J Algebr Comb (2008) 28: 333–349
DOI 10.1007/s10801-007-0104-1

On Weyl-Heisenberg orbits of equiangular lines

Mahdad Khatirinejad

Received: 9 May 2007 / Accepted: 25 October 2007 / Published online: 6 November 2007

Abstract An element $\mathbf{z} \in \mathbb{CP}^{d-1}$ is called fiducial if $\{\mathbf{gz} : \mathbf{g} \in G\}$ is a set of lines with only one angle between each pair, where $G \cong \mathbb{Z}_d \times \mathbb{Z}_d$ is the one-dimensional finite Weyl-Heisenberg group modulo its centre. We give a new characterization of fiducial vectors. Using this characterization, we show that the existence of almost flat fiducial vectors implies the existence of certain cyclic difference sets. We also prove that the construction of fiducial vectors in prime dimensions 7 and 19 due to Appleby (J. Math. Phys. 46(5):052107, 2005) does not generalize to other prime dimensions (except for possibly a set with density zero). Finally, we use our new characterization to construct fiducial vectors in dimension 7 and 19 whose coordinates are real.

Keywords Complex equiangular lines · Weyl-Heisenberg group · Fiducial vector · SIC-POVM

1 Introduction

One of the most challenging problems in algebraic combinatorics is finding large sets of lines with few angles between the pairs. In particular, the problem of finding equiangular lines in real and complex spaces is still wide open. In this paper, we only work with lines which lie in complex space $\mathbb{C}^d$, unless stated otherwise. A line in $\mathbb{C}^d$ is an element in the complex projective space $\mathbb{CP}^{d-1}$, the space of one-dimensional complex vector subspaces of $\mathbb{C}^d$. Each element in $\mathbb{CP}^{d-1}$ can be represented by a unit vector $\mathbf{u}$ in $\mathbb{C}^d$. Note that such a representation is not unique since $\lambda\mathbf{u}$ with $|\lambda| = 1$ represents the same line. In the rest of the paper, we only work with the unit vectors

Research supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).

M. Khatirinejad (✉)
Department of Mathematics, Simon Fraser University, Burnaby, BC, V5A 1S6, Canada
e-mail: mahdad@math.sfu.ca

in $\mathbb{C}^d$ to represent a line. The cosine of the angle between the lines spanned by unit vectors $\mathbf{u}, \mathbf{v} \in \mathbb{C}^d$ is defined as $|\mathbf{u}^*\mathbf{v}|$, the absolute value of their inner product. A set of lines in $\mathbb{C}^d$ spanned by unit vectors $\mathbf{v}_1, \dots, \mathbf{v}_k$ is *equiangular* if there exists a constant α such that $|\mathbf{v}_i^*\mathbf{v}_j| = \alpha$ for every $1 \le i < j \le k$. It is not hard to show that if X is a set of equiangular lines in $\mathbb{C}^d$ then $|X| \le d^2$. If $|X| = d^2$ then X is called a maximum set of equiangular lines. If such a maximum set exists then we must have $\alpha = 1/\sqrt{d+1}$. To the best of our knowledge, such maximum sets are presented in [2, 10–13, 17] for $2 \le d \le 10$ and $d \in \{12, 19\}$. In addition, it is claimed in [7] (with reference to private communication with Markus Grassl) that such sets also exist for $d \in \{11, 13, 15\}$. Mostly, the proof that such given sets are equiangular is not published, as it may generally require pages of tedious algebra to give a complete proof. Nevertheless, the problem is still open for a general d:

Problem 1.1 For any positive integer d, does there exist a set of d^2 equiangular lines in $\mathbb{C}^d$?

