Some remarks on Heisenberg frames and sets of equiangular lines

Len Bos
Dept. of Mathematics and Statistics
University of Calgary
Calgary, Alberta
Canada T2N1N4
e–mail: lpbos@math.ucalgary.ca

Shayne Waldron
Dept. of Mathematics
University of Auckland
Private Bag 92019, Auckland, New Zealand
e–mail: waldron@math.auckland.ac.nz

August 5, 2006

Editors remark: After submission the authors learned that some of their results had be obtained independently by Appleby [2]. The manuscript has been modified to appropriately reference these results.

Abstract

We consider the long standing problem of constructing d^2 equiangular lines in $\mathbb{C}^d$, i.e., finding a set of d^2 unit vectors (ϕ_j) in $\mathbb{C}^d$ with

$$|\langle \phi_j, \phi_k \rangle| = \frac{1}{\sqrt{d+1}}, \qquad j \neq k.$$

Such 'equally spaced configurations' have appeared in various guises, e.g., as complex spherical 2–designs, equiangular tight frames, isometric embeddings $\ell_2(d) \to \ell_4(d^2)$, and most recently as SICPOVMs in quantum measurement theory. Analytic solutions are known only for $d = 2, 3, 4, 5, 6, 8$ and $d = 7, 19$ (Appleby 2005). Recently, numerical solutions which are the orbit of a discrete Heisenberg group H have been constructed for $d \leq 45$. We call these Heisenberg frames.

In this paper we study the normaliser of H, which we view as a group of symmetries of the equations that determine a Heisenberg frame. This allows us to simplify the equations for a Heisenberg frame, e.g., for d odd we have $\frac{1}{8}d^2 + \frac{7}{8}$ real equations in the d coordinates of v and their complex conjugates. From these simplified equations we are able construct analytic solutions for $d = 5, 7$, and make conjectures about the form of a solution. It is hoped that a general solution will come from such a simplified set of equations.

Key Words: complex spherical 2–design, equiangular lines, equiangular tight frame, Grassmannian frame, Heisenberg frame, isometric embeddings, discrete Heisenberg group modulo d, SICPOVM (symmetric informationally–complete positive operator–valued measure)

AMS (MOS) Subject Classifications:

primary: 05B30, 42C15, 65D30, 81P15.

secondary: 51F25, 81R05.

---

1 Introduction

We consider the following problem: find a set of d^2 unit vectors (ϕ_j) in $\mathbb{C}^d$ with

$$|\langle \phi_j, \phi_k \rangle| = \frac{1}{\sqrt{d+1}}, \qquad j \neq k. \tag{1.1}$$

Problems of this type have a long history, dating back to the early study of polyhedra in real Euclidean space, some of which we discuss at the end of this section. Analytic solutions are known only for $d = 2, 3, 4, 5, 6, 8$ and $d = 7, 19$ (Appleby [2]). Most recently it has appeared in quantum measurement theory (cf [10], [11]), where numerical calculations for $d \leq 45$ suggest that it has a solution given by the orbit of a discrete Heisenberg group H of unitary transformations on $\mathbb{C}^d$ (Conjecture 1 of [11]). We call solutions of this type Heisenberg frames.

If v is a unit vector in $\mathbb{C}^d$, then the condition $(hv)_{h\in H}$ is a Heisenberg frame, i.e., $|\langle gv, hv\rangle| = |\langle v, g^{-1}hv\rangle = \frac{1}{\sqrt{d+1}} = 1$, $g \neq h$, is equivalent to

$$|\langle v, hv\rangle| = \frac{1}{\sqrt{d+1}}, \qquad h \in H,\ h \neq 1. \tag{1.2}$$

The key to our results is the following simple observation. If v gives a Heisenberg frame, and U is unitary and in the normaliser of H, i.e., $U^{-1}hU = U^*hU \in H$, $\forall h \in H$, then Uv also gives rise to a Heisenberg frame, since

$$|\langle Uv, hUv\rangle| = |\langle v, U^*hUv\rangle| = |\langle v, U^{-1}hUv\rangle| = \frac{1}{\sqrt{d+1}}, \qquad h \in H,\ h \neq 1.$$

Thus we are naturally led to the normaliser of H in the unitary matrices, which we think of as a group of symmetries of the equations determining a Heisenberg frame.

The remaining sections are as follows. In Section 2, we define the (discrete) Heisenberg group (modulo d), and develop its basic properties. In Section 3, we give three types of elements in the normaliser of H, but *not* in H itself: the Fourier matrix F, a diagonal matrix Q, and certain permutation matrices P_a, $a \in \mathbb{Z}_d^+$. This observation that the normaliser of H is larger than H is the key to the results given here. The elements of (scalar) order three in the group generated by H and F, Q, P_a, $a \in \mathbb{Z}_d^*$ are particularly important, and we determine what they are in Section 4. In Section 5, we observe there is another transformation mapping solutions to solutions, that of pointwise conjugation. This is not a linear map. The equations (1.2) for $v \in \mathbb{C}^d$ to generate a Heisenberg frame are d^2 equations in d complex variables. In Section 6, we give sets of equivalent, and more easily solved equations. In particular, for d odd we have $1 + \frac{1}{8}(d^2 - 1) = \frac{1}{8}d^2 + \frac{7}{8}$ real equations in the d coordinates of v and their complex conjugates. In Section 7, we solve the equivalent sets of equations for $d = 2, 3, 5, 7$. Our solution for $d = 3$ has a neat geometric presentation which is not apparent in earlier solutions.

1.1 Historical remarks

Let X be a set of n unit vectors in $\mathbb{C}^d$ and $t \in \{0, 1, 2, \ldots\}$. Then a simple argument of [15] based on the Cauchy–Schwarz inequality shows that

$$\sum_{x,y \in X} |\langle x, y\rangle|^{2t} \geq \frac{n^2}{\binom{d+t-1}{t}}. \tag{1.3}$$

Incidently, for n unit vectors in $\mathbb{R}^d$ it can be proved that

$$\sum_{x,y \in X} |\langle x, y\rangle|^{2t} \geq \frac{n^2}{\frac{d(d+2)\cdots(d+2t-2)}{1\cdot 3\cdot 5\cdots(2t-1)}}, \tag{1.4}$$

which is sharper for $t \geq 2$, $d > 1$.

Equality in (1.3) is equivalent to many other conditions (cf [7], [9], [6]). These include X being a complex spherical t–design (cubature formula with equal weights for certain polynomials on the complex sphere with the Haar measure), X being a SIC POVM (symmetric informationally complete positive operator valued measure), the existence of an isometric embedding $\ell_2(d) \to \ell_{2t}(n)$ for $t > 0$, and the Waring–type formula

$$\frac{1}{n}\sum_{x \in X} |\langle y, x\rangle|^{2t} = \frac{\langle y, y\rangle^t}{\binom{d+t-1}{d-1}}, \qquad \forall y \in \mathbb{C}^d.$$

It can be shown that if (any one of) these equivalent conditions hold for $t = k$, then they also hold for $t \leq k$. Note the condition for $t = 0$ holds trivially. If X is a set of $n = d^2$ unit vectors in $\mathbb{C}^d$ satisfying (1.1), then there is equality in (1.3) for $t = 2$ since

$$\sum_{x,y \in X} |\langle x, y\rangle|^4 = \frac{n^2 - n}{(\sqrt{d+1})^4} + n = \frac{2d^3}{d+1} = \frac{n^2}{\binom{d+1}{2}}.$$

In particular, the Waring–type formula for $t = 1$ holds, i.e.,

$$\|y\|^2 = \frac{d}{n}\sum_{x \in X} |\langle y, x\rangle|^2, \quad \forall y \in \mathbb{C}^d \quad \Longleftrightarrow \quad y = \frac{d}{n}\sum_{x \in X}\langle y, x\rangle x, \quad \forall y \in \mathbb{C}^d,$$

which is the definition of X being an (equal–norm/isometric) tight frame (cf [14]).

We arrived at this problem as that of finding a tight frame X of n unit vectors which are equiangular, i.e., with $|\langle x, y\rangle| = C$, $x \neq y$. These must give equality in (1.3) for $t = 1$, and satisfy (1.3 for $t = 2$, i.e.,

$$(n^2 - n)C^2 + n = \frac{n^2}{d}, \qquad (n^2 - n)C^4 + n \geq \frac{n^2}{\binom{d+1}{2}},$$

Substituting the formula for C^2 given by the first equation into the second and simplifying gives $(d-1)(n-d^2) \leq 0$. Hence such an equiangular tight frame exists only if

$n \leq d^2$ (for $d > 1$). Thus a solution to the problem, should it exist, is an equiangluar tight frame for $\mathbb{C}^d$ with the maximal number of vectors.

Problems of the type considered here have a long history dating back to the study of polyhedra in real Euclidean space. The analogous problem of finding n equiangular lines in $\mathbb{R}^d$ has received most attention. Here (1.3) leads to the bound $n \leq \frac{1}{2}d(d+1)$. However this is not attained unless $d = 2, 3$ or $d = r^2 - 2$ with $r \neq 1$ an odd integer (cf [8]), and the theory does not seem as neat as in the complex case, e.g., the analogue of the equivalant conditions above (cf [12]).

2 The discrete Heisenberg group

Throughout fix the integer $d \geq 1$, and let ω be the primitive d–th root of unity

$$\omega := e^{2\pi i/d}.$$

Let $S \in \mathbb{C}^{d\times d}$ be the shift (rotation down) matrix, and $\Omega \in \mathbb{C}^{d\times d}$ the diagonal matrix which are given by

$$S := \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \cdot & & \cdot & & & \cdot \\ \cdot & & & \cdot & & \cdot \\ 0 & 0 & 0 & & 1 & 0 \end{bmatrix}, \qquad \Omega := \begin{bmatrix} 1 & 0 & 0 & \cdot & \cdot & 0 \\ 0 & \omega & 0 & \cdot & \cdot & 0 \\ 0 & 0 & \omega^2 & & & 0 \\ \cdot & \cdot & & \cdot & & \\ \cdot & \cdot & & & \cdot & \\ 0 & 0 & 0 & & & \omega^{d-1} \end{bmatrix}. \tag{2.1}$$

These have order d, i.e., $S^d = \Omega^d = I$, and satisfy the **commutativity relation**

$$\Omega^k S^j = \omega^{jk} S^j \Omega^k. \tag{2.2}$$

In particular, the group generated by S and Ω contains the scalar matrices $\omega^r I$.

Definition 1 *The group $H = \langle S, \Omega\rangle$ generated by the matrices S and Ω is called the* **discrete Heisenberg group modulo** *d, or for short the* **Heisenberg group**.

In view of (2.2), the Heisenberg group is given explicitly by

$$H = \{\omega^r T_{jk} : 0 \leq r, j, k \leq d-1\}, \qquad T_{jk} := S^j \Omega^k.$$

Since ω, S, Ω have order d, it is convenient to allow the indices of $\omega^r T_{jk}$ to be integers modulo d. Since S and Ω are unitary, H is a group of unitary matrices. Further, H is closed under taking adjoints as (2.2) gives the **adjoint rule**

$$(T_{jk})^* = (S^j\Omega^k)^* = \Omega^{-k}S^{-j} = \omega^{(-j)(-k)}S^{-j}\Omega^{-k} = \omega^{jk}T_{-j,-k}. \tag{2.3}$$

It is easy to verify that H satisfies the **multiplication rule** $T_{r_0 j_0 k_o} T_{r_1 j_1 k_1} = T_{rjk}$, where

$$\begin{bmatrix} 1 & k & r \\ 0 & 1 & j \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & k_0 & r_0 \\ 0 & 1 & j_0 \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & k_1 & r_1 \\ 0 & 1 & j_1 \\ 0 & 0 & 1 \end{bmatrix}. \tag{2.4}$$

The group H has order d^3, and so the orbit of a $v \neq 0$ consists of d^3 vectors $(hv)_{h\in H}$. But for j, k fixed, the d vectors $\omega^r T_{jk} v$, $0 \leq r \leq d-1$ are scalar multiples of each other, which we identify together. It is in this sense that the orbit of H is interpreted as a set of d^2 (hopefully equiangular) vectors, say $\{T_{jk}v : 0 \leq j, k \leq d-1\}$.

