The monomial representations of the Clifford group

D.M. Appleby\textsuperscript{1} \hspace{1cm} Ingemar Bengtsson\textsuperscript{2} \hspace{1cm} Stephen Brierley\textsuperscript{3,4}

Markus Grassl\textsuperscript{5} \hspace{1cm} David Gross\textsuperscript{6} \hspace{1cm} Jan-Åke Larsson\textsuperscript{7}

\textsuperscript{1}Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, Ontario N2L 2Y5, Canada
\textsuperscript{2}Stockholms Universitet, AlbaNova, Fysikum, S-106 91 Stockholm, Sweden
\textsuperscript{3}Department of Mathematics, University of Bristol, Bristol BS8 1TW, UK
\textsuperscript{4}QuIC, Ecole Polytechnique, Université Libre de Bruxelles, CP 165, 1050 Brussels, Belgium
\textsuperscript{5}Centre for Quantum Technologies, National University of Singapore, Singapore 117543
\textsuperscript{6}Institute for Theoretical Physics, ETH Zürich, 8093 Zürich, Switzerland
\textsuperscript{7}Institutionen för Systemteknik och Matematiska Institutionen, Linköpings Universitet, S-581 83 Linköping, Sweden.

Abstract:

We show that the Clifford group—the normaliser of the Weyl-Heisenberg group—can be represented by monomial phase-permutation matrices if and only if the dimension is a square number. This simplifies expressions for SIC vectors, and has other applications to SICs and to Mutually Unbiased Bases. Exact solutions for SICs in dimension 16 are presented for the first time.
1. Introduction

The Weyl-Heisenberg group [1] first appeared in nineteenth century algebraic geometry, and is at the roots of many things including harmonic analysis, theta functions, and—of course—quantum mechanics. Its automorphism group within the unitary group—the largest subgroup of the unitary group having the Weyl-Heisenberg group as a normal subgroup—appears in quantum information theory under the name of the Clifford group [2, 3].

The particular problem that motivated the present study is known as the SIC problem [4, 5]: in a complex Hilbert space of finite dimension $N$, find $N^2$ unit vectors $|\psi_I\rangle$ such that

$$I \neq J \Rightarrow |\langle \psi_I | \psi_J \rangle|^2 = \frac{1}{N+1}. \quad (1)$$

Such a collection of equiangular vectors [6] is known as a SIC, which is short for a Symmetric Informationally Complete POVM, where POVM is short for Positive Operator Valued Measure. In physics a SIC represents a kind of fiducial measurement, of interest for quantum state tomography [5] and indeed for the very foundations of quantum mechanics [7, 8, 9]. Such measurements can be—and in low dimensions, have been [10, 11, 12]—realised in the laboratory, but—perhaps surprisingly—the theoretical SIC problem as stated is not easy to solve. At the moment exact solutions are known in dimensions 2–16, 19, 24, 35, and 48 (with 16 added here), while convincing numerical solutions are available in dimensions 2–67. These results are due to several authors; we refer to Scott and Grassl [13] for complete references, and just remark that beyond three dimensions the known SICs look appallingly complicated at first sight.

Zauner’s conjecture [4] states that in every dimension there is an orbit of the Weyl-Heisenberg group which forms a SIC, and moreover that every vector in such a SIC is left invariant by an element of the Clifford group of order three. Hence the problem of finding a SIC reduces to that of finding a suitable fiducial vector for the group to act on, and the second—very mysterious—part of the conjecture provides some guidance when one looks for such a fiducial vector. All available evidence supports Zauner’s conjecture [13, 14].

The representation theory of the Weyl-Heisenberg group tells us that once one of its generators is given in diagonal form all its group elements
are represented by monomial phase-permutation matrices, that is by unitary matrices having only one non-zero entry per column, and per row [1]. Being products of a permutation matrix and a diagonal unitary, such matrices are also said to be of shift-and-multiply type. This property of the group can be traced back to the way that the representation is induced from that of its center. It is an important property shared by many, but not all, unitary operator bases of group type (or “nice error bases”, as they are called in quantum information theory) [15].

In general the Clifford group is not represented by phase-permutation matrices. However, after a few preliminaries in section 2, we devote section 3 to a representation of the Weyl-Heisenberg group which is special to the case when the dimension is a square, \( N = n^2 \). It can be thought of as a finite dimensional analogue of the Zak basis [16], and is used in the theory of theta functions [17]. Our observation is that in this representation the entire Clifford group is given by phase-permutation matrices. In section 4 we demonstrate that this remarkable feature is present if and only if the dimension is a square. In the remaining sections we explore some ways in which the phase-permutation basis can be useful. Section 5 illustrates how it is, in a way, aligned to SICs, while section 6 is devoted to exact solutions for SICs in \( 2^2 \) and \( 3^2 \) dimensions. In the former case they are trivial to obtain. In the latter they are not, but they look significantly better compared to how they look in the standard basis [13, 18]. In Section 7, we present new exact solutions for dimension \( 4^2 \); previously these were known in numerical form only. Section 8 contains a remark on Mutually Unbiased Bases, and section 9 summarises our conclusions. There are three appendices containing group theoretical theorems and the fiducial vectors for dimension \( 4^2 \).

2. Preliminaries

We introduce the Weyl-Heisenberg group by writing down a defining representation. Choose a dimension \( N \) and assume that \( \{|0\},\ldots,|N-1\rangle \} \) is an orthonormal basis of \( \mathbb{C}^N \). Define two phase factors \( \omega, \tau \) by

\[
\omega = e^{\frac{2\pi i}{N}}, \quad \tau = -e^{\frac{i\pi}{N}}
\]

(2)
and two operators $X, Z$ by

$$X|u\rangle = |u + 1\rangle, \quad Z|u\rangle = \omega^u|u\rangle, \quad u \in \{0, \ldots, N - 1\},$$

where here and elsewhere the labels of the vectors are computed modulo $N$. The matrix group generated by $\{\tau, X, Z\}$ is the defining representation of the Weyl-Heisenberg group $H(N)$. (It is known [1] that all irreducible representations of $H(N)$ in dimensions larger than one are unitarily equivalent to the defining one). Note that $X$ and $Z$ are represented by phase-permutation matrices, and the same is true for all the elements of the group since the product of two phase-permutation matrices is again a phase-permutation matrix.

The Weyl-Heisenberg groups $H(N)$ behave slightly differently depending on whether $N$ is even or odd. The underlying reason is that while one always has the relations

$$\omega^N = 1, \quad X^N = Z^N = 1,$$

the order of $\tau$ depends on the parity of $N$:

$$\tau^N = \begin{cases} -1 & N \text{ even} \\ 1 & N \text{ odd}. \end{cases}$$

As a consequence we will sometimes end up using arithmetic modulo $N$ in the odd case and modulo $2N$ in the even case. To unify the notation, we introduce the symbol

$$\bar{N} = \begin{cases} N & N \text{ is odd} \\ 2N & N \text{ is even}. \end{cases}$$

Since $ZX = \omega XZ$, the introduction of the phase factor $\tau$ may seem odd. If $N$ is odd, $\tau$ is in fact a power of $\omega$. The reason it is included in the even dimensional case can be traced back to the fact that there are group elements, such as $XZ$, that generate cyclic subgrops of order $2N$. For us it will be crucial that the Clifford group defined below acts on $H(N)$ as we have defined it here.

To analyze the structure of the Weyl-Heisenberg group, we define the group elements

$$D_{ij} = \tau^{ij} X^i Z^j,$$

for $i, j = 0, \ldots, \bar{N} - 1$. One can then verify the central composition law

$$D_{ij} D_{lm} = \tau^{ij - im} D_{i+l,j+m}.$$
Because the (non-scalar) generators \(X, Z\) of \(H(N)\) are just \(D_{10}\) and \(D_{01}\) respectively, the composition law (8) implies that any element of \(H(N)\) is of the form \(\tau^k D_{ij}\) for suitable integers \(i, j, k\).

Note that the phase factor \(\tau^{ij}\) in (7) depends on \(ij\) modulo \(\bar{N}\), whereas \(X^i Z^j\) only depends on \(i\) and \(j\) modulo \(N\) (by virtue of (4)). Hence the group law (8) says that \(H(N)\) modulo phase factors is isomorphic to \(\mathbb{Z}_N^2\), where \(\mathbb{Z}_N\) is the group of integers \(\{0, \ldots, N-1\}\) with addition modulo \(N\).

The situation encountered in the last paragraph will become a general theme below. Depending on our objective, we will take one of two points of view. Sometimes we will be concerned with concrete matrix representations of the groups involved. Then, we will be specific about all phase factors involved, and work with arithmetic modulo \(\bar{N}\). In other situations, however, a more abstract approach turns out to be beneficial. In these cases, we will factor out phases and work solely in terms of the discrete group \(\mathbb{Z}_N^2\) and its symmetry groups.

To make the abstract approach more precise, let \(Z(N)\) be the center of the Heisenberg-Weyl group \(H(N)\). From the group law (8), it is evident that \(Z(N) = \{\tau^k \mathbb{1}\}_{k=0, \ldots, \bar{N}-1}\), its elements are precisely the phase factors times the identity matrix. Our previous observation can now be phrased more succinctly as

\[
H(N)/Z(N) \simeq \mathbb{Z}_N^2. \tag{9}
\]

Unless \(N\) is a prime, the integers modulo \(N\) form a ring but not a field. Therefore, strictly speaking, the “vectors” \((i, j) \in \mathbb{Z}_N^2\) are elements of a module rather than of a vector space. But we permit ourselves a slight abuse of terminology and speak of vectors in \(\mathbb{Z}_N^2\).

We will be concerned with another group: the Clifford group. It consists of all unitary operators \(U_G\) normalising the Weyl-Heisenberg group, in the sense that for all \(i, j\) there are \(i', j', k'\) such that

\[
U_G D_{ij} U_G^\dagger = \tau^{k'} D_{i'j'}. \tag{10}
\]

Not all transformations \((i, j) \mapsto (i', j')\) are possible. The fact that the group law (8) involves addition of vectors in \(\mathbb{Z}_N^2\) suggests that any such transformation must be linear. Further, the fact that the symplectic inner product \((lj - im)\) modulo \(\bar{N}\) of the vectors \((i, j)\) and \((l, m)\) appears in (8) suggests that this inner product might be an invariant

\[
lj - im = l'j' - i'm' \mod \bar{N}. \tag{11}
\]
of the action of the Clifford group.

These intuitions turn out to be true and yield an almost exhaustive understanding of the Clifford group [14]. More precisely, recall that $SL(2, \bar{N})$ is the group of linear transformations on $\mathbb{Z}_\bar{N}$ leaving the symplectic inner product invariant. A $\mathbb{Z}_\bar{N}$-valued matrix

$$ G = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} $$

is an element of $SL(2, \bar{N})$ if and only if

$$ \det G = \alpha \delta - \beta \gamma = 1 \mod \bar{N}. $$

In one direction, we have that for every $G \in SL(2, \bar{N})$, there is an element $U_G$ in the Clifford group such that

$$ U_G D_{ij} U_G^\dagger = D_{G(ij)}. $$

A converse statement will be given below. The unitaries appearing in (14) are known explicitly (c.f. Ref. [14] for more details): if $\beta$ is relatively prime to $\bar{N}$ —so that it has a multiplicative inverse—one finds

$$ U_G = \frac{1}{\sqrt{N}} e^{i\theta} \sum_{u,v=0}^{N-1} \tau^{\beta^{-1}(\delta u^2 - 2uv + \alpha v^2)} \langle u \rangle \langle v |, $$

where $e^{i\theta}$ is an arbitrary phase. If $\beta$ is not relatively prime to $\bar{N}$ we can use the decomposition

$$ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & x \end{pmatrix} \begin{pmatrix} \gamma + x\alpha & \delta + x\beta \\ -\alpha & -\beta \end{pmatrix}, $$

where the integer $x$ can always be chosen so that $\delta + x\beta$ is relatively prime to $\bar{N}$. We remark that in this representation symplectic matrices are represented by unitary phase-permutation matrices if and only if they are of the form

$$ G = \begin{pmatrix} \alpha & 0 \\ \gamma & \alpha^{-1} \end{pmatrix}. $$

They form a rather small subgroup.
Let us return to the more abstract point of view alluded to before. Since phase factors are left invariant by a unitary conjugation

$$U_G(\tau^k 1) U_G^\dagger = \tau^k 1,$$

(18)

the Clifford group acts on $H(N)/Z(N) \simeq \mathbb{Z}_N^2$. It is easy to see that the action of the Clifford group on $H(N)/Z(N)$ is precisely isomorphic to $SL(2,N)$. This equivalence holds irrespective of whether $N$ is even or odd and delivers the converse statement promised above. A proof is given in Appendix A.