Throughout the paper, let $\{\mathbf{e}_j : j \in \mathbb{Z}_d\}$ be the standard basis for $\mathbb{C}^d$, and let ω be a d-th primitive root of unity in $\mathbb{C}$. The coordinates of a vector $\mathbf{z} \in \mathbb{C}^d$ are always indexed by $\mathbb{Z}_d$, the set of integers modulo d. When there is no confusion, we will write (z_j) instead of $(z_j)_{j\in\mathbb{Z}_d}$ to represent $\mathbf{z}$. The conjugate of an element $x \in \mathbb{C}$ is denoted by $\bar{x}$ and $\mathbf{A}^*$ denotes the conjugate transpose of a complex valued matrix $\mathbf{A}$. The *Pauli matrices* for $\mathbb{Z}_d$ are defined by their action on the standard basis as follows:

$$\mathbf{X}_k : \mathbf{e}_j \mapsto \mathbf{e}_{j+k},$$
$$\mathbf{Y}_k : \mathbf{e}_j \mapsto \omega^{jk}\mathbf{e}_j,$$

where $k \in \mathbb{Z}_d$. The group $\mathrm{GP}(d) = \langle \mathbf{X}_j, \mathbf{Y}_k : j, k \in \mathbb{Z}_d\rangle$ is usually called the *generalized Pauli group* or the *one-dimensional finite Weyl-Heisenberg group*. Define

$$\mathcal{H}_d = \mathrm{GP}(d)/Z(\mathrm{GP}(d)),$$

where $Z(G)$ denotes the centre of G. Observe that the quotient group $\mathcal{H}_d = \{\mathbf{X}_j\mathbf{Y}_k\langle\omega\mathbf{I}_d\rangle : j, k \in \mathbb{Z}_d\}$ is isomorphic to $\mathbb{Z}_d \times \mathbb{Z}_d$, where $\mathbf{I}_d$ denotes the identity matrix of order d. All of the known constructions of maximum sets of equiangular lines have the form $\{\mathbf{X}_j\mathbf{Y}_k\mathbf{z} : j, k \in \mathbb{Z}_d\}$ for some $\mathbf{z} \in \mathbb{C}^d$ (except for the set of 64 lines in $\mathbb{C}^8$ constructed by Hoggar [12], in which the group $\mathbb{Z}_2^3$ is used instead of $\mathbb{Z}_8$).

Definition 1.2 *A vector* $\mathbf{z} \in \mathbb{C}^d$ *is called* fiducial *if* $\{\mathbf{g}\mathbf{z} : \mathbf{g} \in \mathcal{H}_d\}$ *is a set of equiangular lines.*

It is widely believed that for every d there exists a fiducial vector in $\mathbb{C}^d$ (for example see [2, 7, 9, 11, 13, 17]). The set of d^2 equiangular lines in $\mathbb{C}^d$ has been discussed in different contexts. For example, in quantum information theory it is a *symmetric informationally complete positive operator valued measure (SIC-POVM)*, which is composed of d^2 rank-one operators all of whose operator inner products are equal. In the quantum information theory community, there has been notable interest to construct such SIC-POVMs in every dimension and most of the focus has been on SIC-POVMs which are invariant under the Weyl-Heisenberg group (i.e. the SIC-POVMs that arise from fiducial vectors). Equiangular lines have several applications to quantum information such as quantum fingerprinting [15] , quantum tomography [5] and quantum cryptographic protocols [8]. They also play a role in the Bayesian formulation of the quantum mechanics [5, 8] where they make nice standard quantum measurements. Equiangular lines have also been studied in the context of spherical codes and designs [6].

In Section 2 we will present a new characterization of fiducial vectors (Theorem 2.2) which plays an essential role in the rest of the paper. In Sections 3, 4, and 5, we study three types of fiducial vectors which are closely related: *almost flat, argument Legendre*, and *real Legendre*. Using the new characterization, we show that the existence of almost flat fiducial vectors implies the existence of certain cyclic difference sets. The fiducial vectors in dimensions 7 and 19 constructed by Appleby [2] are examples of the argument Legendre fiducial vectors. We prove that the construction of these vectors does not generalize to other prime dimensions (except for possibly a set with density zero). We also use our new characterization to construct fiducial vectors in dimension 7 and 19 whose coordinates are real. Finally, a concise fact regarding the non-existence of a general fiducial vector is discussed in Section 6.