Incidently, the group H is irreducible, i.e., the orbit of every $v \neq 0$, $v \in \mathbb{C}^d$ spans $\mathbb{C}^d$, from which it follows (cf [13]) that every nonzero orbit of H is a tight frame for $\mathbb{C}^d$.

3 The normaliser of the Heisenberg group

Here we investigate the **normaliser** of H in the unitary matrices $\mathcal{U}(d)$, i.e., the group

$$N(H) := \{U \in \mathcal{U}(d) : U^{-1}hU = U^*hU \in H, \forall h \in H\}.$$

The normaliser $N(H)$ contains H. We will show it also contains matrices F, Q, P_a, $a \in \mathbb{Z}_d^*$, which are defined below, and hence the group they generate together with S, Ω.

From now on, it is convenient to index the entries of all matrices in $\mathbb{C}^{d\times d}$ by elements of $\mathbb{Z}_d$, i.e., $\{0, \ldots, d-1\}$ rather than $\{1, \ldots, d\}$. For example, the entries of the S and Ω are given by

$$(S)_{jk} = \begin{cases} 1, & \text{j=k+1;} \\ 0, & otherwise \end{cases} \qquad (\Omega)_{jk} = \begin{cases} \omega^j, & \text{j=k;} \\ 0, & otherwise. \end{cases}$$

Let $F \in \mathcal{U}(d)$ be the **Fourier matrix** which is given by

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

Since S is circulant, it is diagonalised by F, which leads to the **conjugacy relation**

$$S = F^* \Omega F. \tag{3.1}$$

Let $Q \in \mathcal{U}(d)$ be the **quadratic diagonal matrix** which is given by

$$(Q)_{jk} := \begin{cases} \omega^{j^2}, & \text{k=j;} \\ 0 & otherwise. \end{cases}$$

Let $\mathbb{Z}_d^*$ be the (multiplicative) group of elements $a \in \mathbb{Z}^d$ with a multiplicative inverse, i.e., an $\overline{a} \in \mathbb{Z}_d$ with $a\overline{a} = 1$ (modulo d). For $a \in \mathbb{Z}_d^*$, let $P_a \in \mathcal{U}(d)$ be the **multiplicative permutation matrix**

$$(P_a)_{jk} := \begin{cases} 1 & \text{ifk=aj;} \\ 0 & \text{otherwise.} \end{cases}$$

Note that $a \mapsto P_a$ is a group isomorphism, and in particular

$$P_a P_b = P_{ab}, \qquad P_a^{-1} = P_{\overline{a}} = P_a^*, \qquad a, b \in \mathbb{Z}_d^*.$$

Let $\overline{A}$ be the matrix obtained from A by taking the complex conjugate of each entry. Then

$$\overline{S} = S, \qquad \overline{\Omega} = \Omega^*, \qquad \overline{F} = F^*, \qquad \overline{Q} = Q^*, \qquad \overline{P_a} = P_a, \tag{3.2}$$

and from (3.1) we obtain

$$S = \overline{S} = \overline{F^*}\,\overline{\Omega}\,\overline{F} = F\Omega^* F^* \quad \Longrightarrow \quad \Omega^* = F^* S F. \tag{3.3}$$

Lemma 1 *The unitary matrices F, Q, P_a, $a \in \mathbb{Z}_d^*$ belong to $N(H)$, since*

$$F^*(S^j\Omega^k)F = \omega^{-jk} S^k \Omega^{-j} \in H, \tag{3.4}$$

$$Q^*(S^j\Omega^k)Q = \omega^{-j^2} S^j \Omega^{k-2j} \in H, \tag{3.5}$$

$$P_a^*(S^j\Omega^k)P_a = S^{aj}\Omega^{\overline{a}k} \in H. \tag{3.6}$$

Proof: From (3.1) and (3.3), we have $F^*\Omega^k F = S^k$ and $F^* S^j F = (\Omega^*)^j = \Omega^{-j}$, so that

$$F^*(S^j\Omega^k)F = (F^*S^jF)(F^*\Omega^kF) = \Omega^{-j}S^k = \omega^{-jk}S^k\Omega^{-j}.$$

Since $(S^j)_{\alpha\beta} = \delta_{\alpha,\beta+j}$, we calculate

$$\begin{aligned} (Q^*S^jQ)_{\alpha\beta} &= (Q^*)_{\alpha\alpha}(S^j)_{\alpha\beta}(Q)_{\beta\beta} = \omega^{-\alpha^2}\delta_{\alpha,\beta+j}\omega^{\beta^2} = \omega^{-(\beta+j)^2}\delta_{\alpha,\beta+j}\omega^{\beta^2} \\ &= \omega^{-j^2}\delta_{\alpha,\beta+j}\omega^{-2j\beta} = \omega^{-j^2}(S^j)_{\alpha\beta}(\Omega^{-2j})_{\beta\beta} = (\omega^{-j^2}S^j\Omega^{-2j})_{\alpha\beta}, \end{aligned}$$

so that $Q^*S^jQ = \omega^{-j^2}S^j\Omega^{-2j}$, and since diagonal matrices commute $Q^*\Omega^kQ = \Omega^k$. Hence

$$Q^*(S^j\Omega^k)Q = (Q^*S^jQ)(Q^*\Omega^kQ) = \omega^{-j^2}S^j\Omega^{k-2j}.$$

Using $(P_a)_{jk} = \delta_{aj,k}$, we calculate

$$\begin{aligned} (P_a^*S^jP_a)_{\alpha\beta} &= (P_{\overline{a}}S^jP_a)_{\alpha\beta} = \sum_r\sum_s (P_{\overline{a}})_{\alpha r}(S^j)_{rs}(P_a)_{s\beta} = \sum_r\sum_s \delta_{\overline{a}\alpha,r}\delta_{r,s+j}\delta_{as,\beta} \\ &= \sum_s \delta_{\overline{a}\alpha,s+j}\delta_{as,\beta} = \sum_s \delta_{\overline{a}\alpha,\overline{a}\beta+j} = \delta_{\alpha,\beta+aj} = (S^{aj})_{\alpha\beta}, \end{aligned}$$

so that $P_a^*S^jP_a = S^{aj}$. Similarly, one shows that $P_a^*\Omega^kP_a = \Omega^{\overline{a}k}$, and hence

$$P_a^*(S^j\Omega^k)P_a = (P_a^*S^jP_a)(P_a^*\Omega^kP_a) = S^{aj}\Omega^{\overline{a}k}.$$

□

Let E be the subgroup of $N(H)$ generated by H together with F, Q and P_a, $a \in \mathbb{Z}_d^+$, i.e.,

$$E := \langle \Omega, S, F, Q, P_a : a \in \mathbb{Z}_d^+ \rangle.$$

Lemma 1 gives a commutativity relation between the elements of H and $K := \langle F, Q, P_a : a \in \mathbb{Z}_d^+ \rangle$, i.e.,

$$(S^j \Omega^k) F = F \omega^{-jk} S^k \Omega^{-j}, \quad (S^j \Omega^k) Q = Q \omega^{-j^2} S^j \Omega^{k-2j}, \quad (S^j \Omega^k) P_a = P_a S^{aj} \Omega^{\overline{a}k},$$

so that elements of E can be expressed in form hk, $h \in H$, $k \in K$. However, for d even this product in not direct since $H \cap K$ contains the matrices

$$\Omega^{\frac{d}{2}} = [(-1)^j \delta_{jk}] = Q^{\frac{d}{2}}, \qquad S^{\frac{d}{2}} = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix} = F^* Q^{\frac{d}{2}} F, \tag{3.7}$$

and also $\omega^{\frac{d}{2}} I = -I = (F Q^{\frac{d}{2}})^4$ when $d/2$ is odd. Hence sometimes we restrict ourselves to the simpler case of d an odd prime. The generators of K satisfy the commutativity relations

$$P_a F = F P_{\overline{a}}, \qquad P_a Q^b = Q^{ba^2} P_a, \tag{3.8}$$

but no such relation between F and Q exists.

It is convenient to generalise the commutativity relation (3.5).

Lemma 2 *We have the commutativity relation*

$$S^j \Omega^k Q^r = \omega^{rj^2 - jk} Q^r \Omega^{k-2rj} S^j. \tag{3.9}$$

Proof: By the commutativity relation (2.2), the result is equivalent to

$$S^j \Omega^k Q^r = \omega^{rj^2 - jk} Q^r \omega^{(k-2rj)j} S^j \Omega^{k-2rj} = \omega^{-rj^2} Q^r S^j \Omega^{k-2rj},$$

which we prove by induction on r. For $r = 0$ this holds trivially for all j, k. For $r > 0$, the induction hypothesis and (3.5) gives

$$\begin{aligned} S^j \Omega^k Q^r &= (S^j \Omega^k Q^{r-1}) Q = \omega^{-(r-1)j^2} Q^{r-1} S^j \Omega^{k-2(r-1)j} Q \\ &= \omega^{-(r-1)j^2} Q^r (Q^* S^j \Omega^{k-2(r-1)j} Q) = \omega^{-(r-1)j^2} Q^r (\omega^{-j^2} S^j \Omega^{k-2(r-1)j-2j}) \\ &= \omega^{-rj^2} Q^r S^j \Omega^{k-2rj}. \end{aligned}$$

□

Proposition 2 *The subgroup of E generated by Ω, S, Q and P_b, $b \in \mathbb{Z}_d^*$ consists of all the matrices of the form*

$$\omega^\rho L_{\alpha\beta\gamma\delta} := \omega^\rho \Omega^\delta Q^\alpha S^\gamma P_\beta, \qquad \rho, \alpha, \gamma, \delta \in \mathbb{Z}_d, \ \beta \in \mathbb{Z}_d^*. \tag{3.10}$$

These satisfy the multiplication rule

$$L_{\alpha\beta\gamma\delta} L_{abcd} = \omega^{-\gamma\beta d + a\beta^2\gamma^2} \Omega^{\delta+\beta d - 2a\beta^2\gamma} Q^{\alpha + a\beta^2} S^{\gamma + c\overline{\beta}} P_{\beta b}. \tag{3.11}$$

Proof: It suffices to prove (3.11). This follows from the commutativity relations

$$P_\beta \Omega^d = \Omega^{\beta d} P_\beta, \qquad P_\beta Q^a = Q^{a\beta^2} P_\beta, \qquad P_\beta S^c = S^{c\overline{\beta}} P_\beta,$$

$$S^\gamma \Omega^{\beta d} = \omega^{-\gamma\beta d} \Omega^{\beta d} S^\gamma, \qquad S^\gamma Q^{a\beta^2} = \omega^{a\beta^2\gamma^2} Q^{a\beta^2} \Omega^{-2a\beta^2\gamma} S^\gamma,$$

which are special cases of (3.5), (3.8) and (3.9), by the calculations

$$\Omega^\delta Q^\alpha S^\gamma P_\beta \Omega^d Q^a = \omega^{-\gamma\beta d + a\beta^2\gamma^2} \Omega^{\delta+\beta d - 2a\beta^2\gamma} Q^{\alpha + a\beta^2} S^\gamma P_\beta, \tag{3.12}$$

and

$$\begin{aligned} L_{abcd} &= (\Omega^\delta Q^\alpha S^\gamma P_\beta)(\Omega^d Q^a S^c P_b) = (\Omega^\delta Q^\alpha S^\gamma P_\beta \Omega^d Q^a)(S^c P_b) \\ &= \omega^{-\gamma\beta d + a\beta^2\gamma^2} \Omega^{\delta+\beta d - 2a\beta^2\gamma} Q^{\alpha + a\beta^2} S^\gamma P_\beta S^c P_b. \end{aligned}$$

which gives the result since $P_\beta S^c P_b = S^{c\overline{\beta}} P_\beta P_b = S^{c\overline{\beta}} P_{\beta b}$. □

For d even, (3.7) implies that

$$\Omega^{\delta + \frac{d}{2}} Q^{\alpha + \frac{d}{2}} = \Omega^\delta Q^\alpha,$$

and so some care must be taken counting the matrices (3.10).