Symplectic matrices of order 3 are of special interest. If $N > 3$ it can be shown that a symplectic matrix is of order 3 if and only if its trace equals $-1 \mod N$ [14]. According to a precise form of Zauner’s conjecture a SIC fiducial can always be chosen to be an eigenvector of the unitary $U_Z$ representing the symplectic matrix

$$G_Z = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$  

(19)

In the standard representation $U_Z$ is not given in monomial form (although monomial representations of other symplectic matrices of order 3 can be found for special values of $N$ [14]).

The phase of $U_Z$ is chosen so that $U_Z^3$ is the identity operator. It is then possible, using Gauss sums, to deduce the dimension of the three eigenspaces of a Zauner unitary in arbitrary dimensions [4]. There are three eigenspaces $\mathcal{E}_0, \mathcal{E}_1, \mathcal{E}_2$ corresponding respectively to the eigenvalues 1, $e^{2\pi i/3}$, $e^{4\pi i/3}$. With an appropriate choice of phase one finds for their dimensions that

| $N$   | 1   | $e^{2\pi i/3}$ | $e^{4\pi i/3}$ |
|-------|-----|---------------|---------------|
| $3k$  | $k + 1$ | $k$           | $k - 1$       |
| $3k + 1$ | $k + 1$ | $k$           | $k$           |
| $3k + 2$ | $k + 1$ | $k + 1$      | $k$           |

The numerical evidence [13] strongly suggests that the eigenspace $\mathcal{E}_0$ always contains SIC fiducials, while if $N = 3k$ or $N = 3k + 1$ the other two eigenspaces never do. The case $N = 3k + 2$ does not occur if $N = n^2$.

Finally we will be interested in the extended Clifford group, which includes anti-unitary operators as well [14]. The determinants of the 2 by 2 matrices are then allowed to take the values $\pm 1$. The extended Clifford group
divides the set of all SICs into orbits in a natural way: acting on a given SIC with an element of this group produces another SIC since we assume that the SIC itself is an orbit under the Weyl-Heisenberg group.

3. Representation with phase-permutation matrices

From now on we are in a Hilbert space of dimension $N = n^2$,

$$\mathcal{H}_N = \mathcal{H}_n \otimes \mathcal{H}_n.$$  

We add one more phase factor to the ones we have defined already:

$$\omega = e^{\frac{2\pi i}{N}}, \quad \tau = -e^{\frac{i\pi}{N}}, \quad \sigma = e^{\frac{2\pi i}{n}}.$$  

Our key observation is that

$$ZX = \omega XZ \Rightarrow [X^n, Z^n] = 0.$$  

Hence the Weyl-Heisenberg group admits an Abelian subgroup,

$$S = \langle X^n, Z^n, \tau I \rangle,$$

of maximal order $N\bar{N}$. By diagonalising the elements of $S$, we define a new basis with basis vectors labelled $|r, s\rangle$, where $r$ and $s$ are integers modulo $n$. Indeed

$$X^n|r, s\rangle = \sigma^r|r, s\rangle, \quad Z^n|r, s\rangle = \sigma^s|r, s\rangle.$$  

Some phase choices are still to be made. We settled for a choice which implies that the generators of the group are represented by

$$X|r, s\rangle = \begin{cases} |r, s + 1\rangle & \text{if } s + 1 \neq 0 \mod n \\ \sigma^r|r, 0\rangle & \text{if } s + 1 = 0 \mod n \end{cases}$$  

$$Z|r, s\rangle = \omega^s|r - 1, s\rangle.$$  

We refer to this representation as the phase-permutation representation. It treats the two generators $X$ and $Z$ in an even-handed way, so in a sense we
have gone “half-way” to the Fourier basis. The relation to the standard Weyl basis is given by

$$|r, s\rangle = \frac{1}{\sqrt{n}} \sum_{t=0}^{n-1} \omega^{-nt} |nt + s\rangle .$$

The matrix effecting this transformation is of the form $F_n \otimes 1$, where $F_n$ is the $n$ by $n$ Fourier matrix.

The entire Weyl-Heisenberg group is represented by phase-permutation matrices, but this time more is true. In this representation the entire Clifford group is represented by phase-permutation matrices. The following armchair argument explains why: In all dimensions, the Clifford group permutes the various maximal Abelian subgroups of the Weyl-Heisenberg group. It also preserves the order of any group element. But if $N = n^2$ there is a unique maximal Abelian subgroup whose elements (modulo phases) have orders that are the divisors of $n$; namely the one that defines our basis. Therefore the Clifford group reorders the elements of this Abelian subgroup, and it follows that it reorders the basis vectors while possibly multiplying them with phases.

The permutations involved are easy to deduce. Let $G$ be a general symplectic matrix as given in eq. (12). Using its inverse we observe that

$$U^\dagger_G X^n U_G = U^\dagger_G D_{n0} U_G = D_{\delta n,-\gamma n} = \tau^{-\gamma \delta N} X^{\delta n} Z^{-\gamma n}$$

$$U^\dagger_G Z^n U_G = U^\dagger_G D_{\beta n,\alpha n} U_G = D_{-\beta n,\alpha n} = \tau^{-\alpha \beta N} X^{-\beta n} Z^\alpha n .$$

As usual the case of odd $n$ is simpler, since $\tau^N = 1$ in this case. Let us therefore assume that $n$ is odd to begin with. We see that

$$X^n U_G |r, s\rangle = U_G X^{\delta n} Z^{-\gamma n} |r, s\rangle = \sigma^{\delta r - \gamma s} U_G |r, s\rangle$$

$$Z^n U_G |r, s\rangle = U_G X^{-\beta n} Z^{\alpha n} |r, s\rangle = \sigma^{-\beta r + \alpha s} U_G |r, s\rangle .$$

It follows that $U_G |r, s\rangle$ is a common eigenvector of the diagonal operators $X^n$ and $Z^n$, and indeed that

$$n \text{ odd} \Rightarrow U_G |r, s\rangle = e^{i\theta s} |\delta r - \gamma s, -\beta r + \alpha s\rangle ,$$

9
where $\theta_{rs}$ is a phase to be determined. It again follows that an arbitrary symplectic unitary is represented by a phase-permutation matrix.

The argument can be extended to the even dimensional case, but since we also need to calculate the phases $\theta_{rs}$ we will proceed a little differently in the general case. First we define

$$m = \begin{cases} 
0 & \text{if } n \text{ is odd} \\
\frac{n}{2} & \text{if } n \text{ is even} .
\end{cases}$$

(33)

We may assume that the matrix element $\beta$ is relatively prime to $\bar{N}$, because if it is not we can fall back on the decomposition (16). Using the standard representation (15), and relation (27) between the two bases, it is straightforward to show that

$$\langle r', s' | U_G | r, s \rangle = \frac{e^{i\theta}}{n^2} \tau^{\beta^{-1}(\delta s'^2 - 2ss' + \alpha s^2)} \times$$

$$\times \sum_{t, t'=0}^{n-1} \omega^{n(t(-r + \beta^{-1}(-s' + \alpha s + m\alpha)))} \omega^{n(t'(r' + \beta^{-1}(\delta s' - s + m\delta))} ,$$

where $m$ was defined in eq. (33). Performing the sums, and using the fact that $\alpha\delta - \beta\gamma = 1$ modulo $n$, we see that

$$\langle r', s' | U_G | r, s \rangle = e^{i\theta} \tau^{\beta^{-1}(\delta s'^2 - 2ss' + \alpha s^2)} \Leftrightarrow \begin{cases} 
\begin{array}{l}
r' = \delta r - \gamma s - m\beta^{-1}(1 + \alpha) \\
n't' = -\beta r + \alpha s + m\alpha 
\end{array}
\end{cases}$$

(35)

and zero otherwise. If $n$ is odd then $m = 0$, and we have reproduced eq. (32) but with the phases now included. If $n$ is even we use modulo 2 arithmetic to polish the $m$-dependent term; note that $\beta = 1$ modulo 2 since $\beta$ is relatively prime to $n$. Thus we arrive at our key result:

**Theorem 1:** When the dimension is a square number $N = n^2$, the Clifford group admits a representation by phase-permutation matrices. For the Weyl-Heisenberg subgroup it is given by eqs. (25). For an $SL(2,\bar{N})$ element of the form (12), with $\beta$ and $N$ relatively prime and $m$ and $s'$ as above, it is
\[ U_G |r, s\rangle = e^{i\theta} \beta^{-1}(\delta s^2 - 2ss' + \alpha s^2) \beta |\delta r - \gamma s + m\gamma\delta, -\beta r + \alpha s + m\alpha\beta\rangle. \] (36)

The overall phase \( \theta \) remains undetermined. The case when \( \beta \) is not relatively prime to \( N \) can be recovered from eq. (16).

Note that if \( G = G' \) modulo \( n \) (using modulo \( n \) arithmetic for the matrix elements) then \( U_G \) and \( U_{G'} \) produce the same permutations of the basis elements, that is to say they differ only by a diagonal unitary.

The group element of most interest to us is Zauner’s unitary, corresponding to the matrix (17). It is given explicitly by

\[
U_Z |r, s\rangle = e^{i\pi \frac{r(N-1)}{12}} \tau r^2 + 2rs | -r - s - m, r\rangle. \] (37)

Here the overall phase \( \theta \) was chosen to ensure that \( U_Z^3 \) is the identity operator.

A general element of the extended Clifford group is obtained by replacing \( SL(2, \bar{N}) \) with the group \( ESL(2, \bar{N}) \). The additional matrices \( E \in ESL(2, \bar{N}) \) can be written as a product

\[ E = GJ, \quad G \in SL(2, \bar{N}), \quad J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \] (38)

To the matrix \( J \) there corresponds an anti-unitary operator \( U_J \) whose action on the phase-permutation basis is given by

\[ U_J |r, s\rangle = | -r, s\rangle. \] (39)

Hence, the extended Clifford group also acts through phase-permutation matrices on the basis vectors.

### 4. Uniqueness proofs

We have seen by construction that the Clifford group admits a representation by phase-permutation matrices if the dimension \( N = n^2 \) is a square. We will now prove the converse, that this is possible only in square dimensions. Since the construction hinged on a special maximal Abelian subgroup of the Weyl-Heisenberg group—it transformed into itself under the Clifford group—we
begin with a theorem that shows that this is a necessary feature of any phase-permutation representation. It actually applies to a slightly more general situation, in which we consider a group \( G \) which may be the entire Clifford group, but which may also be any subgroup of the Clifford group which includes the Heisenberg group \( H(N) \) as a subgroup.

An Abelian subgroup \( S \) of \( H(N) \) is called maximal if no element \( g \in H(N) \setminus S \) commutes with everything in \( S \). Equivalently, \( S \) is maximal if it has the maximal possible order \( N\bar{N} \).

**Theorem 2:** The following two statements are equivalent:

1. There exists a phase-permutation representation of \( G \) on \( \mathbb{C}^N \) which is irreducible when restricted to \( H(N) \).