A note about the proofs: To sustain the flow of the paper we have moved the proofs of some of the theorems to the Appendix.

2 The characterizing identities

One of the interesting properties of a set of equiangular lines of the form $\{\mathbf{gz} : \mathbf{g} \in G\}$ is that with certain assumptions on G, instead of checking the equality of $\binom{|G|}{2}$ inner products, one may only need to check $|G|$ of them:

Observation 2.1 *Let G be any set of matrices that is closed under matrix multiplication and the conjugate transpose operator. Assume G contains the identity matrix $\mathbf{I}$ and let $\mathbf{z}$ be a vector. Then $\{\mathbf{gz} : \mathbf{g} \in G\}$ is a set of equiangular lines if and only if $|\mathbf{z}^*\mathbf{gz}| = c$ for every $\mathbf{g} \in G \setminus \{\mathbf{I}\}$ and $|\mathbf{z}^*\mathbf{z}| = 1$. Here c is the cosine of the common angle between the lines.*

Note that $\mathcal{H}_d$, introduced above, is closed under matrix multiplication and the conjugate transpose operator and also contains the identity matrix.

For a given dimension d, by definition, fiducial vectors form the set of all roots of a system of multivariate polynomials in $z_0, \ldots, z_{d-1}, \bar{z}_0, \ldots, \bar{z}_{d-1}$ over the field $\mathbb{Q}(\omega)$. The following theorem shows that one may only consider $\mathbb{Q}$ instead of $\mathbb{Q}(\omega)$ and it gives a different characterization of fiducial vectors.

Theorem 2.2 *A vector* $\mathbf{z} = (z_j) \in \mathbb{C}^d$ *is fiducial if and only if for every* $(s,t) \in \mathbb{Z}_d \times \mathbb{Z}_d$ *the following identities hold*:

$$f_{s,t}(\mathbf{z}) := \sum_{j\in\mathbb{Z}_d} z_j \bar{z}_{j+s} \bar{z}_{j+t} z_{j+s+t} = \begin{cases} 0 & \textit{for } s,t \neq 0, \\ \frac{1}{d+1} & \textit{for } s \neq 0,\ t = 0 \textit{ or } s = 0,\ t \neq 0, \\ \frac{2}{d+1} & \textit{for } s = t = 0. \end{cases}$$

Proof For every $k \in \mathbb{Z}_d$ we have $\mathbf{X}_s \mathbf{Y}_k \mathbf{z} = (z_{j+s}\omega^{k(j+s)})$. Thus $\mathbf{z}^* \mathbf{X}_s \mathbf{Y}_k \mathbf{z} = \sum_{j\in\mathbb{Z}_d} \bar{z}_j z_{j+s} \omega^{k(j+s)}$. This implies that

$$\begin{aligned} |\mathbf{z}^* \mathbf{X}_s \mathbf{Y}_k \mathbf{z}|^2 &= \left(\sum_{j\in\mathbb{Z}_d} z_j \bar{z}_{j+s} \omega^{-k(j+s)}\right)\left(\sum_{j'\in\mathbb{Z}_d} \bar{z}_{j'} z_{j'+s} \omega^{k(j'+s)}\right) \\ &= \sum_{j,j'\in\mathbb{Z}_d} z_j \bar{z}_{j+s} \bar{z}_{j'} z_{j'+s} \omega^{k(j'-j)} \\ &= \sum_{t\in\mathbb{Z}_d} \sum_{j\in\mathbb{Z}_d} z_j \bar{z}_{j+s} \bar{z}_{j+t} z_{j+t+s} \omega^{kt} \\ &= f_s\left(w^k\right), \end{aligned}$$

where $f_s(x) = \sum_{t=0}^{d-1} f_{s,t}(\mathbf{z}) x^t$. It follows that the vector $\mathbf{z}$ is fiducial if and only if

$$f_s\left(\omega^k\right) = \begin{cases} 1 & \text{for } (s,k) = (0,0), \\ \frac{1}{d+1} & \text{for } (s,k) \neq (0,0). \end{cases} \tag{1}$$