Lemma 3 *For $a, b, c \in \mathbb{Z}_d$ the functions*

$$f(a,b,c) : \mathbb{Z}_d \to \mathbb{C} : j \mapsto \omega^{aj^2 + bj + c} = (\omega^c \Omega^b Q^a)_{jj}$$

are different, unless d is even in which case the following pairs of functions are equal

$$f(a,b,c) = f(a + \frac{d}{2}, b + \frac{d}{2}, c).$$

In particular, the number of (diagonal) matrices of the form

$$\omega^\rho \Omega^\delta Q^\alpha, \qquad \rho, \delta, \alpha \in \mathbb{Z}_d$$

is d^3 for d odd, and $d^3/2$ for d even.

Proof: An easy calculation gives the result for $d = 1, 2$. Suppose that $d \geq 3$, and $f(a_1, b_1, c_1) = f(a_2, b_2, c_2)$, i.e., $a_1 j^2 + b_1 j + c_1 \equiv a_2 j^2 + b_2 j + c_2 \bmod \mathrm{d}$, $\forall j \in \mathbb{Z}_d$. Taking $j = 0, 1, -1$ gives $c_1 \equiv c_2$, $a_1 + b_1 + c_1 \equiv a_2 + b_2 + c_2$, $a_1 - b_1 + c_1 \equiv a_2 - b_2 + c_2$, which we solve to get

$$c_1 \equiv c_2, \qquad 2(a_1 - a_2) \equiv 0, \qquad 2(b_1 - b_2) \equiv 0.$$

If d is odd, then $2 \in \mathbb{Z}_d^*$ (since $2\frac{d+1}{2} \equiv 1$), and we have $a_2 = a_1$, $b_2 = b_1$, $c_2 = c_1$.

If d is even, then $2x \equiv 0$ has two solutions $x = 0, \frac{d}{2}$, and so solving the equations for $j = 0, 1, -1$ gives either $a_2 = a_1$, $b_2 = a_1$ or $a_2 = a_1 + \frac{d}{2}$, $b_2 = b_1 + \frac{d}{2}$. Either of these choices satisfies the equations for all j, since $\frac{d}{2} j^2 + \frac{d}{2} j \equiv \frac{d}{2} j(j+1) \equiv 0$, and so we are done. □

Since $\langle S \rangle \cap \langle P_\beta : \beta \in \mathbb{Z}_d^* \rangle = \{1\}$, the group of permutation matrices generated by S and $\{P_\beta\}_{\beta \in \mathbb{Z}_d^*}$ has order $|\langle S \rangle| \, |\langle P_\beta \rangle| = d\phi(d)$, where $\phi(d)$ is the Euler function. Hence Lemma 3 gives

$$|\langle \Omega, S, Q, P_b : b \in \mathbb{Z}_d^* \rangle| = \#\{\omega^\rho L_{\alpha\beta\gamma\delta}\} = \begin{cases} d^4 \phi(d), & d \text{ odd;} \\ \frac{1}{2} d^4 \phi(d), & d \text{ even.} \end{cases}$$

We now consider a set of matrices in $N(H)$ that involve F.

Theorem 3 *For $\rho, \alpha, \beta, \gamma, \delta, \epsilon \in \mathbb{Z}_d$ and $\beta \in \mathbb{Z}_d^*$, the matrices*

$$\omega^\rho M_{\alpha\beta\gamma\delta\epsilon} := \omega^\rho \Omega^\delta Q^\alpha P_\beta F Q^\gamma \Omega^\epsilon = \frac{1}{\sqrt{d}} [\omega^{\alpha j^2 + \beta jk + \gamma k^2 + \delta j + \epsilon k + \rho}]_{jk} \tag{3.13}$$

are all in the normaliser $N(H)$. These satisfy the multiplication rules:

(a) *If $\gamma + a = 0$, then*

$$M_{\alpha\beta\gamma\delta\epsilon} M_{abc\partial e} = \omega^{c\overline{b}^2(\epsilon+\partial)^2 - e\overline{b}(\epsilon+\partial)} Q^{\alpha + c(\beta\overline{b})^2} \Omega^{\delta - e\beta\overline{b} + 2c\beta\overline{b}^2(\epsilon+\partial)} S^{-\overline{\beta}(\epsilon+\partial)} P_{-\beta\overline{b}}, \tag{3.14}$$

(b) *If d is an odd prime, and $\nu := \overline{\gamma + a} \neq 0$, $r := -\overline{2}^2 \nu (\varepsilon + \partial)^2$, then*

$$M_{\alpha\beta\gamma\delta\epsilon} M_{abc\partial e} = (\gamma + a|d) \frac{1 - i^d}{1 - i} \omega^r \Omega^{\delta - \overline{2}\nu\beta(\epsilon+\partial)} Q^{\alpha - \overline{2}^2 \nu \beta^2} P_{-\overline{2}\nu\beta b} F Q^{c - \overline{2}^2 \nu b^2} \Omega^{e - \overline{2}\nu b(\epsilon+\partial)}. \tag{3.15}$$

Proof: We have already observed $M_{\alpha\beta\gamma\delta\epsilon} \in E \subset N(H)$. First multiply out to get

$$(M_{\alpha\beta\gamma\delta\epsilon})_{jk} = \sum_r \sum_s \sum_t \sum_u \sum_v (\Omega^\delta)_{jr} (Q^\alpha)_{rs} (P_\beta)_{st} (F)_{tu} (Q^\gamma)_{uv} (\Omega^\epsilon)_{vk}$$

$$= \sum_{r,s,t,u,v} \omega^{\delta j}\delta_{jr}\omega^{\alpha r^2}\delta_{rs}\delta_{\beta s,t}\frac{\omega^{tu}}{\sqrt{d}}\omega^{\gamma u^2}\delta_{uv}\omega^{\epsilon v}\delta_{vk} = \frac{1}{\sqrt{d}}\omega^{\delta j+\alpha j^2+\beta jk+\gamma k^2+\epsilon k}.$$

Hence the product of $M_{\alpha\beta\gamma\delta\epsilon}$ and $M_{abc\partial e}$ is given by

$$\begin{aligned}(M_{\alpha\beta\gamma\delta\epsilon}M_{abc\partial e})_{jk} &= \sum_r (M_{\alpha\beta\gamma\delta\epsilon})_{jr}(M_{abc\partial e})_{rk} \\ &= \sum_s \frac{1}{\sqrt{d}}\omega^{\alpha j^2+\beta js+\gamma s^2+\delta j+\epsilon s}\frac{1}{\sqrt{d}}\omega^{as^2+bsk+ck^2+\partial s+ek} \\ &= \frac{1}{d}\omega^{\alpha j^2+\delta j+ck^2+ek}\sum_s \omega^{(\gamma+a)s^2+(\beta j+\epsilon+bk+\partial)s}.\end{aligned} \tag{3.16}$$

Case (a): If $\gamma+a=0$, then the last sum in (3.16) is zero, unless $\beta j+\epsilon+bk+\partial=0$. This gives (3.14), since

$$(S^{-\overline{\beta}(\epsilon+\partial)}P_{-\beta\bar{b}})_{jk} = \sum_r (S^{-\overline{\beta}(\epsilon+\partial)})_{jr}(P_{-\beta\bar{b}})_{rk} = \sum_r \delta_{j,r-\overline{\beta}(\epsilon+\partial)}\delta_{-\beta\bar{b}r,k} = 0$$

$$\iff \quad j = r-\overline{\beta}(\epsilon+\partial),\ -\beta\bar{b}r = k, \quad \iff \quad \beta j+\epsilon+bk+\partial = 0.$$

Case (b): Now suppose $\gamma+a\neq 0$. We have to deal with the quadratic Gauss sum in (3.16). Provided that $2(\gamma+a)$ divides $\beta j+\epsilon+bk+\partial$, e.g., d is an odd prime, we can complete the square

$$(\gamma+a)s^2+(\beta j+\epsilon+bk+\partial)s = (\gamma+a)\{(s+\eta)^2-\eta^2\}, \qquad \eta := \frac{\beta j+\epsilon+bk+\partial}{2(\gamma+a)},$$

and the Gauss sum becomes

$$\sum_s \omega^{(\gamma+a)s^2+(\beta j+\epsilon+bk+\partial)s} = \sum_s \omega^{(\gamma+a)\{(s+\eta)^2-\eta^2\}} = \omega^{-(\gamma+a)\eta^2}G(\gamma+a,d),$$

where

$$G(\gamma+a,d) := \sum_r \omega^{(\gamma+a)r^2} = \sum_s \omega^{(\gamma+a)(s+\eta)^2}.$$

Suppose that d is an odd prime, then the above sum can be evaluated (see [1]:§9.10)

$$G(\gamma+a,d) = (\gamma+a|d)G(1,d), \qquad G(1,d) = \frac{1-i^d}{1-i}\sqrt{d},$$

where $(\gamma+a|d)$ is the Legendre symbol, giving

$$(M_{\alpha\beta\gamma\delta\epsilon}M_{abc\partial e})_{jk} = (\gamma+a|d)\frac{1-i^d}{1-i}\frac{1}{\sqrt{d}}\omega^{\alpha j^2+\delta j+ck^2+ek}\omega^{-(\gamma+a)\eta^2}. \tag{3.17}$$

For d an odd prime, every nonzero element of $\mathbb{Z}_d$ is invertible: in particular 2 and $\gamma+a\neq 0$. Hence we obtain (3.15) by simplifying (3.17) using

$$-(\gamma+a)\eta^2 = -(\overline{\gamma+a})\overline{2}^2(\beta^2j^2+b^2k^2+(\epsilon+\partial)^2+2\beta(\epsilon+\partial)j+2b(\epsilon+\partial)k+2\beta bjk).$$

$\square$

Observe that (3.14) gives an element of the form (3.10), and (3.15) gives one of the form (3.13) multiplied by the scalars $(\gamma + a|d) = \pm 1$ and

$$\frac{1-i^d}{1-i} = \begin{cases} 1, & d \equiv 1 \bmod 4; \\ i & d \equiv 3 \bmod 4. \end{cases} \tag{3.18}$$

The product of matrices of the form (3.10) and (3.13) is of the form (3.13), since by (3.12)

$$\begin{aligned} L_{\alpha\beta\gamma\delta} M_{abcde} &= (\Omega^\delta Q^\alpha S^\gamma P_\beta)(\Omega^d Q^a P_b F Q^c \Omega^e) \\ &= \omega^{-\gamma\beta d + a\beta^2\gamma^2} \Omega^{\delta+\beta d - 2a\beta^2\gamma} Q^{\alpha + a\beta^2} P_{\beta b} F Q^c \Omega^e. \end{aligned} \tag{3.19}$$

Hence (since $F = M_{01000}$), for $d = p$ an odd prime, E consists of the $p^4(p-1)$ matrices of the form (3.10) and the $p^5(p-1)$ matrices of the form (3.13), together with their multiples by ± 1 and powers of the scalars (3.18). Thus it has order

$$|E| = \begin{cases} 2p^4(p-1)(p+1), & p \equiv 1 \bmod 4; \\ 4p^4(p-1)(p+1), & p \equiv 3 \bmod 4. \end{cases} \tag{3.20}$$