2. There exists a maximal Abelian subgroup of \( H(N) \) which is stabilised by \( G \).

**Proof:** First we establish \( 2 \Rightarrow 1 \). Let \( S \) be a maximal Abelian subgroup of \( H(N) \). Choose a basis in which all elements of \( S \) are simultaneously diagonal. If we select one representative from every coset in \( S/Z(N) \), their diagonals define \( N \) orthogonal vectors (because \( H(N)/Z(N) \) defines a unitary operator basis). From this one concludes that a maximal Abelian subgroup defines a joint eigenbasis which is unique up to permutations and rephasings. It is then obvious that \( 2 \Rightarrow 1 \). This was used in section 3.

To prove that \( 1 \Rightarrow 2 \), denote the phase-permutation basis by \( \{|e_a\rangle\}_{a=1}^N \). By assumption \( H(N) \) simply permutes the corresponding rays (vectors up to phase), and acts transitively on them. Let \( S \) be the subgroup of the Heisenberg group leaving the particular projector \( |e_1\rangle\langle e_1| \) invariant. Since the orbit of \( H(N) \) acting on the set of projectors has size \( N \) we know that \( |H(N)|/|S| = N \), that is to say that

\[
|S| = \frac{|H(N)|}{N} = \frac{N^2\bar{N}}{N} = N\bar{N} ,
\]

where \( \bar{N} \) is the cardinality of the center. Modulo phases, \( S \) must thus be a subgroup of \( H(N) \) of order \( N \). By definition, all elements of \( S \) have the common eigenvector \( |e_1\rangle \). But it is a direct consequence of the commutation relations that two elements of the Heisenberg group have a common eigen-
vector if and only if they commute. Therefore $S$ is an abelian subgroup of $H(N)$ and has order $N\bar{N}$. Hence $S$ is maximally Abelian.

Now $H(N)$ acts monomially on the joint eigenvectors of any maximal abelian subgroup. It also acts transitively, by irreducibility. Thus the orbit of $|e_1\rangle$ under $H(N)$ consists precisely of the joint eigenvectors of $S$ (up to phases). But we showed before that the orbit coincides with $\{|e_a\rangle\}_{a=1}^N$. $\blacksquare$

We now focus on the case where $G$ is the full Clifford group. Are there cases beyond square dimensions where there is a maximally Abelian subgroup $S$ of $H(N)$ stabilized by the Clifford group? By Section 2, the orbit of an element of $H(N)/Z(N)$ under the action of the Clifford group corresponds to the orbit of a vector, $v \in \mathbb{Z}_N^2$, under the action of $SL(2,N)$. The following characterization of these orbits is implied by Lemma 27 of [19]. We re-prove it here to make the presentation self-contained.

Recall that the order of a vector $v \in \mathbb{Z}_N^2$ is the least integer $k \geq 1$ such that $kv \equiv 0$, where the triple bar equality sign denotes equality modulo $N$.

**Lemma 1:** The orbits of the action of $SL(2,N)$ on $\mathbb{Z}_N^2$ are the sets

$$\mathcal{O}_k = \{v \in \mathbb{Z}_N^2 \mid \text{ord } v = k\}$$

of vectors of constant order.

**Proof:** We first prove that $S \in SL(2,N)$ cannot change the order of a vector $v$. Indeed, if $kv \equiv 0$, then

$$k(Sv) \equiv S(kv) \equiv S0 = 0$$

so that $\text{ord } Sv \leq \text{ord } v$. Replacing $S$ by $S^{-1}$, we see that $\text{ord } Sv \geq \text{ord } v$. Hence equality must hold as claimed.

The comparatively difficult part is to show that $SL(2,N)$ acts transitively on the sets $\mathcal{O}_k$. Let $v \in \mathbb{Z}_N^2$ be of order $k$. By definition we thus have that

$$N \mid (kv_i) \Rightarrow \frac{N}{k} \mid v_i,$$

where $v_i, i = 1, 2$ are the components of $v$. Therefore, the vector

$$v' := \frac{1}{N/k} v$$

13
is well-defined as an element of \( \mathbb{Z}_N^2 \). One checks that \( \text{ord} \, v' = N \).

We go on to show that there is a symplectic matrix \( S \in SL(2, N) \) whose first column equals \( v' \). That is the case if there are integers \( x, y \) such that

\[
1 \equiv \det \begin{pmatrix} v'_1 & x \\ v'_2 & y \end{pmatrix} = v'_1 y - v'_2 x. \tag{45}
\]

By Bézout’s identity, there are integers \( a, b \) such that

\[
v'_1 a + v'_2 b = g, \tag{46}
\]

where \( g = \gcd(v'_1, v'_2) \). It must be the case that \( g \) and \( N \) are co-prime, for otherwise \((N/g)\) would be an integer smaller than \( N \) such that \((N/g)v' \equiv 0\), which would contradict the fact that \( \text{ord} \, v' = N \). Thus there exists a multiplicative inverse \( g^{-1} \) of \( g \) modulo \( N \). Hence

\[
y = g^{-1} a, \quad x = -g^{-1} b \tag{47}
\]

provides a solution to (45).

Finally, let \( w \) be another vector of order \( k \). Let \( S_v \) be a symplectic matrix with first column equal to \( v' \), let \( S_w \) be a symplectic matrix with first column equal to \( w' \). Then

\[
S_w S_v^{-1} v' \equiv w' \Rightarrow S_w S_v^{-1} v \equiv w. \tag{48}
\]

Thus any two elements of \( \mathcal{O}_k \) can be mapped onto each other by means of an element of \( SL(2, N) \). \( \Box \)

The preceding lemma allows us to decide in which dimensions there is a monomial representation of the Clifford group just by counting orbit sizes. It seems simpler to do that in prime-power dimensions.

**Lemma 2:** Let \( N = p_1^{q_1} \ldots p_k^{q_k} \) be the decomposition of the dimension into powers of distinct primes.

There is an order-\( N \) subgroup of \( \mathbb{Z}_N^2 \) which is stabilized by \( SL(2, N) \) if and only if the same is true for all dimensions \( N_i = p_i^{q_i} \), for \( i = 1, \ldots, k \).

The statement follows from the more general fact that the Weyl-Heisenberg group and the Clifford group factor into direct products for composite \( N \). It is proven in Appendix B. We are ready to conclude this section:
Theorem 3: There exists a monomial representation of the Clifford group which contains the Weyl-Heisenberg group as an irreducible subgroup if and only if the dimension $N = n^2$ is a square.

Proof: Using the notions of Lemma 2, let $N_i = p_i^{n_i}$. Let $V \subset \mathbb{Z}_{N_i}^2$ be a non-trivial subgroup which is invariant under the action of $SL(2, N)$.

Let $k = \max\{\text{ord } v | v \in V\}$ be the largest order of any element in $V$. By Lagrange’s Theorem, $k$ is of the form $k = p_i^l$ for $0 \leq l \leq q_i$. Because $v \in V \Rightarrow p_i v \in V$, there is also an element of order $p_i^{l-1}$ in $V$, and, indeed, any power of $p_i$ up to the $l$th appears as the order of some element in $V$.

By Lemma 1 and the assumption that $V$ be $SL$-invariant, we find that

$$V = \left\{ v \in \mathbb{Z}_{N_i}^2 | \text{ord } v \leq p_i^l \right\} = p_i^{q_i - l} \mathbb{Z}_{N_i}^2.$$  \hspace{1cm} (49)

Hence $|V| = p_i^{2l}$, which is equal to $N_i$ if and only if $l = q_i/2$. That is possible if and only if $q_i$ is even, which implies the claim. \(\square\)

In the remaining sections we turn our attention to applications of the phase-permutation basis. We return to our original motivation of SICs. First we discuss a general property of SICs on the phase-permutation basis, and then in sections 6 and 7 we use this basis to construct SICs in dimensions $2^2$, $3^2$, and $4^2$. The sixteen dimensional case has so far not been solved in the Weyl basis. Finally, in section 8 we consider sets of Mutually Unbiased Bases (MUB) in the phase-permutation basis.

5. Images of SICs in the probability simplex

For the first application, recall that a quantum state together with an orthonormal basis gives rise to a probability vector, with the basis vectors themselves forming a simplex. In physics this is connected to quantum measurements, in mathematics it is an example of the moment map. Anyway, if the quantum state is a pure state represented by the Hilbert space vector

$$(z_0, z_1, \ldots, z_{N-1})^T = (\sqrt{p_0}, \sqrt{p_1}e^{i\mu_1}, \ldots, \sqrt{p_{N-1}}e^{i\mu_{N-1}})^T,$$  \hspace{1cm} (50)

then its image with respect to the same orthonormal basis is a probability vector with components $p_i$. The probability vector gives the barycentric coordinates of a point within the probability simplex associated to the basis.
chosen. We assumed that the vector is a unit vector, which indeed implies that

\[ \sum_{i=0}^{N-1} p_i = 1. \]  \hspace{1cm} (51)

If we have a set of such pure states connected by a group which is represented by phase permutation matrices, then their probability vectors will be related by permutations of the coordinate axes. It follows that they lie on a sphere centered around the midpoint of the probability simplex.

More can be said if we deal with the \( N^2 \) unit vectors forming an orbit under the Weyl-Heisenberg group and obeying the SIC condition. Let the components of a SIC fiducial vector be given by eq. (50). In the standard basis, where the subgroup generated by \( Z \) is diagonalised, it is known that [20, 21]

\[ \sum_{i=0}^{N-1} p_i p_{i+x} = \begin{cases} \frac{2}{N+1} & \text{if } x = 0 \\ \frac{1}{N+1} & \text{if } x \neq 0 \mod N \end{cases} \]  \hspace{1cm} (52)

The length of the probability vector, that is the radius of the sphere in which it is inscribed, is thereby determined. The remaining equations also admit an interesting geometrical interpretation [22]. Since the matrix representing \( Z \) is diagonal, the \( N \) states \( Z^r |\psi_F\rangle \) all project to the same probability vector. Moreover the \( i \)th component of the vector \( X^x |\psi_F\rangle \) is \( p_{i-x} \), so from these equations we can read off not only the length of the probability vectors but also their mutual angles. The conclusion turns out to be that the image of the \( N^2 \) SIC vectors is itself a regular simplex with \( N \) vertices. Once this geometrical interpretation is available it is unsurprising that the \( N \) equations (52) are redundant and do not by themselves determine all the coefficients \( p_i \) (unless \( N = 2 \)). But they are still helpful.

The reason why the \( N^2 \) vectors in the SIC give rise to only \( N \) images in the projection is that the images form an orbit under the subgroup that is complementary to the diagonalised subgroup. It is clear that something similar should happen in the phase-permutation basis, where again there is an Abelian subgroup of order \( N \) that does not move the projected points. To show this we denote the components of the SIC fiducial \( |\psi_F\rangle \) by \( z_{rs} = \sqrt{p_{rs} e^{i \mu_{rs}}} \), and find

16
\[ \langle \psi_0 | X^{nu} Z^{nv} | \psi_0 \rangle = \sum_{r,s=0}^{n-1} p_{rs} \sigma^{ru+sv} \]

\[ \Rightarrow |\langle \psi_0 | X^{nu} Z^{nv} | \psi_0 \rangle|^2 = \sum_{r,s=0}^{n-1} \sum_{r',s'=0}^{n-1} p_{rs} p_{r's'} \sigma^{(r-r')u+(s-s')v} . \] (53)

The absolute values on the left hand side are known from the condition defining a SIC. Using this, and summing over the integers \( u \) and \( v \), we find

\[ \sum_{r,s=0}^{n-1} p_{rs}^2 = \frac{1}{N} \left( 1 + \frac{N - 1}{N + 1} \right) = \frac{2}{N + 1} . \] (54)

More generally we can take a Fourier transform of eq. (53). This gives \( N - 1 \) additional equations for the absolute values,

\[ \sum_{r,s=0}^{n-1} p_{rs} p_{r+x,s+y} = \frac{1}{N + 1} . \] (55)

Here \( x, y \) are integers modulo \( n \), not both zero. This is analogous to what happens in the standard basis, and the geometrical interpretation is the same: when the SIC is projected to the basis simplex we see a regular simplex centered at the origin with just \( N \) vertices. Its orientation differs from the projection to the standard basis (see Fig 1).