Let $\Omega_d = \{x \in \mathbb{C} : x^d = 1\}$. For $s = 0$, the above identity holds if and only if $f_0(x) - 1/(d+1)$ vanishes on $\Omega_d \setminus \{1\}$ and $f_0(1) = 1$, that is $\sum_{t\in\mathbb{Z}_d} f_{0,t}(\mathbf{z}) = 1$. For every $s \neq 0$, identity (1) holds if and only if $f_s(x) - 1/(d+1)$ vanishes on Ω_d. Since $f_s(x) - 1/(d+1)$ is a polynomial of degree at most $d-1$, this is equivalent to the fact that $f_s(x)$ is identically equal to zero. That is $f_{s,t}(\mathbf{z}) = 0$ when $t \neq 0$, and $f_{s,0}(\mathbf{z}) = 1/(d+1)$. Since $f_{s,t}(\mathbf{z}) = f_{t,s}(\mathbf{z})$, by combining the above cases, we get the desired result. □

Remark. We have noted that the above theorem has also been discovered independently in [3], a few months after the original submission of this article.

Remark. For every $s,t \in \mathbb{Z}_d$, we have $f_{s,t}(\mathbf{z}) = f_{t,s}(\mathbf{z}) = \overline{f_{s,-t}(\mathbf{z})}$. Therefore the set $\mathbb{Z}_d \times \mathbb{Z}_d$ in Theorem 2.2 can be replaced with the set:

$$\{(s,t) \in \mathbb{Z}_d \times \mathbb{Z}_d : 0 \le s \le t \le \lfloor d/2 \rfloor\}.$$

As an immediate corollary, we get the following necessary conditions for a vector to be fiducial:

Corollary 2.3 *Let* $\mathbf{z} = (r_j e^{i\theta_j})$, *where* $r_j \in \mathbb{R}$ *and* $\theta_j \in [0, 2\pi)$, *be a fiducial vector in* $\mathbb{C}^d$. *Then the following identities hold*:

$$\sum_{j \in \mathbb{Z}_d} r_j^2 r_{j+s}^2 = \begin{cases} \frac{1}{d+1} & \textit{for } s \in \mathbb{Z}_d \setminus \{0\}, \\ \\ \frac{2}{d+1} & \textit{for } s = 0. \end{cases} \tag{2}$$

Remark Note that the set $\{\mathbf{X}_0\mathbf{Y}_k\mathbf{z} : k \in \mathbb{Z}_d\}$ is equiangular if and only if (2) holds, and also note that $\{\mathbf{X}_0\mathbf{Y}_k\langle\omega\mathbf{I}_d\rangle : k \in \mathbb{Z}_d\}$ is a subgroup of $\mathcal{H}_d$ isomorphic to $\mathbb{Z}_d$. Therefore, the equiangular condition test for this set is independent of the argument values of the coordinates of $\mathbf{z}$ and it is only dependent on their absolute values.

A note on equiangular vectors A set of vectors in $\mathbb{R}^d$ is called equiangular if the inner product between every two distinct vectors in the set is a constant. Note the difference between equiangular vectors and equiangular lines where we require the absolute value of the inner products to be a constant. Now, assume that $\mathbf{z} = (r_j e^{i\theta_j})$, where $r_j \in \mathbb{R}$ and $\theta_j \in [0, 2\pi)$, is a fiducial vector in $\mathbb{C}^d$. Also, let $\mathbf{x} = (\sqrt{\frac{d+1}{2}} r_j^2)$. Then, using Corollary 2.3, one may observe that $S = \{\mathbf{x}, \mathbf{X}_1\mathbf{x}, \ldots, \mathbf{X}_{d-1}\mathbf{x}\}$ is a set of d equiangular vectors on the unit sphere in $\mathbb{R}^d$ with common angle 60°. Note that the set S is unique up to a unitary transformation $\mathbf{Q}$. This is because the matrix whose set of columns is S can be decomposed to $\mathbf{QR}$, where $\mathbf{Q}$ is a unitary and $\mathbf{R}$ is an upper triangular matrix.