Example. For $d = p$ an odd prime, (3.15) gives the 'commutativity' between F and Q

$$F^* Q F = \frac{1-i^p}{1-i} Q^{-\overline{2}^2} P_{-\overline{2}} F Q^{-\overline{2}^2},$$

while if d not an odd prime and $\gamma + a \neq 0$, the product (3.15) may not be of the form (3.10) or (3.13), e.g., for $d = 4$, we have

$$F^* Q F = \frac{1}{2} \begin{bmatrix} i+1 & 0 & 1-i & 0 \\ 0 & i+1 & 0 & 1-i \\ 1-i & 0 & i+1 & 0 \\ 0 & 1-i & 0 & i+1 \end{bmatrix} =: A, \qquad A^2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

It can be deduced from the results in [2], where the quotient of $N(H)$ with the scalar matrices is considered, that the normaliser of H consists of E and the scalar matrices, i.e.,

$$N(H) := \langle \Omega, S, F, Q, P_a, cI : a \in \mathbb{Z}_d^+, c \in \mathbb{C} \rangle.$$

We also observe the matrix R given by

$$R_{jk} := \mu^{j(j+d)} \delta_{jk}, \qquad \mu := e^{\frac{2\pi i}{2d}}$$

normalises the Heisenberg group up to a scalar (and so maps solutions to solutions), i.e.,

$$R^*(S^j \Omega^k) R = \mu^{j(d-j)} S^j \Omega^{k-j}.$$

This R is a square root of Q, and belongs to E for d odd, i.e.,

$$R^2 = Q, \qquad R = Q^{\frac{d+1}{2}} \quad (d \text{ odd}).$$

4 Elements of scalar order three

Based on extensive numerical calculations, it appears that:

Conjecture 4 *(Zauner). For $d > 3$ odd, the vectors $v \in \mathbb{C}^d$ which give rise to a Heisenberg frame are eigenvectors of a matrix in E which has scalar order 3, where the corresponding eigenvalue has multiplicity greater than one.*

Definition 5 *A matrix $A \in \mathbb{C}^{d \times d}$ has* **scalar order 3** *if $A \neq I$ and $A^3 = \mu I$, for $\mu \in \mathbb{C}$.*

Note that matrices of order 3 have scalar order 3, and that if a matrix of scalar order 3 has finite order (e.g., it is in E) then some power of it has order 3. If d is an odd prime, then (3.20) and Cauchy's theorem implies that E has elements of (scalar) order 3.

Since vectors v generating Heisenberg frames appear to be eigenvectors of elements of scalar order 3, it is natural to identify these (see below). Our vision is to then seek (analytic) solutions by representing v in terms of the eigenvectors of an appropriate element of $A \in E$ order 3. There are two factors to balance here: we want A to have small eigenspaces and also to have a simple form.

Lemma 4 *The matrix $\omega^\rho L_{\alpha\beta\gamma\delta}$, $\beta \neq 1$ has scalar order 3 if and only if $\beta^3 \equiv 1 \bmod \mathrm{d}$.*

Proof: By applying (3.11) twice, we obtain

$$(\omega^\rho L_{\alpha\beta\gamma\delta})^3 = \omega^t \Omega^{(\delta - 2\alpha\beta^2\gamma)(1+\beta+\beta^2)} Q^{\alpha(1+\beta^2+\beta^4)} S^{\gamma(1+\overline{\beta}+\overline{\beta}^2)} P_{\beta^3},$$

where $t = 3\rho - \gamma\beta\delta + \alpha\beta^2\gamma^2 - \gamma\beta(\delta + \beta\delta - 2\alpha\beta^2\gamma) + \beta^2\gamma^2(\alpha + \alpha\beta^2)$. This can be a scalar multiple only if $\beta^3 = 1$. But if $\beta^3 = 1$, then $(\omega^\rho L_{\alpha\beta\gamma\delta})^3$ is scalar multiple of the identity, since

$$1 + \beta + \beta^2 = \frac{\beta^3 - 1}{\beta - 1} = 0, \qquad 1 + \beta^2 + \beta^4 = 1 + \overline{\beta} + \overline{\beta}^2 = \frac{\beta^6 - 1}{\beta^2 - 1} = 0.$$

□

Lemma 5 *Let $d = p$ an odd prime, then $\omega^\rho M_{\alpha\beta\gamma\delta\varepsilon}$ has of scalar order 3 if and only if*

$$\beta \equiv 2(\alpha + \gamma) \not\equiv 0 \bmod \mathrm{d}.$$

Proof: If $\gamma+\alpha=0$, then (3.14) and (3.19) imply that $(\omega^\rho M_{\alpha\beta\gamma\delta\varepsilon})^3$ is a matrix of the form (3.13), and so cannot be a scalar multiple of the identity.

Now suppose that $d=p$ an odd prime, and $\gamma+\alpha\neq 0$. Then (3.15) gives

$$(M_{\alpha\beta\gamma\delta\varepsilon})^2=\mu M_{abcde}, \qquad \mu\in\mathbb{C}, \quad a=\alpha-\overline{2}^2(\overline{\gamma+\alpha})\beta^2, \quad b=-\overline{2}(\overline{\gamma+\alpha})\beta^2.$$

So by Theorem 3, $(\omega^\rho M_{\alpha\beta\gamma\delta\varepsilon})^3$ can be a scalar matrix only if $\gamma+a=0$ and $-\beta\overline{b}=1$. Now $-\beta\overline{b}=1$ is equivalent to $\beta=2(\alpha+\gamma)$, and with this choice $\gamma+a=\gamma+\alpha-\overline{2}^2(\overline{\gamma+\alpha})\beta^2=0$, and

$$a=-\gamma, \qquad b=-\beta, \qquad c=\gamma-\overline{2}\beta, \qquad d=-\varepsilon, \qquad e=-\delta.$$

By (3.14), it follows that if $\beta=2(\alpha+\gamma)$ then $(\omega^\rho M_{\alpha\beta\gamma\delta\varepsilon})^3$ is a scalar matrix since

$$\alpha+c(\beta\overline{b})^2=0, \qquad \delta-e\beta\overline{b}+2c\beta\overline{b}^2(\varepsilon+d)=0, \qquad -\overline{\beta}(\varepsilon+d)=0.$$

$\square$

Examples. If there is a solution to $\beta^3=1$ mod d (which implies that d is odd), then the permutation matrix P_β has order 3, e.g., P_2 for $d=7$, P_4 for $d=9$, and P_3 for $d=13$.

For $d=p$ an odd prime, it follows that $Q^{\frac{d+1}{2}}F$ and $FQ^{\frac{d+1}{2}}$ have scalar order 3, since $\beta=2(\alpha+\gamma)=2\frac{d+1}{2}=1$. In particular, for $d=5$, the matrix Q^3F has scalar order 3.

5 Conjugate solutions

We have observed than if a unit vector $v\in\mathbb{C}^d$ generates a Heisenberg frame, i.e.,

$$|v^*S^j\Omega^k v|^2=\frac{1}{d+1}, \qquad (j,k)\neq(0.0),$$

then so does Uv for any U in the normaliser of H. There is another simple operation that maps v to another solution, namely (entrywise) conjugation, since (3.2) gives

$$\overline{v^*S^j\Omega^k v}=\overline{v}^*\overline{S}^j\overline{\Omega}^k\overline{v}=\overline{v}^*S^j\Omega^{-k}\overline{v} \quad\Longrightarrow\quad |v^*S^j\Omega^k v|=|\overline{v}^*S^j\Omega^{-k}\overline{v}|.$$

Note that $v\mapsto\overline{v}$ is not linear (it is norm preserving).

Now consider the set $\mathcal{V}$ of all unit vectors $v\in\mathbb{C}^d$ that generate a Heisenberg frame, which we often refer to as 'solutions'. We say that solutions v and w are **equivalent** if

$$v=\alpha Uw, \qquad |\alpha|=1, \quad U\in E,$$

i.e., they are in the same G–orbit of $\mathcal{V}$ under the (multiplication) action of the group

$$G:=\{\alpha U:|\alpha|=1,U\in E\}.$$

It follows from (3.2) that E is closed under (entrywise) conjugation, as is therefore G, and so conjugation maps a G–orbit of $\mathcal{V}$ either to itself, or to another G–orbit. In the latter case, we say that a solutions v and w are **conjugate to each other** if v and $\overline{v}$ are in different orbits and w belongs to the orbit of $\overline{v}$.

6 Equivalent equations for Heisenberg frames

If $v \in \mathbb{C}^d$ is a unit vector, then the d^2 unit vectors $\{S^j\Omega^k v : j,k \in \mathbb{Z}_d\}$ form a tight frame for $\mathbb{C}^d$, which we call a **Heisenberg frame** if (1.1) holds.

By (1.2), it follows that $v \in \mathbb{C}^d$ is a Heisenberg frame if and only if

$$|v^* S^j \Omega^k v|^2 = \frac{1}{d+1}, \qquad (j,k) \neq (0,0), \qquad \|v\|^2 = 1.$$

These d^2 quartic equations in $v_1, \ldots, v_d$, $\overline{v_1}, \ldots, \overline{v_d}$ with coefficients from $\mathbb{Q}[\omega]$ have proven difficult to solve (for $d > 3$). We now find equivalent and more tractable sets of equations.

Our equivalent sets of equations come from the observation that $v^* S^j \Omega^k v$ are the eigenvalues of certain circulant matrices. Recall (see [3],Th. 3.2.2) that each circulant matrix

$$C = \operatorname{circ}(z) := [z, Sz, \ldots, S^{d-1}z] \in \mathbb{C}^{d\times d}, \qquad z \in \mathbb{C}^d$$

is diagonalised by the Fourier transform matrix F, with eigenvalues given by

$$\lambda_k = \sum_r z_r \omega^{kr}, \qquad k = 0, \ldots, d-1.$$

For $j \neq 0$, we calculate

$$v^* S^j \Omega^k v = (S^{-j}v)^* \Omega^k v = \sum_r \overline{v_{r+j}} \omega^{kr} v_r = \sum_r (v_r \overline{v_{r+j}}) \omega^{kr}, \qquad k = 0, \ldots, d-1,$$

which are the eigenvalues of the circulant matrix $\operatorname{circ}(U_j)$, where $(U_j)_r := v_r \overline{v_{r+j}}$.

Since these values $|v^* S^j \Omega^k v|$ must be constant for v to generate a Heisenberg frame, it is natural to consider when the eigenvalues of a circulant matrix have constant modulus.

Lemma 6 *A nonzero circulant matrix $C_z := \operatorname{circ}(z)$, $z \in \mathbb{C}^d$ has eigenvalues of constant modulus if and only if*

$$C_z^* C_z = \|z\|^2 I,$$

i.e., $\frac{1}{\|z\|} C_z$ is unitary and C_z has eigenvalues of modulus $\|z\|$.

Proof: Since C_z is circulant, it is diagonalised by F, i.e., $C_z = F^* \Lambda F$ with Λ diagonal, and hence $C_z^* C_z = F^* \Lambda^* \Lambda F$. But $\Lambda^* \Lambda$ is diagonal and its diagonal entries are the modulus squared of the eigenvalues of C_z. Hence C_z has eigenvalues of constant modulus α if and only if $\Lambda^* \Lambda$ is the scalar matrix $\alpha^2 I$, in which case $C_z^* C_z = \alpha^2 F^* F = \alpha^2 I$. By evaluating the $(1,1)$–entries of $C_z^* C_z = \alpha^2 I$, we get $\|z\|^2 = \alpha^2$. □

Theorem 6 *Suppose that $v \in \mathbb{C}^d$, and let*

$$U_j := \begin{bmatrix} v_0\overline{v_{0+j}} \\ v_1\overline{v_{1+j}} \\ v_2\overline{v_{2+j}} \\ \vdots \\ v_{d-1}\overline{v_{d-1+j}} \end{bmatrix}, \quad 0 \le j \le d-1, \qquad m_d := \frac{1}{2}\begin{cases} d-1, & d \text{ odd;} \\ d, & d \text{ even.} \end{cases}$$

Then v is a unit vector and generates a Heisenberg frame if and only if

(a) $\|U_0\|^2 = \dfrac{2}{d+1}$,

(b) $\|U_j\|^2 = \dfrac{1}{d+1}$, $\quad 1 \le j \le m_d$,

(c) $\langle U_j, S^k U_j\rangle = 0$, $\quad 1 \le j, k \le m_d$.