6. SIC fiducials for \( N = 2^2 \) and \( 3^2 \)

If we use the phase-permutation representation it becomes very easy to find the SICs in \( N = 2^2 \) dimensions. In fact the absolute values entering the fiducial are determined by Zauner’s conjecture, normalisation, and eq. (54). Alternatively one can simply solve the equations defining a Weyl-Heisenberg covariant SIC. Before doing so it is convenient to rephase the basis through

\[ (|0, 0\rangle, |0, 1\rangle, |1, 0\rangle, |1, 1\rangle) \rightarrow (\tau^{-2}|0, 0\rangle, \tau^{-7}|0, 1\rangle, \tau^{-5}|1, 0\rangle, |1, 1\rangle) . \] (56)
Figure 1: The images of an $N = 4$ SIC, in the two bases we discuss. The phase-permutation basis (the large tetrahedron on the right) is aligned to the SIC (the small tetrahedron) in a way that the standard basis (the large tetrahedron on the left) is not. The corresponding pictures for $N = 9$ (not shown) are eight dimensional, and would show that the faces of the eigenvalue simplex for the phase-permutation basis are nicely aligned with the image of the SIC.

This gives the representation

$$X = \tau \begin{pmatrix} 0 & i & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & i & 0 \end{pmatrix}, \quad Z = \tau \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ i & 0 & 0 & 0 \\ 0 & i & 0 & 0 \end{pmatrix}. \quad (57)$$

There are altogether $4^4 = 256$ possible solutions for a SIC fiducial, giving rise to 16 SICs altogether. The solutions are

$$\begin{pmatrix} x \\ i^{s_1} \\ i^{t_1} \\ i^{u_1} \end{pmatrix}, \quad \begin{pmatrix} i^{s_2} \\ x \\ i^{t_2} \\ i^{u_2} \end{pmatrix}, \quad \begin{pmatrix} i^{s_3} \\ i^{t_3} \\ x \\ i^{u_3} \end{pmatrix}, \quad \begin{pmatrix} i^{s_4} \\ i^{t_4} \\ i^{u_4} \\ x \end{pmatrix}, \quad (58)$$

where $s_i, t_i, u_i$ are integers from 0 to 3,

$$x = \sqrt{2 + \sqrt{5}}, \quad (59)$$

and an overall normalisation has been ignored. This simple form of the SIC vectors has been found before by Zauner [23], who arrived at it by casting
the Zauner unitary into phase-permutation form, and from an alternative point of view by Belovs [24]. Each of the vectors is left invariant by a Zauner unitary of order 3, and the 16 SICs form a single orbit under the Clifford group. The result of the numerical searches [5, 13] is thus fully confirmed. The images in the probability simplex (see section 5, and Fig. 1) coincide for all the SICs, and they are nicely oriented. The structure of the \( N = 4 \) SICs, and their entanglement properties, were studied in detail recently [25].

The case of \( N = 3^2 \) is much harder. Lest our readers be disappointed by this, we strongly recommend they begin by looking at the answer found—by means of a Magma calculation—in the standard representation [13, 18]. Afterwards our result will come as a pleasant surprise.

With our canonical choice of \( U_Z \), Zauner’s conjecture implies that the SIC fiducial takes the special form

\[
|\psi\rangle = -z_1 \omega^7 |1, 1\rangle - z_2 \omega |2, 2\rangle +
\]

\[
+ z_3 (\omega^6 |0, 2\rangle + |1, 0\rangle + \omega^8 |2, 1\rangle) + z_4 (\omega^6 |0, 1\rangle + |2, 0\rangle + \omega^5 |1, 2\rangle) .
\]

We included some convenient phase factors. We exploit the arbitrariness in the overall phase to write the \( z_j \) in the form

\[
z_1 = \sqrt{p_1} e^{i\mu_0} \quad z_2 = \sqrt{p_2} e^{-i\mu_0} \quad z_3 = \sqrt{p_3} e^{i\mu_3} \quad z_4 = \sqrt{p_4} e^{i\mu_4}
\]

where it is assumed that \(-\pi/2 < \mu_0 \leq \pi/2\).

The necessary and sufficient condition for a normalized vector \( |\psi\rangle \) to be a fiducial vector is that

\[
|\langle \psi|D_{jk}|\psi\rangle|^2 = \frac{1}{10}
\]

for all \( j, k \) not both zero—a total of 80 equations. However the Zauner symmetry means that if eq. (62) is satisfied for the vector \((j, k)\) it is automatically satisfied for the \((\text{up to} \) two other vectors obtained by acting with the Zauner matrix. Also, if it is satisfied for \((j, k)\) it is automatically satisfied for \((-j, -k)\). Consequently we can reduce the 80 equations to 15, which it will be convenient to group as follows
1. 2 group 1 equations

\[ |\langle \psi | D_{0,3} | \psi \rangle|^2 = |\langle \psi | D_{3,6} | \psi \rangle|^2 = \frac{1}{10} \]  \hspace{1cm} (63)

Assuming normalization these equations are equivalent to eqs. (55).

2. 3 group 2 equations

\[ |\langle \psi | D_{3j+1,6j+2} | \psi \rangle|^2 = \frac{1}{10} \] \hspace{1cm} (64)

with \( j = 0, 1, 2 \).

3. 9 group 3 equations

\[ |\langle \psi | D_{3j,6j+3k+1} | \psi \rangle|^2 = \frac{1}{10} \] \hspace{1cm} (65)

with \( j, k = 0, 1, 2 \).

Together with normalization this gives us 16 conditions on the 7 real parameters in eq. (61), so there is still a high degree of redundancy in the equations. The nature of the dependencies will become clear in the course of solving them.

We begin by considering the normalization condition and group 1 equations. As can be seen from eqs. (54) and (55) (which are equivalent to them) they only involve the absolute values. Explicitly:

\[ p_1 + p_2 + 3p_3 + 3p_4 = 1 \]
\[ p_1^2 + p_2^2 - p_1p_2 = \frac{1}{10} \] \hspace{1cm} (66)
\[ 3p_3^2 + 3p_4^2 + 3p_3p_4 - p_3 - p_4 = -\frac{1}{10} \]

These equations are not hard to solve. Setting

\[ p_1 = a_1 + b_1 , \quad p_2 = a_1 - b_1 , \quad p_3 = a_3 + b_3 , \quad p_4 = a_3 - b_3 \] \hspace{1cm} (67)

diagonalizes them. It is then readily deduced
\[ a_3 = \frac{1}{6}(1-2a_1), \quad b_1^2 = \frac{1}{30}(1-10a_1^2), \quad b_3^2 = \frac{1}{180}(-1+20a_1-60a_1^2). \quad (68) \]

To fix the free parameter in the expressions just derived we need to consider the group 2 equations. This will also give us the phase \( e^{i\mu_0} \). It is convenient to write the equations in the form

\[ \sum_{r,s=0}^2 \sigma^{i(r-s)} e_r e^*_s = \frac{1}{10} \quad (69) \]

with \( j = 0, 1, 2 \) and where

\[ e_0 = z_1 z_2^* , \quad e_1 = i\sqrt{3}\omega^2 p_3 , \quad e_2 = -i\sqrt{3}\omega^7 p_4 . \quad (70) \]

Inverting the Fourier transform we see that eqs. (69) are equivalent to the 2 conditions

\[ |e_0|^2 + |e_1|^2 + |e_2|^2 = \frac{1}{10} \quad (71) \]

\[ e_0 e_1^* + e_1 e_2^* + e_2 e_0^* = 0 \]

The first of these is a consequence of the group 1 equations. Solving the second for \( e_0 = z_1 z_2^* \) gives

\[ z_1 z_2^* = \frac{e_2^3 e_1^* - e_1^2 e_2^*}{|e_1|^2 - |e_2|^2} = \frac{\sqrt{3}(a_3^2 - b_3^2)(\sqrt{3}b_3 - ia_3)}{4a_3 b_3} . \quad (72) \]

Taking the square of the absolute value on both sides and using eqs. (68) we find

\[ (1 - 40a_1 + 40a_1^2)(-11 + 100a_1 - 120a_1^2 - 800a_1^3 + 1600a_1^4) = 0 . \quad (73) \]

Solving this equation and taking account of the requirement that \( b_1, b_3 \) both be real we deduce
\[ a_1 = \frac{1}{40} \left( 5 - s_05\sqrt{3} + s_03\sqrt{5} + \sqrt{15} \right) \]

\[ b_1 = \frac{s_2}{60} \sqrt{15 \left( \sqrt{15} + s_0\sqrt{3} \right)} \]

\[ a_3 = \frac{1}{120} \left( 15 + s_05\sqrt{3} - s_03\sqrt{5} - \sqrt{15} \right) \]

\[ b_3 = \frac{s_1}{60} \sqrt{5 \left( -18 - s_07\sqrt{3} + s_06\sqrt{5} + 5\sqrt{15} \right)} \]

where \( s_0, s_1 \) and \( s_2 \) are arbitrary signs. This fixes the absolute values. Note that the only choice of sign that affects the set of absolute values is \( s_0 \), which suggests—correctly—that \( s_0 \) labels two different orbits of the Clifford group.

To determine the phase \( e^{i\mu_0} \), we substitute these expressions into eq. (72) and simplify. We obtain

\[ e^{2i\mu_0} = \frac{1}{4} \sqrt{2 \left( 6 + s_0\sqrt{3} - \sqrt{15} \right)} - \frac{i s_1}{4} \sqrt{2 \left( 2 - s_0\sqrt{3} + \sqrt{15} \right)} \]

Taking account of the assumption that \(-\pi/2 < \mu_0 \leq \pi/2\) we deduce

\[ e^{i\mu_0} = \sqrt{\frac{1}{2} + c_0} - is_1 \sqrt{\frac{1}{2} - c_0} \]

where

\[ c_0 = \frac{1}{8} \sqrt{2(6 + s_0\sqrt{3} - \sqrt{15})} \]

Note that the numbers given in these expressions as nested square roots can be constructed with ruler and compass, so the ancient Greeks might have approved—especially since the 9th root of unity cannot be so constructed.

