBKSC04] 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
- [Rei89] Reiter H 1989 *Metaplectic Groups and Segal Algebras (Lecture Notes in Mathematics vol 1382)* (Berlin: Springer)
- [Sco17] Scott A J 2017 SICs: extending the list of solutions (arXiv:[1703.03993](https://arxiv.org/abs/1703.03993))
- [SG10] Scott A J and Grassl M 2010 Symmetric informationally complete positive-operator-valued measures: a new computer study *J. Math. Phys.* **51** 042203
- [VW05] Vale R and Waldron S 2005 Tight frames and their symmetries *Constr. Approx.* **21** 83–112
- [Wal18] Waldron S F D 2018 *An Introduction to Finite Tight Frames (Applied and Numerical Harmonic Analysis)* (New York: Springer)
- [Zau10] Zauner G 2010 Quantum designs: foundations of a non-commutative design theory *PhD Thesis* University of Vienna (Engl. transl. of 1999 Doctoral Thesis including a new preface)