Proof: First we observe that (b) and (c) hold equivalently with m_d replaced by $d-1$, since

$$U_{-j} = S^j(\overline{U_j}), \qquad \langle U_j, S^{-k}U_j\rangle = \overline{\langle U_j, S^k U_j\rangle}.$$

Hence the conditions (b) and (c) are equivalent to

$$\operatorname{circ}(U_j)^* \operatorname{circ}(U_j) = \frac{1}{d+1} I, \qquad j \ne 0.$$

Since the eigenvalues of U_j, $j \ne 0$ are $\lambda_k = v^* S^j \Omega^k v$, by Lemma 6 this is equivalent to

$$|v^* S^j \Omega^k v| = \frac{1}{\sqrt{d+1}}, \qquad j = 1, \ldots, d-1, \quad k = 0, \ldots, d-1.$$

Now suppose that (b) holds, then

$$\|v\|^4 = \|U_0\|^2 + \sum_{j=1}^{d-1} \|U_j\|^2 \frac{d-1}{d+1} \quad \Longleftrightarrow \quad \|v\|^4 - 1 = \|U_0\|^2 - \frac{2}{d+1},$$

and (a) is equivalent to $\|v\| = 1$ (given that (b) holds). Hence if v is unit vector which generates a Heisenberg frame (a),(b) and (c) hold.

Thus it remains only to show that if (a),(b) and (c) hold (so $\|v\| = 1$), then

$$|v^* \Omega^k v| = \frac{1}{\sqrt{d+1}}, \qquad k = 1, \ldots, d-1. \tag{6.1}$$

Now for any $\beta \in \mathbb{R}$,

$$v^* \Omega^k v = \sum_r |v_r|^2 \omega^{kr} = \sum_r (|v_r|^2 + \beta)\omega^{kr}, \qquad k = 1, \ldots, d-1,$$

so that $v^*\Omega^k v$, $k\neq 0$ are eigenvalues of the circulant matrix $C_z=\mathrm{circ}(z)$, $z_r:=|v_r|^2+\beta$. By Lemma 6, this has all its eigenvalues of modulus $1/\sqrt{d+1}$ if and only if

$$\|z\|^2=\sum_r(|v_r|^2+\beta)^2=\sum_r|v_r|^4+2\beta\sum_r|v_r|^2+d\beta^2=\|U_0\|^2+2\beta\|v\|^2+d\beta^2=\frac{1}{d+1},$$

and $C_z^*C_z=\|z\|^2 I$. Since $\|U_0\|^2=1/(d+1)$ and $\|v\|=1$, the quadratic above becomes

$$d\beta^2+2\beta+1/(d+1)=0 \quad\iff\quad \beta=\frac{\sqrt{d+1}\pm 1}{d\sqrt{d+1}}.$$

If we take either of these two choices of β, then $C_z^*C=\|z\|^2 I$ holds, since

$$\begin{aligned}\langle z,S^jz\rangle &= \sum_r(|v_r|^2+\beta)(|v_{r-j}|^2+\beta)=\sum_r|v_r|^2|v_{r-j}|^2+2\beta\sum_r|v_r|^2+d\beta^2\\ &= \|U_{-j}\|^2+2\beta\|v\|^2+d\beta^2=d\beta^2+2\beta+1/(d+1)=0, \qquad j\neq 0,\end{aligned}$$

and hence (6.1) holds. □

Lemma 7 *The condition* (c) *of Theorem 6 can be reduced to*

$$\langle U_j,S^kU_j\rangle=0, \qquad 1\le j\le k\le m_d. \tag{6.2}$$

Proof: Making the substitution $r=s-j+k$, we obtain

$$\begin{aligned}\langle U_j,S^kU_j\rangle &= \sum_r(U_j)_r\overline{(S^kU_j)_r}=\sum_r v_r\overline{v_{r+j}}\,\overline{v_{r-k}\overline{v_{r-k+j}}}=\sum_r v_r v_{r-k+j}\overline{v_{r+j}v_{r-k}}\\ &= \sum_s v_{s-j+k}v_s\overline{v_{s+k}v_{s-j}}=\sum_s v_s v_{s-j+k}\overline{v_{s-j}v_{s+k}}=\langle U_k,S^jU_k\rangle.\end{aligned}$$

Suppose that (6.2) holds. Then the equation $\langle U_j,S^kU_j\rangle=0$ also holds for $j>k$, since

$$\langle U_j,S^kU_j\rangle=\langle U_k,S^jU_k\rangle=0.$$

□

Thus we have an equivalent set of $m_d+1+\frac{1}{2}m_d(m_d+1)=\frac{1}{2}(m_d+1)(m_d+2)\le\frac{1}{4}d^2$ quartic equations in $v_1,\ldots,v_d$, $\overline{v_1},\ldots,\overline{v_d}$ with coefficients from $\mathbb{Q}$.

Theorem 7 *Suppose that d is odd and $v\in\mathbb{C}^d$. Let*

$$V_j:=\begin{bmatrix} v_{0-j}v_{0+j}\\ v_{1-j}v_{1+j}\\ v_{2-j}v_{2+j}\\ \vdots\\ v_{d-1-j}v_{d-1+j}\end{bmatrix}, \quad 0\le j\le d-1, \qquad m_d:=\frac{1}{2}(d-1).$$

Then v is a unit vector and generates a Heisenberg frame if and only if *(a)* $\|V_0\|^2 = \dfrac{2}{d+1}$,

(b) $\|V_j\|^2 = \dfrac{1}{d+1}, \quad 1 \le j \le m_d$,

(c) $\langle V_j, V_k\rangle = 0, \quad 0 \le j \ne k \le m_d$.

Proof: First note that $V_{-j} = V_j$. Recall $(U_j)_r = v_r\overline{v_{r+j}}$, and observe

$$(S^{-j}V_j)_r = (V_j)_{r+j} = v_{r+j-j}v_{r+j+j} = v_r v_{r+2j},$$

so that

$$\|V_j\| = \|S^{-j}V_j\| = \|U_{2j}\|.$$

In particular, $\|V_0\| = \|U_0\|$, and so condition (a) is equivalent to that of Theorem 6. Further, the conditions (b) are also equivalent, since if $1 \le j \le \frac{m_d}{2}$, then $2j$ is even, with

$$\|U_{2j}\| = \|V_j\|, \qquad 2 \le 2j \le m_d,$$

and if $\frac{m_d}{2} < j \le m_d$ then $d-2j$ is odd, with

$$\|U_{d-2j}\| = \|U_{-2j}\| = \|V_{-j}\| = \|V_j\|, \qquad 1 \le d-2j \le m_d.$$

Finally,

$$\begin{aligned}
\langle V_j, V_k\rangle &= \sum_r (V_j)_r(\overline{V_k})_r = \sum_r v_{r-j}v_{r+j}\overline{v_{r-k}v_{r+k}} = \sum_r v_{r+j}\overline{v_{r+j+(k-j)}}\,\overline{v_{r-k}\overline{v_{r-k+(k-j)}}} \\
&= \sum_r (U_{k-j})_{r+j}(\overline{U_{k-j}})_{r-k} = \langle S^{-j}U_{k-j}, S^kU_{k-j}\rangle = \langle U_{k-j}, S^{j+k}U_{k-j}\rangle,
\end{aligned}$$

and it follows, by Lemma 7, that the orthogonality conditions are equivalent. $\square$

This gives $1 + m_d + \frac{1}{2}m_d(m_d-1) = 1 + \frac{1}{8}(d^2-1)$ equations.

7 Analytic solutions

We now solve the equivalent equations to find analytic solutions for the primes $d = 2, 3, 5, 7$.

7.1 The case $d = 2$

For $d = 2$, $\omega = -1$, and

$$U_0 = \begin{bmatrix} |v_0|^2 \\ |v_1|^2 \end{bmatrix}, \qquad U_1 = \begin{bmatrix} v_0\overline{v_1} \\ v_1\overline{v_0} \end{bmatrix}, \qquad m_d = 1,$$

so that the equations of Theorem 6 are

$$\|U_0\|^2 = |v_0|^4 + |v_1|^4 = \frac{2}{3}, \qquad \|U_1\|^2 = 2|v_0|^2|v_1|^2 = \frac{1}{3}, \qquad \langle U_1, SU_1\rangle = v_0^2\overline{v_1}^2 + \overline{v_0}^2 v_1^2 = 0.$$

Recalling that the first can be replaced by $|v_0|^2 + |v_1|^2 = 1$, we substitute in the polar form $v_j = r_j e^{\theta_j}$, and solve to get

$$6r_0^4 - 6r_0^2 + 1 = 0, \quad r_0^2 + r_1^2 = 1 \quad \iff \quad r_0^2 = \frac{3 \pm \sqrt{3}}{6}, \quad r_1^2 = \frac{3 \mp \sqrt{3}}{6},$$

$$\cos\bigl(2(\theta_1 - \theta_0)\bigr) = 0 \quad \iff \quad 2(\theta_1 - \theta_0) = \frac{\pi}{2} + \pi n \quad \iff \quad e^{i\theta_1} = e^{i\theta_0} e^{\frac{\pi}{4}i} i^n, \quad n = 0, 1, 2, 3.$$

This gives one solution, up to equivalence. Since [11] were unaware that F maps solutions to solutions, they count two inequivalent solutions v and w, for which we observe

$$w = e^{\frac{\pi}{6}i} F\Omega S v, \qquad v = \frac{1}{\sqrt{6}} \begin{bmatrix} \sqrt{3+\sqrt{3}} \\ e^{\frac{\pi}{4}i}\sqrt{3-\sqrt{3}} \end{bmatrix}, \quad w = \frac{1}{\sqrt{6}} \begin{bmatrix} -\sqrt{3-\sqrt{3}} \\ e^{\frac{\pi}{4}i}\sqrt{3+\sqrt{3}} \end{bmatrix}.$$

It is interesting to observe that there are nonscalar matrices C which map solutions to solutions, but which are *not* in the normaliser of H, e.g.,

$$C := \begin{bmatrix} 1 & \\ & i \end{bmatrix}, \qquad C^*\Omega C = \Omega, \quad C^*SC = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} = i\Omega S.$$

This matrix is in the normaliser of the group $\langle i\rangle H$.

7.2 The case of $d = 3$

Let $d = 3$. This case has some interesting geometric features: it appears to be the only one where there are infinitely many inequivalent solutions (cf [11]). Since

$$V_0 = \begin{bmatrix} v_0^2 \\ v_1^2 \\ v_2^2 \end{bmatrix}, \qquad V_1 = \begin{bmatrix} v_{-1}v_1 \\ v_0v_2 \\ v_1v_0 \end{bmatrix} = \begin{bmatrix} v_2v_1 \\ v_0v_2 \\ v_1v_0 \end{bmatrix}, \qquad m_d = 1,$$

with $r_j := |v_j|$, the equations of Theorem 7 become

(a) $\|V_0\|^2 = r_0^4 + r_1^4 + r_2^4 = \dfrac{1}{2}$,

(b) $\|V_1\|^2 = r_2^2 r_1^2 + r_0^2 r_2^2 + r_1^2 r_0^2 = \dfrac{1}{4}$,

(c) $\langle V_0, V_1 \rangle = \overline{v}_2 \overline{v}_1 v_0^2 + \overline{v}_0 \overline{v}_2 v_1^2 + \overline{v}_1 \overline{v}_0 v_2^2 = 0$.