To calculate the remaining two phases we turn to the group 3 equations. It is convenient to write the equations in the form

\[ \sum_{r,s=0}^{2} \sigma^{j(r-s)} e_{kr} e^*_{ks} = \frac{1}{10} \]
with \( j, k = 0, 1, 2 \) and where

\[
e_{k0} = \left(1 + 2(-1)^k \cos \left(\frac{(3k+2)\pi}{9}\right)\right) z_3^* z_4
\]

\[
e_{k1} = -\left(\tau^{6k-5} z_1^* + \tau^{-(6k-5)} z_2^*\right) z_3
\]

\[
e_{k2} = -\left(\tau^{6k-5} z_1 + \tau^{-(6k-5)} z_2\right) z_4^*.
\]

Inverting the Fourier transform in eqs. (78) we see that the nine group 3 equations are actually equivalent to the six equations

\[
|e_{k0}|^2 + |e_{k1}|^2 + |e_{k2}|^2 = \frac{1}{10} \tag{79}
\]

\[
e_{k0}e_{k1}^* + e_{k1}e_{k2}^* + e_{k2}e_{k0}^* = 0 \tag{80}
\]

with \( k = 0, 1, 2 \). Using eq. (72) and some elementary trigonometry one finds that for all three values of \( k \) eq. (79) is equivalent to the single condition

\[
3(a_3^2 - b_3^2) + 4a_1a_3 = \frac{1}{10} \tag{81}
\]

which is an immediate consequence of the group 1 equations. We are thus left with the three eqs. (80). It will be convenient to write them in the form

\[
f_1 = f_2 = f_3 = 0 \tag{82}
\]

where

\[
f_j = \sum_{k=0}^{2} \sigma^{jk} (e_{k0}e_{k1}^* + e_{k1}e_{k2}^* + e_{k2}e_{k0}^*). \tag{83}
\]

Writing the expressions out in full we find that \( f_2 = \tau^2 f_1 \). So the nine equations with which we started reduce to just the two equations \( f_0 = f_1 = 0 \). It is readily confirmed that these are equivalent to
The quantities on the right hand sides are all known so these formulae give explicit expressions for the two remaining phases. Simplifying them and taking the cube roots we find

\[ e^{3i\mu_3} = -\frac{1}{2\sqrt{3}} \left( \frac{z_1^2 + z_1z_2 + z_2^2}{z_1^* + z_2^*} + \frac{i(z_1^2 - z_1z_2 - z_2^2)}{\sqrt{3}(z_1^* - z_2^*)} \right) \]  
\[ e^{3i\mu_4} = -\frac{1}{2\sqrt{4}} \left( \frac{z_1^2 + z_1z_2 + z_2^2}{z_1^* + z_2^*} - \frac{i(z_1^2 - z_1z_2 - z_2^2)}{\sqrt{3}(z_1^* - z_2^*)} \right) \]  

The quantities on the right hand sides are all known so these formulae give explicit expressions for the two remaining phases. Simplifying them and taking the cube roots we find

\[ e^{i\mu_3} = \sigma^{m_3} \left( -\sqrt{\frac{1}{2} - c_1 + c_2 + is_1s_2 \sqrt{\frac{1}{2} + c_1 - c_2}} \right)^{\frac{1}{3}} \]  
\[ e^{i\mu_4} = \sigma^{m_4} \left( -\sqrt{\frac{1}{2} - c_1 - c_2 + is_1s_2 \sqrt{\frac{1}{2} + c_1 + c_2}} \right)^{\frac{1}{3}} \]  

where

\[ c_1 = \frac{s_0}{8} \sqrt{9 - s_04\sqrt{3} + s_03\sqrt{5} - 2\sqrt{15}} \]  
\[ c_2 = \frac{s_1s_0}{24} \sqrt{15(-19 + s_012\sqrt{3} - s_09\sqrt{5} + 6\sqrt{15})} . \]

Here \( m_3 \) and \( m_4 \) can take the values 0, 1, 2. The entire solution is given in terms of radicals, as expected (but not understood!).

Altogether there are \( 2^3 \cdot 3^2 = 72 \) fiducial vectors, splitting into 2 different orbits of the extended Clifford group labelled by \( s_0 = \pm 1 \). The solution with \( s_0 = s_1 = s_2 = m_3 = m_4 = 1 \) is the fiducial 9a as labelled by Scott and Grassl [13], while switching the sign of (only) \( s_0 \) leads to their fiducial 9b.
Figure 2: A change of basis for dimension $N = 16$ resulting in a Zauner matrix which is a permutation, where $\tau = -\exp(\pi i/16)$.

7. SIC fiducials for $N = 4^2$

The first dimension for which the approach helped in finding a new solution is $N = 16 = 4^2$. We were unable to obtain a solution by hand as we did for $N = 9$. However, we were able to obtain a solution using Magma.

We use a basis such that both $X^4$ and $Z^4$ are diagonal. The change of basis is given by the matrix $T$ in Figure 2, and the Weyl-Heisenberg group in this basis are shown in Figure 3.

In this basis, the Zauner matrix is a permutation matrix. Hence a fiducial vector is of the form

$$|\psi\rangle = x_0(|0\rangle + |2\rangle + |6\rangle) + x_1(|1\rangle + |9\rangle + |10\rangle) + x_3(|3\rangle + |14\rangle + |15\rangle)$$

$$+ x_4|4\rangle + x_5(|5\rangle + |11\rangle + |12\rangle) + x_7(|7\rangle + |8\rangle + |13\rangle).$$

In order to solve the equations for these six complex variables $x_i$, one of which can assumed to be real, we followed the approach described in [18]. Computing a Gröbner basis modulo a single 23-bit prime using Magma [26] took
**Figure 3:** Generators $X$ and $Z$ of the Weyl-Heisenberg group in dimension $N = 4^2$ in the adapted basis. Here $\tau = -\exp(\pi i/16)$ denotes a primitive 32nd root of unity.
about three days and required about 30 GB of memory. The polynomials in
a Gröbner basis with respect to so-called grevlex order have coefficients with
90 digits in the numerators and denominators. Changing to lexicographic
order which is used to solve the equations, the coefficients grow to some 900
digits. Nonetheless, we succeed to obtain a less complex representation of a
solution. The solutions are given in a number field
\[ K = \mathbb{Q}(\sqrt{2}, \sqrt{13}, \sqrt{17}, r_2, r_3, t_1, t_2, t_3, t_4, \sqrt{-1}), \]  
(88)
of degree 1024, where

\[ r_2 = \sqrt{221} - 11, \quad r_3 = \sqrt{15 + 17}, \]

\[ t_1 = \sqrt{15 + (4 - \sqrt{17})r_3 - 3\sqrt{17}}, \]

\[ t_2^2 = ((3 - 5\sqrt{17})\sqrt{13} + (39\sqrt{17} - 65))r_3 + ((16\sqrt{17} - 72)\sqrt{13} + 936))t_1 - 208\sqrt{13} + 2288, \]

\[ t_3 = \sqrt{2 - \sqrt{2}}, \quad t_4 = \sqrt{2 + t_3}. \]

Note that we do not explicitly use a 32nd root of unity, it can be expressed
as
\[ \omega_{32} = \frac{1}{2}((\sqrt{2}(1 - t_3) - 1)t_4 - t_4\sqrt{-1}). \]
(90)
The Galois group of \( K \) is isomorphic to \( C_8 \times ((C_2 \times C_2 \times C_{16}) \rtimes C_2) \), and \( K \) is an Abelian extension of \( \mathbb{Q}(\sqrt{221}) \). The coefficients of a non-normalized fiducial vector of eq. (87) are as follows:

\[ x_0 = -\frac{40}{13}\sqrt{13}r_3t_1t_2 \]
(91)

\[ x_1 = \left( (21\sqrt{2} + 22\sqrt{13} + 16\sqrt{17} + 5\sqrt{26} + 5\sqrt{34} + 4\sqrt{221} + \sqrt{442} + 74)r_2r_3 \\
+ (-77\sqrt{2} - 26\sqrt{13} - 18\sqrt{17} - 33\sqrt{26} - 19\sqrt{34} + 2\sqrt{221} - 7\sqrt{442} + 42)r_2 \\
+ (-45\sqrt{2} + 30\sqrt{13} - 10\sqrt{17} + 15\sqrt{26} + 5\sqrt{34} + 10\sqrt{221} + 5\sqrt{442} - 30)r_3 \\
+ (30\sqrt{13} + 30\sqrt{17} + 10\sqrt{221} - 70)t_1t_4 \\
+ ((3\sqrt{2} + 3\sqrt{13} + 9\sqrt{17} - \sqrt{26} + 7\sqrt{34} + 11\sqrt{221} + 3\sqrt{442} + 121)r_2r_3 \\
+ (-82\sqrt{2} - 88\sqrt{13} - 24\sqrt{17} - 74\sqrt{26} - 2\sqrt{34} + 24\sqrt{221} - 2\sqrt{442} + 264)r_2 \\
+ (175\sqrt{2} + 80\sqrt{13} - 20\sqrt{17} + 75\sqrt{26} - 25\sqrt{34} - 5\sqrt{442} + 380)r_3 \\
+ (200\sqrt{2} + 220\sqrt{13} - 300\sqrt{17} + 160\sqrt{26} - 160\sqrt{34} - 20\sqrt{221} - 40\sqrt{442} + 180))t_4 \right) \sqrt{-1} \]
(92)
\[
x_3 = \left( \left( 34 + 442 + 380 \right) t_4 \right) \sqrt{-1} + \left( 10\sqrt{2} + 15\sqrt{13} + 15\sqrt{17} + 6\sqrt{26} + 8\sqrt{34} + \sqrt{221} + 21 \right) r_2 r_3 (93) \\
+ (-5\sqrt{2} + 16\sqrt{13} + 28\sqrt{17} - 7\sqrt{26} - 21\sqrt{34} - 8\sqrt{221} - 5\sqrt{442} - 108) r_2 \\
+ (70\sqrt{2} + 10\sqrt{26} + 80) r_3 \\
- 10\sqrt{2} - 130\sqrt{13} - 250\sqrt{17} - 70\sqrt{26} - 70\sqrt{34} - 30\sqrt{221} - 10\sqrt{442} - 630) t_1 t_4 \\
+ (10\sqrt{2} + 51\sqrt{13} + 33\sqrt{17} - 24\sqrt{26} - 22\sqrt{34} + 2\sqrt{221} + 29) r_2 r_3 \\
+ (-32\sqrt{2} + 4\sqrt{13} - 28\sqrt{17} - 8\sqrt{26} - 4\sqrt{34} - 44\sqrt{221} - 20\sqrt{442} - 524) r_2 \\
+ (265\sqrt{2} - 30\sqrt{13} - 35\sqrt{17} - 15\sqrt{26} - 35\sqrt{34} + 10\sqrt{221} + 5\sqrt{442} + 310) r_3 \\
+ (260\sqrt{2} - 200\sqrt{13} - 560\sqrt{17} - 100\sqrt{26} - 260\sqrt{34} + 20\sqrt{442} - 600)) t_4 \right) \sqrt{-1} \\
\]