From (a) and (b), we obtain

$$r_0^4 + r_1^4 + r_2^4 = 1/2 = 2(1/4) = 2(r_0^2 r_1^2 + r_1^2 r_2^2 + r_2^2 r_0^2),$$

which can be rearranged to give

$$r_0^4 + (r_1^4 + 2r_1^2 r_2^2 + r_2^4) - 2r_0^2(r_1^2 + r_2^2) = 4r_1^2 r_2^2.$$

Completing the square on the left yields

$$(r_0^2 - (r_1^2 + r_2^2))^2 = 4r_1^2 r_2^2.$$

We now consider several cases. Firstly, if $r_0^2 \geq r_1^2 + r_2^2$, then taking square roots,

$$r_0^2 - (r_1^2 + r_2^2) = 2r_1 r_2 \quad \Longrightarrow \quad r_0^2 = r_1^2 + 2r_1 r_2 + r_2^2 = (r_1 + r_2)^2 \quad \Longrightarrow \quad r_0 = r_1 + r_2.$$

Secondly, if $r_0^2 < r_1^2 + r_2^2$, then

$$r_0^2 - (r_1^2 + r_2^2) = -2r_1 r_2 \quad \Longrightarrow \quad r_0^2 = r_1^2 - 2r_1 r_2 + r_2^2 = (r_1 - r_2)^2,$$

so that $r_0 = r_1 - r_2$ when $r_1 \geq r_2$, and $r_0 = r_2 - r_1$ when $r_2 \geq r_1$. Thus we have three cases

$$r_0 = r_1 + r_2, \qquad r_1 = r_0 + r_2, \qquad r_2 = r_0 + r_1.$$

From (a) and (b) it follows that $r_0^2 + r_1^2 + r_2^2 = 1$. Hence since $r_j \geq 0$, these three cases describe the three sides of a spherical triangle in the first octant on the unit sphere. The vertices of this triangle are given by the intersections of the three great circles, i.e.,

$$\begin{aligned}
r_0 = r_1 + r_2 \quad &\text{and} \quad r_1 = r_0 + r_2 \quad \Longrightarrow \quad r_0 = r_1 = \tfrac{1}{\sqrt{2}}, r_2 = 0,\\
r_0 = r_1 + r_2 \quad &\text{and} \quad r_2 = r_0 + r_1 \quad \Longrightarrow \quad r_0 = r_2 = \tfrac{1}{\sqrt{2}}, r_1 = 0,\\
r_1 = r_0 + r_2 \quad &\text{and} \quad r_2 = r_0 + r_1 \quad \Longrightarrow \quad r_1 = r_2 = \tfrac{1}{\sqrt{2}}, r_0 = 0.
\end{aligned}$$

We now proceed to equation (c)

$$\overline{v}_2 \overline{v}_1 v_0^2 + \overline{v}_0 \overline{v}_2 v_1^2 + \overline{v}_1 \overline{v}_0 v_2^2 = 0.$$

We consider several cases:

First Vertex $(r_0, r_1, r_2) = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0)$. Since $r_2 = |v_2| = 0$, equation (c) is trivially satisfied, and as there are no other conditions, we have solutions

$$v = \frac{1}{\sqrt{2}} \begin{bmatrix} e^{i\theta} \\ e^{i\phi} \\ 0 \end{bmatrix}, \qquad \theta, \phi \in \mathbb{R}.$$

Similarly, the other vertices give permutations of these solutions.

Second Vertex $(r_0, r_1, r_2) = (\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}})$. Gives solutions

$$v = \frac{1}{\sqrt{2}} \begin{bmatrix} e^{i\theta} \\ 0 \\ e^{i\phi} \end{bmatrix}, \qquad \theta, \phi \in \mathbb{R}.$$

Third Vertex $(r_0, r_1, r_2) = (0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$. Gives solutions

$$v = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ e^{i\theta} \\ e^{i\phi} \end{bmatrix}, \qquad \theta, \phi \in \mathbb{R}.$$

First Triangle Edge $r_0 = r_1 + r_2$, $r_1, r_2 > 0$. For convenience, let $z_j := v_j^2/\overline{v}_j$, so that $|z_j| = |v_j| = r_j$. Then dividing (c) by $\overline{v}_0\overline{v}_1\overline{v}_2$ yields the equivalent equation

$$z_0 + z_1 + z_2 = 0.$$

Since $z_0 = -z_1 - z_2$ and $|z_0| = r_0 = r_1 + r_2 = |-z_1| + |-z_2|$, the complex numbers $z_0, -z_1, -z_2$ must have the same argument, i.e.,

$$z_0 = r_0 e^{i\phi}, \quad z_1 = -r_1 e^{i\phi}, \quad z_2 = -r_2 e^{i\phi}, \qquad \phi \in \mathbb{R}.$$

Hence, writing $v_j = r_j e^{i\theta_j}$, so that $z_j = r_j e^{3i\theta_j}$, we calculate

$$\begin{aligned}
r_0 e^{3i\theta_0} &= r_0 e^{i\phi} &&\implies && \theta_0 = \frac{\phi}{3} + \frac{2\pi}{3}k_0, \quad k_0 = 0, 1, 2, \\
r_1 e^{3i\theta_1} &= -r_1 e^{i\phi} &&\implies && \theta_1 = \frac{\phi}{3} + \frac{\pi}{3} + \frac{2\pi}{3}k_1, \quad k_1 = 0, 1, 2, \\
r_2 e^{3i\theta_2} &= -r_2 e^{i\phi} &&\implies && \theta_2 = \frac{\phi}{3} + \frac{\pi}{3} + \frac{2\pi}{3}k_2, \quad k_2 = 0, 1, 2.
\end{aligned}$$

Since ϕ is arbitrary, so is θ_0. Hence after the change of variables $\theta := (\phi + 2\pi k_0)/3$, we can describe the solutions corresponding to the point (r_0, r_1, r_2) on this edge of the triangle by

$$v_0 = r_0 e^{i\theta}, \quad v_1 = r_1 e^{i\theta} e^{i\frac{\pi}{3}} \omega^{j_1}, \quad v_2 = r_2 e^{i\theta} e^{i\frac{\pi}{3}} \omega^{j_2}, \quad \theta \in \mathbb{R}, \quad j_1, j_2 \in \{0, 1, 2\},$$

where $\omega := e^{\frac{2\pi i}{3}}$. We can give a more precise description of this edge by solving the equations $r_0^2 + r_1^2 + r_2^2 = 1$ and $r_0 = r_1 + r_2$ for r_1, r_2 in terms of r_0, which gives

$$r_1 = \frac{r_0 \pm \sqrt{2 - 3r_0^2}}{2} \quad \text{and} \quad r_2 = \frac{r_0 \mp \sqrt{2 - 3r_0^2}}{2}.$$

Note the half of the edge where $r_1 \geq r_2$ is given by the choice of '+' in the formula for r_1, and the choice '$-$' gives the half with $r_1 \leq r_2$. For these to give $r_1, r_2 > 0$, we must have

$$2 - 3r_0^2 \geq 0, \quad r_0 - \sqrt{2 - 3r_0^2} > 0 \quad \Longleftrightarrow \quad r_0^2 \leq \frac{2}{3}, \quad r_0^2 > \frac{1}{2}.$$

Hence $\frac{1}{2} < r_0^2 \leq \frac{2}{3}$ along this edge, with r_1 and r_2 given by the formula above.

The other edges are similar.

Second Triangle Edge $r_1 = r_0 + r_2,\ r_0, r_2 > 0$. The same as the first edge with the roles of v_0 and v_1 interchanged.

Third Triangle Edge $r_2 = r_0 + r_1,\ r_0, r_1 > 0$. The same as the first edge with the roles of v_0 and v_2 interchanged.

Clearly the diagonal matrices Ω and Q map a solution corresponding to a particular vertex or edge to another such solution, and $\langle S, P_j : j \in \mathbb{Z}_3^+ \rangle$ is the group of six permutation matrices which permute the coordinates of $v \in \mathbb{C}^3$ and hence map a vertex/edge solution to another vertex/edge solution (where the vertex/edge may be different). The action of the Fourier transform matrix

$$F = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix}, \qquad F^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \qquad F^4 = I, \qquad \omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$$

on solutions is much more complicated. Consider it applied to a first vertex solution

$$v = \frac{1}{\sqrt{2}} \begin{bmatrix} e^{i\theta} \\ e^{i\phi} \\ 0 \end{bmatrix}, \quad Fv = \frac{1}{\sqrt{6}} \begin{bmatrix} e^{i\theta} + e^{i\phi} \\ e^{i\theta} + \omega e^{i\phi} \\ e^{i\theta} + \omega^2 e^{i\phi} \end{bmatrix}, \quad F^2 v = \frac{1}{\sqrt{2}} \begin{bmatrix} e^{i\theta} \\ 0 \\ e^{i\phi} \end{bmatrix}.$$

If we choose $\theta = \phi + \pi + \frac{2\pi}{3} j$, then the j–entry of Fv is zero, and we have a vertex solution. Since $(\theta, \phi) \mapsto Fv$ is continuous, it then follows that Fv can be a solution corresponding to any vertex or edge of the triangle by making an appropriate choice of θ and ϕ. It is interesting to observe that such a large set of solutions is given by the simple formula

$$v = \frac{1}{\sqrt{6}} \begin{bmatrix} e^{i\theta} + e^{i\phi} \\ e^{i\theta} + \omega e^{i\phi} \\ e^{i\theta} + \omega^2 e^{i\phi} \end{bmatrix}, \qquad \theta, \phi \in \mathbb{R}.$$

Since F^2 is a permutation, $F^2 v$ is vertex solution, $F^3 v$ is permutation of Fv, and $F^4 v = v$.

7.3 The case $d = 5$

Let $d = 5$, so that

$$\omega = -\frac{1}{4} + \frac{\sqrt{5}}{4} + \frac{1}{4}\sqrt{2}\sqrt{5+\sqrt{5}}i.$$

We find a solution v which is an eigenspace of the element of order three given by

$$A := (FQ^2)^2 = -Q^3 F.$$

This solution was obtained by Zauner [16].

Proposition 8 *If d is odd, then*

$$Q^{\frac{d+1}{2}}F = (-i)^{\frac{d-1}{2}}(FQ^{\frac{d-1}{2}})^2, \qquad (FQ^{\frac{d-1}{2}})^6 = (-1)^{\frac{d-1}{2}}I, \tag{7.1}$$

and hence $Q^{\frac{d+1}{2}}F$ has scalar order 3.

Proof: For d prime (7.1) follows from Theorem 3 and Lemma 5, and for d not prime, the Gauss sums can also be evaluated to obtain the result. Thus $A := Q^{\frac{d+1}{2}}F$ has scalar order three, since

$$A^3 = (Q^{\frac{d+1}{2}}F)^3 = (FQ^{\frac{d+1}{2}})^3 = (-i)^{\frac{d-1}{2}}I.$$

□

Lemma 8 *The matrix $B = FQ^2$ has spectrum $\{\mu, \mu^2, \mu^3, \mu^4, \mu^5\}$, $\mu := e^{\frac{\pi}{3}i} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$. Its orthonormal eigenvectors corresponding to μ and μ^4 are*

$$x := \begin{bmatrix} r_0 \\ r_1\omega^4 \\ -r_2\omega \\ -r_2\omega \\ r_1\omega^4 \end{bmatrix}, \qquad y := \begin{bmatrix} 0 \\ -r_3\omega^4 \\ r_4\omega \\ -r_4\omega \\ r_3\omega^4 \end{bmatrix} \tag{7.2}$$

respectively, where the $r_j > 0$ are given by

$$r_0 = \sqrt{\frac{5+\sqrt{5}}{15}}, \qquad r_1 = \frac{1}{2\sqrt{2}}\left(1 + \sqrt{\frac{5-2\sqrt{5}}{15}}\right), \qquad r_2 = \frac{1}{2\sqrt{2}}\left(1 - \sqrt{\frac{5-2\sqrt{5}}{15}}\right),$$

$$r_3^2 = \frac{1}{4}\left(1 + \sqrt{\frac{5+2\sqrt{5}}{15}}\right), \qquad r_4^2 = \frac{1}{4}\left(1 - \sqrt{\frac{5+2\sqrt{5}}{15}}\right).$$

Proof: The calculations in the original derivation are involved. It is difficult to simplify the surds, e.g.,

$$\sqrt{5} = \omega + \omega^4 - \omega^2 - \omega^3 = 1 + 2(\omega + \omega^4) = -1 - 2(\omega^2 + \omega^3).$$

We note the following eigenvectors with entries from the field $\mathbb{Q}[\omega, \mu]$,

$$\tilde{x} = \begin{bmatrix} 2\omega^3(\sqrt{5}\mu + 1 - w - w^3 + w^4) \\ (\sqrt{5}\mu - 1)(1+\omega) + 2\omega^2 \\ (\sqrt{5}\mu + \omega^2)(\sqrt{5}\mu + \omega^4) + \omega^3 - 2\omega^2 \\ (\sqrt{5}\mu + \omega^2)(\sqrt{5}\mu + \omega^4) + \omega^3 - 2\omega^2 \\ (\sqrt{5}\mu - 1)(1+\omega) + 2\omega^2 \end{bmatrix}, \qquad \tilde{y} = \begin{bmatrix} 0 \\ \omega - 1 \\ \omega^3 - \omega + \sqrt{5}\mu \\ -\omega^3 + \omega - \sqrt{5}\mu \\ 1 - \omega \end{bmatrix},$$

for which

$$\frac{\tilde{x}}{\|\tilde{x}\|} = e^{-\frac{11}{15}\pi i} x, \qquad \frac{\tilde{y}}{\|\tilde{y}\|} = e^{\frac{7}{10}\pi i} y.$$

However, it is easy to verify the result once it is obtained. □

Thus $A = (FQ^2)^2 = B^2$ has a 2–dimensional eigenspace for the eigenvalue $\mu^2 = e^{\frac{2\pi}{3} i}$ with an orthonormal basis given by the vectors x and y of (7.2).

Theorem 9 *Define a complex number*

$$z := \frac{\sqrt{1+\sqrt{3}}}{2\sqrt{2}} \left(\sqrt{\frac{5-\sqrt{5}}{5}} - i\sqrt{\frac{5+\sqrt{5}}{5}} \right).$$

Then the four unit vectors v in the $e^{\frac{2\pi}{3} i}$ eigenspace of A given by

$$v = v_\beta := \alpha x + \beta y, \qquad \alpha = \tfrac{1}{2}\sqrt{3 - \sqrt{3}} = \sqrt{1 - |z|^2}, \quad \beta = z, -z, \overline{z}, -\overline{z}$$

each generate a Heisenberg frame for $\mathbb{C}^5$.

Proof: It is straightforward (but tedious) to check that all the equations are satisfied. We leave the details to the reader who might note that

$$\left(\frac{z}{|z|}\right)^4 = \frac{-3+4i}{5}, \qquad |z|^2 = \frac{1+\sqrt{3}}{4}.$$

□

Observe that the permutation matrix $P_{-1} = F^2$ commutes with A, so if v is a solution in an eigenspace of A, then is $F^2 v$ is a solution in the same eigenspace. In this case

$$F^2 v_z = v_{-z}, \quad F^2 v_{-z} = v_z, \qquad F^2 v_{\overline{z}} = v_{-\overline{z}}, \quad F^2 v_{-\overline{z}} = v_{\overline{z}}.$$

There are two inequivalent solutions in this eigenspace: v_z and $v_{\overline{z}}$, which are conjugate to each other. The following comparison with the numerical results of [11], indicates that these are all of the solutions. In [11] solutions v and w are considered equivalent if

$$v = \alpha U w, \qquad |\alpha| = 1, \quad U \in H.$$

We allow $U \in E$ (and so have fewer equivalence classes). Let E act on the equivalence classes considered in [11]. Then the equivalence class [v] containing v is stabilised by A, $\langle -I \rangle$ (which have orders 3, 2) and by H (of order 125), so that size of its orbit is

$$|\text{Orbit of } [v]| = \frac{|E|}{\text{Stab}([v])} = \frac{30000}{6 \cdot 125} = 40.$$

Taking the conjugate of this orbit gives another 40 solutions, which accounts for the total of 80 (inequivalent) solutions found numerically by [11].

7.4 The case $d = 7$

Let $d = 7$, then the permutation matrix P_2 has order three. We will find a solution v which is an eigenvector P_2 for the eigenvalue 1, i.e., satisfying $v_{2j} = v_j$, $0 \leq j \leq d-1$, which we write as

$$v = \begin{bmatrix} a \\ b \\ b \\ c \\ b \\ c \\ c \end{bmatrix}, \qquad a, b, c \in \mathbb{C}.$$

Consider the equations of Theorem 7, in terms of the vectors V_n, $0 \leq n \leq (d-1)/2 = 3$, defined by $(V_n)_j = v_{j-n} v_{j+n}$.

$$V_0 = \begin{bmatrix} a^2 \\ b^2 \\ b^2 \\ c^2 \\ b^2 \\ c^2 \\ c^2 \end{bmatrix}, \qquad V_1 = \begin{bmatrix} bc \\ ab \\ bc \\ b^2 \\ c^2 \\ bc \\ ac \end{bmatrix}.$$

Since $P_2 v = v$, we have

$$(V_n)_j = v_{j-n} v_{j+n} = v_{2(j-n)} v_{2(j+n)} = v_{2j-2n} v_{2j+2n} = (V_{2n})_{2j},$$

i.e., $V_n = P_2 V_{2n}$ or, equivalently, $V_{2n} = P_2^{-1} V_n = P_2^2 V_n$. Hence we calculate

$$V_2 = P_2^2 V_1, \qquad V_3 = V_{-3} = V_4 = P_2^2 V_2 = P_2^2(P_2^2 V_1) = P_2 V_1.$$

Since V_2, V_3 are permutations of V_1, the equations of Theorem 7 reduce to

(a) $\|V_0\|^2 = \dfrac{2}{d+1}$,

(b) $\|V_1\|^2 = \dfrac{1}{d+1}$,

(c) $\{V_0, V_1, P_2 V_1, P_2^2 V_1\}$ is an orthogonal set.

Using $P_2 V_0 = V_0$ and $P_2^* = P_2^{-1} = P_2^2$, we calculate

$$\langle V_0, P_2 V_1\rangle = \langle P_2^2 V_0, V_1\rangle = \langle V_0, V_1\rangle, \qquad \langle V_0, P_2^2 V_1\rangle = \langle P_2 V_0, V_1\rangle = \langle V_0, V_1\rangle,$$

$$\langle V_1, P_2^2 V_1\rangle = \overline{\langle P_2^2 V_1, V_1\rangle} = \overline{\langle V_1, P_2 V_1\rangle}, \qquad \langle P_2 V_1, P_2^2 V_1\rangle = \langle V_1, P_2^4 V_1\rangle = \langle V_1, P_2 V_1\rangle.$$

Hence $\{V_0, V_1, P_2 V_1, P_2^2 V_1\}$ is an orthogonal set if and only if $\langle V_0, V_1\rangle = 0$, $\langle V_1, P_2 V_1\rangle = 0$. Consequently, the equations we must solve are:

(1) $\|V_0\|^2 = 1/4 : \quad |a|^4 + 3|b|^4 + 3|c|^4 = 1/4$

(2) $\|V_1\|^2 = 1/8 : \quad 3|b|^2|c|^2 + |b|^4 + |c|^4 + |a|^2|b|^2 + |a|^2|c|^2 = 1/8$

(3) $\langle V_0, V_1\rangle = 0 : \quad \overline{b}\overline{c}a^2 + \overline{a}|b|^2 b + c|b|^2 b + \overline{b}^2 c^2 + \overline{c}^2 b^2 + \overline{b}|c|^2 c + \overline{a}|c|^2 c = 0$

(4) $\langle V_1, P_2 V_1\rangle = 0 : \quad |b|^2|c|^2 + a|b|^2\overline{c} + b|c|^2\overline{c} + b^2\overline{ac} + c^2\overline{a}\overline{b} + c|b|^2\overline{b} + a|c|^2\overline{b} = 0.$

Consider the first two equations in $|a|, |b|, |c|$. The first minus twice the second gives

$$|a|^4 - 2|a|^2(|b|^2 + |c|^2) + |b|^4 + |c|^4 - 6|b|^2|c|^2 = 0,$$

which may be expressed as

$$(|a|^2 - (|b|^2 + |c|^2))^2 = 8|b|^2|c|^2,$$

so that

$$|a|^2 - (|b|^2 + |c|^2) = \pm 2\sqrt{2}|b||c|. \tag{7.3}$$

Now a solution will satisfy $\|v\|^2 = |a|^2 + 3(|b|^2 + |c|^2) = 1$. From this subtract (7.3) to get

$$4(|b|^2 + |c|^2) = 1 \mp 2\sqrt{2}|b||c|. \tag{7.4}$$

Now we make a simplifying assumption, that $b, c \in \mathbb{R}$. Since we may multiply a solution by a scalar to get an equivalent solution this is effectively the condition $b/c \in \mathbb{R}$. The equations (3),(4) become

(3) $\langle V_0, V_1\rangle = 0: \quad a^2bc + \overline{a}(b^3+c^3) + bc(b+c)^2 = 0$

(4) $\langle V_1, P_2V_1\rangle = 0: \quad bc(bc + (a+\overline{a})(b+c) + b^2 + c^2) = 0$. In view of (7.3), $bc = 0$ does not yield a solution and so (4) simplifies to (4) $\langle V_1, P_2V_1\rangle = 0: \quad bc + (a+\overline{a})(b+c) + b^2 + c^2 = 0$.

Let $a = x + iy$, then (by taking real and imaginary parts) we have *five* real equations in the *four* real variables x, y, b, c.

Since $a + \overline{a} = 2x$, solving (4) for x gives

$$x = -\frac{b^2 + c^2 + bc}{2(b+c)}. \tag{7.5}$$

Here we cannot have $b + c = 0$, since substituting this into (3) gives $a^2bc = 0$, which doesn't yield a solution. Next expand equation (3)

$$(x^2 - y^2 + 2ixy)bc + (x - iy)(b^3 + c^3) + bc(b+c)^2 = 0,$$

and take its imaginary part to obtain

$$y(2xbc - (b^3 + c^3)) = 0. \tag{7.6}$$

We now treat the two cases: $y \neq 0$ and $y = 0$.