\[
x_4 = \left( \left( \frac{11}{26} \sqrt{13} - \frac{1}{2} \sqrt{17} - \frac{3}{26} \sqrt{221} - \frac{1}{2} \right) r_2 r_3 \\
+ (10\sqrt{2} + \frac{20}{13} \sqrt{26} + \frac{10}{13} \sqrt{442}) r_2 t_2 \sqrt{-1} \right) (94) \\
+ \left( \left( \frac{11}{26} \sqrt{13} + \frac{1}{2} \sqrt{17} + \frac{3}{26} \sqrt{221} + \frac{1}{2} \right) r_2 r_3 \\
+ (10\sqrt{2} + \frac{20}{13} \sqrt{26} + \frac{10}{13} \sqrt{442}) r_2 t_1 t_2 \right) \right) \sqrt{-1} \\
\]
\[ x_5 = \left( \left( -\frac{75}{2} \sqrt{2} - 4\sqrt{13} - 2\sqrt{17} - \frac{25}{2} \sqrt{26} - \frac{15}{2} \sqrt{34} - \frac{5}{2} \sqrt{442} + 10 \right) r_2 r_3 \\
+ \left( -\frac{22}{2} - 24\sqrt{13} - 12\sqrt{17} + 14\sqrt{26} + 2\sqrt{34} - 4\sqrt{221} - 2\sqrt{442} - 24 \right) r_2 \\
+ (15\sqrt{2} - 5\sqrt{13} - 5\sqrt{17} + 25\sqrt{26} - 5\sqrt{34} - 5\sqrt{221} + 5\sqrt{442} + 35) r_3 \\
+ (270\sqrt{2} + 60\sqrt{13} + 180\sqrt{17} + 10\sqrt{26} + 70\sqrt{34} + 20\sqrt{221} + 10\sqrt{442} + 620) t_1 \\
+ ((-85\sqrt{2} - 28\sqrt{13} - 4\sqrt{17} - 3\sqrt{26} + \sqrt{34} + 4\sqrt{221} - 5\sqrt{442} - 36) r_2 r_3 \\
+ (-190\sqrt{2} - 86\sqrt{13} + 22\sqrt{17} + 34\sqrt{26} + 22\sqrt{34} + 22\sqrt{221} - 10\sqrt{442} + 122) r_2 \\
+ (300\sqrt{2} - 60\sqrt{13} + 40\sqrt{17} + 40\sqrt{26} - 20\sqrt{34} - 220) r_3 \\
+ (650\sqrt{2} - 60\sqrt{13} + 460\sqrt{17} + 110\sqrt{26} - 130\sqrt{34} + 60\sqrt{221} + 10\sqrt{442} + 660)) \right)^{\frac{1}{2}} \\
+ ((\frac{1}{2} \sqrt{2} + 23\sqrt{13} + 19\sqrt{17} - \frac{3}{2} \sqrt{26} - \frac{9}{2} \sqrt{34} + 3\sqrt{221} + \frac{1}{2} \sqrt{442} + 63) r_2 r_3) (95) \\
+ (152\sqrt{2} - 20\sqrt{17} + 28\sqrt{26} + 24\sqrt{34} + 4\sqrt{221} + 12\sqrt{442} + 64) r_2 \\
+ (-70\sqrt{2} - 5\sqrt{13} + 15\sqrt{17} + 10\sqrt{34} - 5\sqrt{221} + 55) r_3 \\
+ (350\sqrt{2} - 100\sqrt{13} - 100\sqrt{17} + 50\sqrt{26} + 110\sqrt{34} - 20\sqrt{221} + 10\sqrt{442} + 60)) t_1 \\
+ ((-43\sqrt{2} - 28\sqrt{13} + 24\sqrt{17} - 23\sqrt{26} - 19\sqrt{34} + 8\sqrt{221} + 3\sqrt{442} + 108) r_2 r_3 \\
+ (476\sqrt{2} - 22\sqrt{13} - 26\sqrt{17} + 28\sqrt{26} + 4\sqrt{34} + 6\sqrt{221} + 36\sqrt{442} + 26) r_2 \\
+ (-170\sqrt{2} - 20\sqrt{13} - 40\sqrt{17} + 50\sqrt{26} + 10\sqrt{34} - 10\sqrt{442} + 60) r_3 \\
+ 410\sqrt{2} - 160\sqrt{13} - 120\sqrt{17} + 150\sqrt{26} + 270\sqrt{34} - 30\sqrt{442} + 280 \\
\right) \left( \left( -\frac{1}{2} \sqrt{2} - 23\sqrt{13} + 19\sqrt{17} + \frac{3}{2} \sqrt{26} + \frac{9}{2} \sqrt{34} - 3\sqrt{221} - \frac{1}{2} \sqrt{442} - 63 \right) r_2 r_3 \\
+ (-152\sqrt{2} + 20\sqrt{17} - 28\sqrt{26} - 24\sqrt{34} - 4\sqrt{221} - 12\sqrt{442} - 64) r_2 \\
+ (-70\sqrt{2} - 5\sqrt{13} + 15\sqrt{17} + 10\sqrt{34} - 5\sqrt{221} + 55) r_3 \\
+ (350\sqrt{2} - 100\sqrt{13} - 100\sqrt{17} + 50\sqrt{26} + 110\sqrt{34} - 20\sqrt{221} + 10\sqrt{442} + 60)) t_1 \\
+ ((-43\sqrt{2} - 28\sqrt{13} + 24\sqrt{17} - 23\sqrt{26} - 19\sqrt{34} + 8\sqrt{221} + 3\sqrt{442} - 108) r_2 r_3 \\
+ (-476\sqrt{2} + 22\sqrt{13} + 26\sqrt{17} - 28\sqrt{26} - 4\sqrt{34} - 6\sqrt{221} - 36\sqrt{442} + 26) r_2 \left( 96 \right) \\
+ (-170\sqrt{2} - 20\sqrt{13} - 40\sqrt{17} + 50\sqrt{26} + 10\sqrt{34} - 10\sqrt{442} + 60) r_3 \\
+ (410\sqrt{2} - 160\sqrt{13} - 120\sqrt{17} + 150\sqrt{26} + 270\sqrt{34} - 30\sqrt{442} + 280)) \right)^{\frac{1}{2}} \\
+ (\left( -\frac{75}{2} \sqrt{2} - 4\sqrt{13} - 2\sqrt{17} - \frac{25}{2} \sqrt{26} - \frac{15}{2} \sqrt{34} - \frac{5}{2} \sqrt{442} + 10 \right) r_2 r_3 \\
+ (-22\sqrt{2} - 24\sqrt{13} - 12\sqrt{17} + 14\sqrt{26} + 2\sqrt{34} - 4\sqrt{221} - 2\sqrt{442} - 24) r_2 \\
+ (-15\sqrt{2} + 5\sqrt{13} + 5\sqrt{17} - 25\sqrt{26} + 5\sqrt{34} + 5\sqrt{221} - 5\sqrt{442} - 35) r_3 \\
+ (-270\sqrt{2} - 60\sqrt{13} - 180\sqrt{17} - 10\sqrt{26} - 70\sqrt{34} - 20\sqrt{221} - 10\sqrt{442} - 620) t_1 \\
+ (-85\sqrt{2} - 28\sqrt{13} - 4\sqrt{17} - 3\sqrt{26} + \sqrt{34} + 4\sqrt{221} - 5\sqrt{442} - 36) r_2 r_3 \\
\right)^{\frac{1}{2}}
Fiducial vectors for SICs with respect to the standard representation of the Weyl-Heisenberg group are given in Appendix C. It turns out that the two numerical solutions with orbits labelled 16\(a\) and 16\(b\) in [13] are related by the Galois automorphism of \(\mathbb{K}\) induced by simultaneously changing the signs of \(\sqrt{13}\) and \(\sqrt{17}\).

8. A remark on Mutually Unbiased Bases

Although our main emphasis has been on SICs, we note that square dimensions are special also in the Mutually Unbiased Bases (MUB) problem. In dimensions \(N = n^2\), Wocjan and Beth have shown that one can construct sets of Mutually Unbiased Bases using \(n\) by \(n\) Latin squares [27]. In this section, we examine a variant of the MUB problem making use of the phase-permutation basis.

We would like to find all vectors, and all bases, unbiased with respect to the two eigenbases defined by two complementary cyclic subgroups of the Weyl-Heisenberg group. This problem has been studied in connection with the MUB existence problem in dimension six [28] and in another guise is also known as the cyclic \(N\)-roots problem [29]. The two bases can be taken to be the standard basis \(|u\rangle_0\), the eigenbasis of the subgroup generated by \(Z\), and the Fourier basis \(|u\rangle_\infty\), which is the eigenbasis of the subgroup generated by \(X\). (The labels 0 and \(\infty\) do have a logical explanation [21].) We are looking for all vectors \(|\psi\rangle\) such that

\[
|\langle \psi | u \rangle_0|^2 = |\langle \psi | u \rangle_\infty|^2 = \frac{1}{N},
\]

for all \(N\) values of \(u\). The answer is known for \(N \leq 9\), and it is also known that such vectors always belong to a complete basis unbiased with respect to the two bases we start out with. Here we just want to report what this problem looks like when \(N = n^2\) and the phase-permutation basis is used.
The two eigenbases are now given by

\[ |a + nb\rangle_0 = \frac{1}{\sqrt{n}} \sum_{r=0}^{n-1} \sigma^{-br} |r, a\rangle, \quad Z|a + nb\rangle_0 = \omega^{a + nb} |a + nb\rangle_0 \] \hspace{1cm} (98)

\[ |a + nb\rangle_\infty = \frac{1}{\sqrt{n}} \sum_{r=0}^{n-1} \sigma^{-br} \omega^{-ar} |a, r\rangle, \quad X|a + nb\rangle_\infty = \omega^{a + nb} |a + nb\rangle_\infty \] \hspace{1cm} (99)

We look for bases unbiased with respect to this pair, of the form

\[ |a + nb\rangle_k = \frac{1}{\sqrt{n}} \sum_{r=0}^{n-1} \omega_k(r, a, b) |r, \lambda_k(r, a)\rangle \] \hspace{1cm} (100)

Here \( \omega_k(r, a, b) \) is a phase factor, and \( \lambda_k \) is a map from \( \mathbb{Z}_n \times \mathbb{Z}_n \) to \( \mathbb{Z}_n \), where \( \mathbb{Z}_n \) is the set of integers modulo \( n \).

Unbiasedness with respect to the standard basis holds if and only if the function \( \lambda_k(r, a) \) is injective for fixed \( a \). To see this, we argue by contradiction. Suppose \( \lambda_k(r, a) \) is not injective for some fixed \( a \), then there exists an integer \( x \in \mathbb{Z}_n \) such that \( \lambda_k(r, a) \neq x \) for all \( r \). Now consider the inner product

\[ \langle x + nb | 0 \rangle a + nb \rangle_k = \frac{1}{\sqrt{n}} \sum_{r=0}^{n-1} q^b r \omega_k(r, a, b) \delta_{x, \lambda_k(r, a)} \] \hspace{1cm} (101)

\[ = 0, \hspace{1cm} (102) \]

since by assumption, \( \delta_{x, \lambda_k(r, a)} = 0 \) for all \( r \). Hence, if \( \lambda_k \) is not injective there is at least one vector from the standard basis that is orthogonal to the new basis. There are no way to choose the phases \( \omega_k \) to make it MU to every vector in the standard basis.

Similarly, unbiasedness with respect to the Fourier basis holds if and only if the function is injective for fixed \( r \). This means that the function \( \lambda_k(r, a) \) defines a Latin square, an \( n \) by \( n \) array such that each row and column contain the symbols from an \( n \)-letter alphabet exactly once.

As an example, let \( n = p \) be a prime number. Then the Weyl-Heisenberg group contains \( p+1 \) cyclic subgroups altogether. Two of them were accounted for from the start, and the remaining \( p - 1 \) examples give rise to the choice

\[ \lambda_k(r, a) = a + kr, \quad k \in \{1, 2, \ldots, p - 1\} \] \hspace{1cm} (103)
By inspection one finds that these $p - 1$ bases are maximally entangled. In addition, the Latin squares that define the bases are Mutually Orthogonal, which ensures that we have a collection of $p + 1$ Mutually Unbiased Bases.

The fact that $x - 1$ Mutually Orthogonal Latin squares of order $n$ give rise to $x + 1$ Mutually Unbiased Bases—regardless of whether they originate from group theory or not—was first observed by Wocjan and Beth [27]. The only new observation here is that Latin squares appear naturally in the cyclic $N$-roots problem when the phase-permutation basis is used.

To illustrate the idea, consider dimension $N = 2^2$. The two eigenbases are given by

$$|0\rangle_0 = \frac{1}{\sqrt{2}} (|0,0\rangle + |1,0\rangle) \quad |2\rangle_0 = \frac{1}{\sqrt{2}} (|0,0\rangle - |1,0\rangle) \quad (104)$$

$$|1\rangle_0 = \frac{1}{\sqrt{2}} (|0,1\rangle + |1,1\rangle) \quad |3\rangle_0 = \frac{1}{\sqrt{2}} (|0,1\rangle - |1,1\rangle), \quad (105)$$

and

$$|0\rangle_\infty = \frac{1}{\sqrt{2}} (|0,0\rangle + |0,1\rangle) \quad |2\rangle_\infty = \frac{1}{\sqrt{2}} (|0,0\rangle - |0,1\rangle) \quad (106)$$

$$|1\rangle_\infty = \frac{1}{\sqrt{2}} (|1,0\rangle - i|1,1\rangle) \quad |3\rangle_\infty = \frac{1}{\sqrt{2}} (|1,0\rangle + i|1,1\rangle). \quad (107)$$

The Latin square $\lambda_1 = a + r$, then generates the third basis

$$|0\rangle_1 = \frac{1}{\sqrt{2}} (|0,0\rangle + \theta_0|1,1\rangle) \quad |2\rangle_1 = \frac{1}{\sqrt{2}} (|0,0\rangle + \theta_2|1,1\rangle) \quad (108)$$

$$|1\rangle_1 = \frac{1}{\sqrt{2}} (|0,1\rangle + \theta_1|1,0\rangle) \quad |3\rangle_1 = \frac{1}{\sqrt{2}} (|0,1\rangle + \theta_3|1,0\rangle), \quad (109)$$

unbiased with respect to eqs. (105) and (107). We have removed an overall phase from each vector leaving the remaining free phases $\theta_0, \ldots, \theta_3$. The conditions for the vectors to form a basis are simply that $1 + \theta_0 \theta_2 = 0$ and $1 + \theta_1 \theta_3 = 0$.