Case $y \neq 0$: Solving (7.6) gives

$$x = \frac{b^3 + c^3}{2bc}. \tag{7.7}$$

Comparing (7.5) and (7.7), we have

$$\frac{b^3 + c^3}{2bc} + \frac{b^2 + c^2 + bc}{2(b+c)} = 0$$

so that

$$(b+c)(b^3 + c^3) + bc(b^2 + c^2 + bc) = (b^2 + c^2 + bc)^2 - 2b^2c^2 = 0.$$

Solving $(b^2 + c^2 + bc)^2 = 2b^2c^2$, gives

$$b^2 + c^2 = (-1 \pm \sqrt{2})bc = (-1 + \sqrt{2}\delta)bc, \qquad \delta \in \{-1, 1\}. \tag{7.8}$$

Given that $b, c \in \mathbb{R}$, we may rewrite (7.4) as

$$4(b^2 + c^2) = 1 + 2\sqrt{2}\varepsilon bc, \qquad \varepsilon \in \{-1, 1\}. \tag{7.9}$$

Solving (7.8) and (7.9) for $b^2 + c^2$ and bc gives

$$b^2 + c^2 = \frac{1}{4}\frac{\sqrt{2}\varepsilon - 2 + 2\delta(2\delta - \varepsilon)}{(2\delta - \varepsilon)^2 - 2}, \qquad bc = \frac{1}{4}\frac{\sqrt{2}(2\delta - \varepsilon) + 2}{(2\delta - \varepsilon)^2 - 2}.$$

Multiply top and bottom by $-\delta\varepsilon$ to make the denominators positive

$$b^2+c^2=\frac{1}{4}\frac{-\sqrt{2}\delta-2\delta\varepsilon+2}{4-3\delta\varepsilon},\qquad bc=\frac{1}{4}\frac{\sqrt{2}(\delta-2\varepsilon)-2\delta\varepsilon}{4-3\delta\varepsilon},$$

and combine to obtain

$$(b\pm c)^2=b^2+c^2\pm 2bc=\frac{1}{4}\frac{2-2\delta\varepsilon(1\pm 2)+\sqrt{2}(-\delta\pm 2\delta\mp 4\varepsilon)}{4-3\delta\varepsilon}.$$

The values $(b+c)^2$ and $(b-c)^2$ given by this formula are both nonnegative only if $\delta=-1$, which gives

$$(b+c)^2=\frac{1}{4}\frac{2+6\varepsilon+\sqrt{2}(-1-4\varepsilon)}{4+3\varepsilon},\qquad (b-c)^2=\frac{1}{4}\frac{2-2\varepsilon+\sqrt{2}(3+4\varepsilon)}{4+3\varepsilon}.$$

Since multiplying v by the scalar -1 gives an equivalent solution, we may assume that $b+c>0$, and since the permutation matrix $P_{-1}=F^2$ maps v to another solution with the b and c interchanged, we may further assume that $b>0$ and $b>c$, i.e., $b-c>0$, giving

$$b+c=2\alpha,\qquad \alpha=\frac{1}{4\sqrt{4+3\varepsilon}}\sqrt{2+6\varepsilon-\sqrt{2}(1+4\varepsilon)}>0,$$
$$b-c=2\beta,\qquad \beta=\frac{1}{4\sqrt{4+3\varepsilon}}\sqrt{2-2\varepsilon+\sqrt{2}(3+4\varepsilon)}>0.$$

We therefore have

$$b=\alpha+\beta,\qquad c=\alpha-\beta,$$

where the possible values of α and β are

$$\alpha=\frac{\sqrt{3\sqrt{2}-4}}{4},\quad \beta=\frac{\sqrt{4-\sqrt{2}}}{4}\quad(\varepsilon=-1),\qquad \alpha=\frac{\sqrt{8-5\sqrt{2}}}{4\sqrt{7}},\quad \beta=\frac{\sqrt[4]{2}}{4}\quad(\varepsilon=1).$$

The choice $\varepsilon=-1$ does not lead to a solution, since this implies

$$3(b^2+c^2)=3((\alpha+\beta)^2+(\alpha-\beta)^2)=6(\alpha^2+\beta^2)=\frac{3}{4}\sqrt{2}>1,$$

contradicting $\|v\|^2=|a|^2+3(b^2+c^2)=1$. For choice $\varepsilon=1$, we determine the possible values of a. Using equation (4) to eliminate $\overline{a}$ from (3), gives

$$(bc)\,a^2+(-b^3-c^3)\,a+(b^3c+bc^3+c^2b^2-b^4-c^4)=0,$$

which is a quadratic in a with real coefficients. Solving this in the form

$$(\alpha^2-\beta^2)\,a^2-2\alpha(\alpha^2+3\beta^2)\,a+(\alpha^4-3\beta^4-14\alpha^2\beta^2)=0,$$

leads to a complex conjugate pair of solutions

$$a=-\frac{\sqrt{8-5\sqrt{2}}(2\sqrt{2}+1\pm 7i)}{2\sqrt{7}(3\sqrt{2}-2)}\approx -0.31093791\mp 0.56852731i,\quad \arg(a)\approx\mp 118.68^\circ.$$

With the values of b, c given below, this gives inequivalent solutions

$$b = \frac{1}{4}\left(\frac{\sqrt{8-5\sqrt{2}}}{\sqrt{7}} + \sqrt[4]{2}\right), \qquad c = \frac{1}{4}\left(\frac{\sqrt{8-5\sqrt{2}}}{\sqrt{7}} - \sqrt[4]{2}\right).$$

Case $y = 0$: Substitute (7.5), with $x = a$, into equation (3), and factor to obtain

$$-\frac{(2b^2+3bc+2c^2)(b^4-2b^3c-5b^2c^2-2bc^3+c^4)}{4(b+c)^2} = 0.$$

Since the quadratic form $(b, c) \mapsto 2b^2 + 3bc + 2c^2$ is positive definite, we must have

$$b^4 - 2b^3c - 5b^2c^2 - 2bc^3 + c^4 = (b^2+c^2)^2 - 2bc(b^2+c^2) - 7b^2c^2 = 0.$$

Solving the above quadratic in $b^2 + c^2$ gives

$$b^2+c^2 = \frac{2bc \pm \sqrt{4b^2c^2 + 28b^2c^2}}{2} = (1\pm 2\sqrt{2})bc = (1+2\sqrt{2}\delta)bc, \qquad \delta \in \{-1, 1\}. \quad (7.10)$$

Solving (7.9) and (7.10) for $b^2 + c^2$ and bc gives

$$b^2 + c^2 = \frac{2\sqrt{2}+\delta}{2(4\sqrt{2}+2\delta-\sqrt{2}\varepsilon\delta)}, \qquad bc = \frac{\delta}{2(4\sqrt{2}+2\delta-\sqrt{2}\varepsilon\delta)},$$

and so

$$(b \pm c)^2 = b^2 + c^2 \pm 2bc = \frac{2\sqrt{2}+\delta\pm 2\delta}{2(4\sqrt{2}+2\delta-\sqrt{2}\varepsilon\delta)}.$$

The values $(b \pm c)^2$ given by this formula are both nonnegative only if $\delta = 1$, which gives

$$(b+c)^2 = \frac{2\sqrt{2}+3}{2(4\sqrt{2}+2-\sqrt{2}\varepsilon)}, \qquad (b-c)^2 = \frac{2\sqrt{2}-1}{2(4\sqrt{2}+2-\sqrt{2}\varepsilon)}.$$

As in the previous case, we may assume wlog that $b + c > 0$, $b - c > 0$, so that

$$b = \alpha+\beta, \quad c = \alpha-\beta, \qquad \alpha = \frac{\sqrt{2\sqrt{2}+3}}{2\sqrt{2}\sqrt{4\sqrt{2}+2-\sqrt{2}\varepsilon}}, \qquad \beta = \frac{\sqrt{2\sqrt{2}-1}}{2\sqrt{2}\sqrt{4\sqrt{2}+2-\sqrt{2}\varepsilon}}.$$

The choice $\varepsilon = -1$ does not lead to a solution, and for $\varepsilon = 1$, we get

$$\alpha = \frac{\sqrt{2\sqrt{2}+3}}{2\sqrt{2}\sqrt{3\sqrt{2}+2}} = \frac{\sqrt{6+5\sqrt{2}}}{4\sqrt{7}}, \qquad \beta = \frac{\sqrt{2\sqrt{2}-1}}{2\sqrt{2}\sqrt{3\sqrt{2}+2}} = \frac{\sqrt{2-\sqrt{2}}}{4},$$

which gives a solution, with the $a = x$ obtained from (7.5) as

$$a = -\frac{\sqrt{3\sqrt{2}-2}}{2\sqrt{7}}.$$

Theorem 10 *For $d = 7$, there are three inequivalent vectors of the form*

$$v = (a, b, b, c, b, c, c)^T, \qquad a \in \mathbb{C}, \quad b, c \in \mathbb{R}$$

which generate a Heisenberg frame for $\mathbb{C}^7$, namely the pair of conjugate solutions given by

$$a = -\frac{\sqrt{8-5\sqrt{2}}(2\sqrt{2}+1 \pm 7i)}{2\sqrt{7}(3\sqrt{2}-2)}, \quad b = \frac{\sqrt{8-5\sqrt{2}}}{4\sqrt{7}} + \frac{\sqrt[4]{2}}{4}, \quad c = \frac{\sqrt{8-5\sqrt{2}}}{4\sqrt{7}} - \frac{\sqrt[4]{2}}{4},$$

and the all real solution given by

$$a = -\frac{\sqrt{3\sqrt{2}-2}}{2\sqrt{7}}, \qquad b = \frac{\sqrt{6+5\sqrt{2}}}{4\sqrt{7}} + \frac{\sqrt{2-\sqrt{2}}}{4}, \qquad c = \frac{\sqrt{6+5\sqrt{2}}}{4\sqrt{7}} - \frac{\sqrt{2-\sqrt{2}}}{4}.$$

Proof: Since the above system of equations solved above was over determined, we need to check the solutions derived above satisfy *all* the equations. This is easily done.

A numerical calculation shows the orbits of the above solutions under E are distinct, and so these solutions are not equivalent. □

These solutions were obtained independently by [2]. Due to the nature of his derivation he was unaware that there is a *real solution* (an equivalent solution with complex entries was given). Since the number variables involved in a real solution is halved, such solutions (if they exist in higher dimensions) should in principle be easier to find.

We now count the number of times [11] count vectors in the E–orbit of the above v as different solutions. Since each v is stabilised by P_2, $\langle i \rangle$ and H, this is

$$|\text{Orbit of } [v]| = \frac{|E|}{\text{Stab}([v])} = \frac{460992}{3 \cdot 4 \cdot 7^3} = 112.$$

Since our three solutions are inequivalent they account for all the $336 = 3 \times 112$ solutions found numerically by [11].

References

[1] Apostol, T. M. Introduction to analytic number theory, Springer (New York), 1976.

[2] Appleby, D. M., *Symmetric informationally complete–positive operator valued measures and the extended Clifford group*, J. Math. Phys., 46, 2005, 1–27.

[3] Davis, P. J., Circulant matrices, Wiley (New York), 1979.

[4] Eldar, Y. C., Forney, G. D., *Optimal Tight Frames and Quantum Measurement*, IEEE Trans. Inform. Theory, 48, 2002, 599–610.

[5] Hoggar, S. G., 64 *lines from a quaternionic polytope*, Geom. Dedicata, 69 no.- 3, 1998, 287–289.

[6] Klappenecker, A., Rötteler, M., *Mutually Unbiased Bases are Complex Projective* 2*–designs*, preprint, 2005.

[7] König, H., Cubature formulas on spheres; Math. Res., 107, 1999, 201–211.

[8] Lemmens, P. W. H., Seidel, J. J., *Equiangular lines*, J. Algebra, 24, 1973, 494–512.

[9] Lyubich, Yu. I., Shatalova, O. A., *Isometric embeddings of finite-dimensional* ℓ_p*-spaces over the quaternions*, Algebra i Analiz, 16, 2004, 15–32.

[10] Renes, J. M.; Frames, Designs, and Spherical Codes in Quantum Information Theory, University of New Mexico, 2004.

[11] Renes, J. M., Blume–Kohout, R., Scott, A. J., Caves, C. M., *Symmetric informationally complete quantum measurements*, J. Math. Phys., 45, 2004, 2171–2180.

[12] Seidel, J. J., *Definitions for spherical designs*, J. Statist. Plann. Inference, 95 no. 1–2, 2001, 307–313.

[13] Vale, R., Waldron, S., *The vertices of the platonic solids are tight frames*, (Advances in constructive approximation: Vanderbilt 2003), M. Neamtu and E. B. Saff (eds.), Nashboro Press (Brentwood, TN), 2004, 495–498.

[14] Waldron, S., *Generalized Welch bound equality sequences are tight frames*, IEEE Trans. Inform. Theory, 49, 2003, 2307–2309.

[15] Welch, L. R., *Lower Bounds on the Maximum Cross Correlation of Signals*, IEEE Trans. Inform. Theory, 20, 1974, 397–399.

[16] Zauner, G. Ph. D. Thesis (Quantendesigns Grundzüge einer nichtkommutativen Designtheorie) University of Vienna, 1999.