In dimension $N = 4$, this method constructs the complete set of solutions to the cyclic $N$-roots problem. In dimension 9 however, whilst we find the two parameter family of solutions, there are 6,156 other isolated points [30].
9. Conclusions and questions

Our main result is that the entire Clifford group admits a representation using only monomial phase-permutation matrices if and only if the dimension is a square number. We also gave such a representation explicitly.

In the course of the proof we proved some theorems about the Weyl-Heisenberg and Clifford groups that we suspect are known, but which we were unable to find in the literature.

We used this representation to gain some insight into the SIC problem. It shares with the standard representation the elegant property that a SIC when orthogonally projected onto the simplex spanned by the basis within the body of density matrices is again a regular simplex, with \( N \) rather than \( N^2 \) vertices. Expressions for the SIC fiducials are much simplified, but are still considerably hard to calculate when the dimension exceeds \( 2^2 \). At least the case \( N = 4 \) is now trivial, and we can now solve the case \( N = 9 \) by hand. More significantly, we find for the first time an exact solution to the SIC problem in dimension \( N = 16 \).

We have applied the phase-permutation representation to the problem of finding all vectors unbiased with respect to both the standard and the Fourier bases. Families of solutions can then be constructed naturally from Latin squares. Finally, we note that quantum mechanics in square-dimensional Hilbert spaces is of particular importance because they admit bipartite entanglement; we therefore expect that the phase-permutation representation will have many other applications.

Acknowledgments: We thank Åsa Ericsson for the idea of Section 8 and Steve Donkin for discussions on Appendix B. The authors gratefully acknowledge the hospitality of the Nordita workshop on the Foundations of Quantum Mechanics. We thank Berge Englert for inviting IB to CQT, which led to some motivating discussions.

DMA was supported in part by the U. S. Office of Naval Research (Grant No. N00014-09-1-0247). Research at Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research & Innovation. IB is supported by the Swedish Research Council under contract VR 621-2007-4060. SB was supported by the EU FP7 FET-Open research project COMPAS (Contract
No. 212008). DG gratefully acknowledges support by the Institut Mittag-Leffler (Djursholm, Sweden), where his contribution to this work was done. DG’s research is supported by the German Science Foundation (DFG grants CH 843/1-1 and CH 843/2-1) and the Swiss National Science Foundation.

References

[1] H. Weyl: Theory of Groups and Quantum Mechanics, Dutton, New York 1932.

[2] D. I. Fivel, Remarkable phase oscillations appearing in the lattice dynamics of Einstein-Podolsky-Rosen states, Phys. Rev. Lett. 74 (1995) 835.

[3] D. Gottesman, A theory of fault-tolerant quantum computation, Phys. Rev. A57 (1998) 127.

[4] G. Zauner: Quantendesigns. Grundzüge einer nichtkommutativen Designtheorie, PhD thesis, Univ. Wien 1999. Available in English translation at http://www.gerhardzauner.at.

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

[6] P. W. H. Lemmens and J. J. Seidel, Equiangular lines, J. Algebra 24 (1973) 494.

[7] C. A. Fuchs and R. Schack, Quantum-Bayesian coherence, eprint arXiv:0906.2187.

[8] C. A. Fuchs, QBism, the Perimeter of Quantum Bayesianism, eprint arXiv:1003.5209.

[9] D. M. Appleby, Á. Ericsson and C. A. Fuchs, Properties of QBist state spaces, Found. of Phys. 41 (2011) 564.

[10] J. Du, M. Sun, X. Peng and T. Durt, Realization of entanglement assisted qubit-covariant symmetric-informationally-complete positive-operator-valued measurements, Phys. Rev. A74 (2006) 042341.
[11] T. Durt, A. Lamas-Linares, A. Ling and C. Kurtsiefer, *Wigner tomography of two qubit states and quantum tomography*, Phys. Rev. A78 (2008) 042338.

[12] Z. E. D. Medendorp, F. A. Torres-Ruiz, L. K. Shalm, G. N. M. Tabia, C. A. Fuchs and A. M. Steinberg, *Experimental characterization of qutrits using SIC-POVMs*, Phys. Rev. A83 (2011) 051801R.

[13] A. J. Scott and M. Grassl, *SIC-POVMs: A new computer study*, J. Math. Phys. 51 (2010) 042203.

[14] D. M. Appleby, *SIC-POVMs and the extended Clifford group*, J. Math. Phys. 46, 052107 (2005).

[15] A. Klappenecker and M. Rötteler, *On the monomiality of nice error bases*, IEEE Trans. Inform. Theory 5 (2005) 1.

[16] J. Zak, *Dynamics of electrons in solids in external fields*, Phys. Rev. 168 (1968) 686.

[17] D. Mumford: *Tata Lectures on Theta I*, Birkhäuser, Boston 1983.

[18] M. Grassl, *Computing equiangular lines in complex space*, in Proc. Mathematical Methods in Computer Science (MMICS 2008), Karlsruhe, Germany, Dec. 2008, Lecture Notes in Computer Science 5393 (2008) 89.

[19] D. Gross, *Hudson’s Theorem for finite-dimensional quantum systems*, J. Math. Phys. 47, 122107 (2006).

[20] M. Khatirinejad, *On Weyl-Heisenberg orbits of equiangular lines*, J. Algebra. Comb. 28 (2008) 333.

[21] D. M. Appleby, H. B. Dang and C. A. Fuchs, *Symmetric Informationally-Complete quantum states as analogues to orthonormal bases and Minimum Uncertainty States*, eprint arXiv:0707.2071.

[22] D. M. Appleby, *SIC-POVMs and MUBs: Geometrical relationships in prime dimensions*, in L. Accardi et al (eds.): Proc of the Växjö Conference on Foundations of Probability and Physics - 5, AIP Conf. Proc. 1101, New York 2009. Also available as arXiv:0905.1428.
Appendix A: Action of the Clifford group

**Lemma 3:** The action of the Clifford group on $H(N)/Z(N) \simeq \mathbb{Z}_N^2$ is isomorphic to $SL(2, N)$.

**Proof:** Let $G : \mathbb{Z}_N^2 \rightarrow \mathbb{Z}_N^2$ be a transformation induced by the action of a Clifford unitary on $H(N)/Z(N)$. First, we show that $G$ must be an element of $SL(2, N)$. 
That $G$ is linear follows from the fact that $H(N)/Z(N)$ is a projective representation of $Z_N^2$. Now consider the following commutation relation, which is a simple consequence of (8):

$$D_{ij}D_{kl} = \omega^{kj-il}D_{kl}D_{ij}$$

(110)

for $i, j, k, l \in Z_N$. Conjugate every matrix appearing in the relation above by the Clifford unitary $U_G$. All the phase factors $\tau^{k'}$ appearing in the definition (10) cancel, because they occur on both sides of the equality. With $(i', j') = G(i, j)$ and $(k', l') = G(k, l)$, we conclude that

$$\omega^{kj-il} = \omega^{k'j'-i'l'}.$$  

(111)

Because $\omega$ has order $N$, $G$ preserves symplectic inner products modulo $N$. Thus, $G \in SL(2, N)$ as claimed.

Next, we have to show that every transformation in $SL(2, N)$ can be realized. For $N$ odd, this is the content of (14) proven in Ref. [14]. Hence, we only need to consider the case of even $N$. In this case, (14) says that if $G \in SL(2, \bar{N})$, then $G \mod N$ may be realized as a transformation of $H(N)/Z(N)$. Therefore, what remains to be shown is that every matrix $G$ in $SL(2, N)$ can be written as $\bar{G} \mod N$ for some $\bar{G} \in SL(2, 2N)$.

Write $N$ as $N = 2^m n$ for $n$ odd. In Appendix B, we show that

$$H(N) \simeq H(2^m) \times H(n), \quad SL(2, \bar{N}) \simeq SL(2, 2^m) \times SL(2, n).$$

(112)

What is more, “the even and the odd parts do not mix” in the sense that $SL(2, 2^m)$ only acts on $H(2^m)$ and $SL(2, n)$ only acts on $H(n)$. Therefore, we need to prove the claim only for the case $N = 2^m$.

So let $G \in SL(2, N)$. Then $\det G = kN + 1$ for some integer $k$. If $k$ is even, then $\det G \equiv 1 \mod 2N$ and therefore $G \in SL(2, 2N)$, so we are done. Thus we assume that $k$ is odd. Not all matrix elements of $G$ are even, for then the range of $G$ would consist only of vectors with even components. This would contradict that fact that $G$ is invertible. Assume for now that $\alpha$, the top left matrix element of $G$, is odd (we label the matrix elements of $G$ as in (12)). Then it has an inverse $\alpha^{-1}$ modulo $2N$. Now let

$$\bar{G} = \left( \begin{array}{cc} \alpha & \beta \\ \gamma & \delta + \alpha^{-1}N \end{array} \right).$$

(113)

37
Then
\[ \det \bar{G} = \det G + \alpha \alpha^{-1} N = (k + \alpha \alpha^{-1}) N + 1 \equiv 1 \mod 2N. \] (114)
Thus \( \bar{G} \in SL(2,2N) \). The cases where one of the other matrix elements of \( G \) is odd are treated analogously. \( \square \)

**Appendix B: Tensor Product Representation**

The Weyl-Heisenberg group in dimension \( N \) is defined in terms of three generators \( \tilde{X}, \tilde{Z} \) and \( \tilde{\tau} \) and the relations between them. We denote the abstract group elements with a tilde; their standard unitary representations, defined in eq. (3), appear without. In odd dimensions, the Weyl-Heisenberg group, \( H(N) \) is given by
\[
\left\langle \tilde{X}, \tilde{Z}, \tilde{\tau} : \tilde{X}^N = \tilde{Z}^N = \tilde{\tau}^N = 1, \quad \tilde{Z} \tilde{X} = \tilde{\tau} \tilde{X} \tilde{Z}, \quad \tilde{\tau} \tilde{X} = \tilde{X} \tilde{\tau}, \quad \tilde{\tau} \tilde{Z} = \tilde{Z} \tilde{\tau} \right\rangle
\] (115)
whilst for \( N \) even, we choose to enlarge the centre and define \( H(N) \) to be
\[
\left\langle \tilde{X}, \tilde{Z}, \tilde{\tau} : \tilde{X}^N = \tilde{Z}^N = \tilde{\tau}^{2N} = 1, \quad \tilde{Z} \tilde{X} = \tilde{\tau}^2 \tilde{X} \tilde{Z}, \quad \tilde{\tau} \tilde{X} = \tilde{X} \tilde{\tau}, \quad \tilde{\tau} \tilde{Z} = \tilde{Z} \tilde{\tau} \right\rangle.
\] (116)

When the dimension has the prime factorization \( N = n_1 n_2 \ldots n_r \), where \( n_j = p_j^{u_j} \), the group is a direct product of smaller groups,
\[
H(N) = H(n_1) \times H(n_2) \times \cdots \times H(n_r).
\] (117)
To see this, we construct an isomorphism as follows. Let the group elements of \( H(n_j) \) be generated by \( \tilde{X}_j, \tilde{Z}_j \) and \( \tilde{\tau}_j \) and define elements of \( H(n_1) \times \cdots \times H(n_r) \) as
\[
x = (\tilde{X}_1, \ldots, \tilde{X}_r), \quad z = (\tilde{Z}_1, \ldots, \tilde{Z}_r), \quad t = (\tilde{\tau}_1, \ldots, \tilde{\tau}_r).
\] (118)
The elements \( x, z \) and \( t \) satisfy the relations for the group \( H(N) \) since, for example,
\[
x^N = ((\tilde{X}_1^{n_1})^{N/n_1}, (\tilde{X}_2^{n_2})^{N/n_2}, \ldots, (\tilde{X}_r^{n_r})^{N/n_r}) = (1, 1, \ldots, 1).
\] (119)
Therefore, the map
\[ \theta : \tilde{X}^a \tilde{Z}^b \tilde{\tau}^c \to x^a z^b t^c \]  
(120)
is a homomorphism.

The image of \( \theta \) is given by all elements of the form \( x^a z^b t^c \) and we now show that it contains the group \( H(n_1) \times \cdots \times H(n_r) \). The Chinese remainder theorem tells us that since \( n_j \) and \( n_k \) are coprime for all \( j \neq k \) there exists an integer \( \lambda_1 \) such that \( \lambda_1 \equiv 1 \mod n_1 \) and \( \lambda_1 \equiv 0 \mod n_j \) for \( j = 2, \ldots, r \). The integer \( \lambda_1 \) picks out the first component of \( x \),
\[ x^{\lambda_1} = (\tilde{X}_1^{\lambda_1}, \tilde{X}_2^{\lambda_1}, \ldots, \tilde{X}_r^{\lambda_1}) = (\tilde{X}_1, 1, \ldots, 1). \]  
(121)

In the same way, there exist integers, \( \lambda_2, \ldots, \lambda_r \) and \( \mu_1, \ldots, \mu_r \) such that
\[ x^{\lambda_j} = (1, \ldots, 1, \tilde{X}_j, 1, \ldots, 1) \]
\[ z^{\mu_j} = (1, \ldots, 1, \tilde{Z}_j, 1, \ldots, 1). \]  
(122)

The components of the element \( t \) are computed modulo \( \bar{n}_j \) so we need to modify our argument slightly. In even dimensions, the Chinese remainder theorem still applies since only one of the factors, say \( n_1 \), is even. The integer \( 2n_1 \) is therefore coprime to \( n_j \) for all \( j \), and we can again find integers \( \nu_1, \ldots, \nu_r \) such that
\[ t^{\nu_j} = (1, \ldots, 1, \tilde{\tau}_j, 1, \ldots, 1). \]  
(123)

Finally, the size of the two groups are equal,
\[ |H(N)| = N^2 \bar{N} = |H(n_1) \times \cdots \times H(n_r)| \]  
so \( \theta \) is an isomorphism.

Now for the Clifford group \( C(N) \). We use the fact that \( C(N) \) is the semi-direct product of \( H(N) \) and \( SL(2, \bar{N}) \). We start by taking elements of \( SL(2, \bar{N}) \) and computing their components modulo \( \bar{n}_j \), that is,
\[ F_j \equiv \left( \begin{array}{cc} \alpha_j & \beta_j \\ \gamma_j & \delta_j \end{array} \right), \]  
(124)
where \( \alpha_j = \alpha \mod \bar{n}_j \), \( \beta_j = \beta \mod \bar{n}_j \), \( \gamma_j = \gamma \mod \bar{n}_j \) and \( \delta_j = \delta \mod \bar{n}_j \). Then the map
\[ \Gamma : SL(2, \bar{N}) \to SL(2, \bar{n}_1) \times \cdots \times SL(2, \bar{n}_r), \]  
(125)
defined by
\[ \Gamma(F) = (F_1, \ldots, F_r), \]  
(126)
is an isomorphism. The proof follows a similar argument to the above and implies that

$$C(N) \simeq H(n_1) \times \cdots \times H(n_r) \times SL(2, \bar{n}_1) \times \cdots \times SL(2, \bar{n}_r)$$

$$\simeq H(n_1) \times SL(2, \bar{n}_1) \times \cdots \times H(n_r) \times SL(2, \bar{n}_r)$$

$$\simeq C(n_1) \times \cdots \times C(n_r).$$

Theorem 19.18 of Ref. [31]). Let $G$ and $J$ be groups, then every irreducible representation of the group $G \times J$ is a tensor product of an irreducible representation of $G$ with an irreducible representation of $J$. The Weyl-Heisenberg and Clifford groups are direct products of the groups defined over the prime factorization and therefore all irreducible representations can be written as a tensor product of irreducible representations of the smaller groups.

Care is required when writing down the isomorphisms in terms of the standard unitary representation, $X, Z$ and $\tau$, defined in eq. (3). If we define the map

$$\eta : x^a z^b t^c \rightarrow (\tau_1^c \ldots \tau_r^c) \left( X_1^a Z_1^b \otimes \cdots \otimes X_r^a Z_r^b \right),$$

we have the problem that in general,

$$\tau_1^c \ldots \tau_r^c \neq \tau^c,$$

meaning that the right hand side of eq. (128) cannot be the image of $\theta$ under any unitary induced mapping. To fix this problem, we redefine $\eta$ to be

$$\eta' : x^a z^b t^c \rightarrow (\tau_1^{\kappa_1} \ldots \tau_r^{\kappa_r}) \left( X_1^a Z_1^b \otimes \cdots \otimes X_r^a Z_r^b \right),$$

where $\kappa_j$ is the multiplicative inverse of $N/n_j$ mod $\bar{n}_j$. The map $\eta'$ then satisfies all of the required properties to be an isomorphism.

To construct the isomorphism for the standard unitary representation of the Clifford group, we take the image of the symplectic matrices, $F_j$ to be $U_{F_j'}$, where

$$F_j' = \begin{pmatrix} \alpha_j & \kappa_j^{-1} \beta_j \\ \kappa_j^{-1} \gamma_j & \delta_j \end{pmatrix},$$

rather than $U_{F_j}$. Whilst we did not need the explicit form of the two isomorphisms in this paper, we hope that it will prove a useful tool elsewhere.
Appendix C: Fiducial vectors for $N = 16$

16a

$$w_2 := \sqrt{2};$$
$$w_{13} := \sqrt{3};$$
$$w_{17} := \sqrt{17};$$
$$I := \sqrt{-1};$$
$$w_{26} := w_2 w_{13};$$
$$w_{34} := w_2 w_{17};$$
$$w_{221} := w_{13} w_{17};$$
$$w_{442} := w_2 w_{13} w_{17};$$

$$r_2 := \sqrt{w_{13} w_{17} - 11};$$
$$r_3 := \sqrt{15 + w_{17}};$$
$$t_1 := \sqrt{15 + (4 - w_{17}) r_3 - 3 w_{17}};$$
$$t_2 := \sqrt{(-5 w_{17} + 3) w_{13} + (39 w_{17} - 65)} r_3 + (16 w_{17} - 72) w_{13} + 936;$$
$$t_3 := \sqrt{72 w_{17} - 108 w_{13} - 112 w_{17} - 200 w_{26} - 520 w_{34} + 40 w_{442} - 1200};$$

$$c_01 := (-20/13, w_{26} + 3 r_1 t_1 t_2 + (-90 w_2 + 60 w_{13}) + 30 w_{26} + 10 w_{34} + 20 w_{221} + 10 w_{442} - 60) r_3 + (60 w_{13} + 60 w_{17} + 20 w_{221} + 140) t_1 t_3 + (350 w_2 + 160 w_{13} - 40 w_{17} + 150 w_{26} - 50 w_{34} + 10 w_{442} + 760) r_3 + (400 w_2 + 400 w_{13} - 600 w_{17}) + 320 w_{26} - 320 w_{34} - 40 w_{221} - 80 w_{442} + 360) t_3 + I + (-40/13, w_{13} - 20 w_{26} + r_3 + t_1 t_2 + (160 w_2 + 20 w_{26} + 160 w_{13} - 500 w_{17} - 160 w_{26} - 160 w_{34} + 60 w_{221} - 20 w_{442} - 120) t_1 + t_3 + (530 w_2 + 60 w_{13} - 100 w_{17} - 30 w_{26} - 70 w_{34} + 20 w_{221} + 10 w_{442} + 620) r_3 + (520 w_2 - 600 w_{13} - 1120 w_{17} - 200 w_{26} - 520 w_{34} + 40 w_{442} - 1200)) t_3.$$
\( c_{16} := (\cdots + 12w_2 - 10w_{13} + 7w_{17} - 62w_{26} + 30w_{34} - 10w_{442} + 280) \times 3 \times + 240w_2 + 20w_{13} + 8w_{17} + 4w_{26} + 20w_{34} + 34w_{442} - 280; \)

\( \phi := [c_{01}, c_{02}, c_{03}, c_{04}, c_{05}, c_{06}, c_{07}, c_{08}, c_{09}, c_{10}, c_{11}, c_{12}, c_{13}, c_{14}, c_{15}, c_{16}]; \)

16b

\( w_2 := \text{Sqrt}(2); \)

\( w_{13} := \text{Sqrt}(13); \)

\( I := \text{Sqrt}(-1); \)

\( w_{26} := w_2 w_{13}; \)
w34 := w2*w17;
w221 := w13*w17;
w442 := w2*w13*w17;
r2 := Sqrt(w13*w17+11);
r3 := Sqrt(15+w17);
t1 := Sqrt(((-5*w17+3)*w13+(39*w17-65))*r3+((16*w17-72)*w13+936))*t1-208+w13+2288);
t3 := Sqrt(2-w2);
t4 := Sqrt(2+t3);

c01 := (-20/13*w26*r3*t1*t2+((-90*w2+60*w13-20*w17-11)*r3+(400*w2440+w34-600+w34-400+w221-800w442+360))*t3)+11 (-40/13*w13-20/13*w26)*r3*t1*t2+((140+w2+20*w26+160)*r3-20*w2-260+w13-500+w17-140*w26-140*w34-60*w221-20*w442-1260)*t1*t3+((530*w2-60*w13+100*w17-30*w26-70*w34+20*w221+10*w442+620)*r3+(520*w2-400+w13-1120+w17-200*w26-520*w34+400*w442-1200))*t3;
c02 := (((10/2-4*w26-2*w34)*r2+r2*r2+(-24*w2-24*w26-12*w34-4*w442)*r2+(-50*w13+10*w17-10*w221-30)*r3+(350*w2-70+w34-70*w26-110*w34-10*w221-10*w442-10)*t1*t3+(((-52/2*w2+11*w13+3*w17+27/2*w26+21/2*w34+3*w221+3/2*w442+43)*r2+r2*t2+((44*w242+14*w13+14*w17+12*w26+64*w34+44*w442)*r2+(-85*w2+50*w13-10*w17-25*w26+15*w34+10*w221))*t1*t3+((53/2*w2+11*w13+3*w17+27/2*w26+21/2*w34+44*w442)*r2+((25*w2+25*w13+5*w17+15*w26-5*w34+5*w221+5*w442+5)*t1)*t4+((33/2*w2-28*w26-28*w34+64*w442))*t1*t3+((-32/13*w2+20*w13+13*w17+140*w2640+w34+20*w221+540))*t1*t4+((-53/2*w2-28*w26-28*w34+64*w442))*t1+((-35/2*w2+11*w13+3*w17+7/2*w26-1/2*w34-2*w221-3/2*w442-11)*r2*r2+(-75*w2+26*w13-2*w17+5*w26-5*w34+2*w221-5*w442+22))*t2+((25*w2+25*w13+5*w17+15*w26-5*w34+5*w221+5*w442+5)*t1)*t3+((-462*w2+25*w13+5*w17+15*w26-5*w34+5*w221+5*w442+5)*t1)*t4+((-600*w2+90*w13-150*w17-250*w26-250*w34-50*w221-50*w442-50)*t1+((-100*w2-250*w13+150*w17+30*w26-70*w34+20*w221+10*w442+620)*r3+(520*w2-400+w13-1120+w17-200*w26-520*w34+400*w442-1200))*t3;

\text{phi} := \{ c_{01}, c_{02}, c_{03}, c_{04}, c_{05}, c_{06}, c_{07}, c_{08}, c_{09}, c_{10}, c_{11}, c_{12}, c_{13}, c_{14}, c_{15}, c_{16} \}