In the following three sections, we will treat three types of fiducial vectors: *almost flat, argument Legendre*, and *real Legendre*. The argument Legendre fiducial vectors are almost flat and are discussed by Appleby [2] in specific dimensions. Since the real Legendre fiducial vectors have very similar properties to the argument Legendre ones and also all of the coordinates of such vectors have the same argument, we have also investigated this class of fiducial vectors.

3 Almost flat fiducial vectors

A vector in $\mathbb{C}^d$ is called *flat* if all its coordinates have the same absolute value. It is proved [9] that there are at most $d^2 - d + 1$ flat equiangular lines in $\mathbb{C}^d$ (and there are exactly $d^2 - d + 1$ such lines when $d - 1$ is a prime power). In particular, no flat fiducial vectors exist (this can also be concluded easily from Corollary 2.3). To take it one step further, we say a vector is *almost flat* if it is flat except for one coordinate. Appleby [2] constructed fiducial vectors in dimensions 7 and 19 which are almost flat. Using an eigenvalue argument, Roy [14] proved that for almost flat fiducial vectors in $\mathbb{C}^d$, the absolute values of the coordinates are determined in terms of d. We provide an alternative proof of this fact here:

Theorem 3.1 *Let* $\mathbf{z}$ *be a fiducial vector in* $\mathbb{C}^d$ *such that one coordinate of* $\mathbf{z}$ *has absolute value* b, *and all other coordinates have absolute value* a. *Then*

$$a^2 = \frac{1 \mp 1/\sqrt{d+1}}{d}, \qquad b^2 = \frac{1 \pm (d-1)/\sqrt{d+1}}{d}.$$

Proof Since $\mathbf{z}$ is a unit vector, we have $b^2 + (d-1)a^2 = 1$. By letting $s = 0$ in Corollary 2.3, we get $b^4 + (d-1)a^4 = 2/(d+1)$. Solving for a^2 and b^2, we get the stated values. □

Remark. Note that $(a^2, b^2) = ((1 + 1/\sqrt{d+1})/d, (1 - (d-1)/\sqrt{d+1})/d)$ is only possible for $d \leq 3$, since we must have $a^2, b^2 \geq 0$.

In fact, we can prove a stronger result. Namely, the existence of a cyclic difference set in $\mathbb{Z}_d$ is a necessary condition for the existence of fiducial vectors in which the coordinates take exactly two distinct absolute values. Before stating the result, recall that a (d, k, λ)-*cyclic difference set* is a set $D = \{\alpha_1, \ldots, \alpha_k\} \subseteq \mathbb{Z}_d$ such that each element in $\mathbb{Z}_d \setminus \{0\}$ can be represented as a difference $\alpha_i - \alpha_j$ in exactly λ different ways (see for example [4]). The proof of the following theorem is given in Appendix B.

Theorem 3.2 *Let $a \neq b$ be real numbers and k, d be integers such that $0 < k \leq d/2$. Let $\mathbf{z} = (z_j) \in \mathbb{C}^d$ be a fiducial vector such that k coordinates of $\mathbf{z}$ have absolute value b, and all other coordinates have absolute value a. Let $D = \{j \in \mathbb{Z}_d : |z_j| = b\}$. Then*

$$a^2 = \frac{1}{d}\left(1 \mp \sqrt{\frac{k(d-1)}{(d+1)(d-k)}}\right), \qquad b^2 = \frac{1}{d}\left(1 \pm \sqrt{\frac{(d-k)(d-1)}{k(d+1)}}\right),$$

and D forms a (d, k, λ)-cyclic difference set in $\mathbb{Z}_d$. In particular, $d-1$ must divide $k(k-1)$.

Remark. Note that $(a^2, b^2) = ((1 + \sqrt{k(d-1)/(d+1)/(d-k)})/d,\ (1 - \sqrt{(d-k)(d-1)/(d+1)/k})/d)$ is only possible for $d \leq 2k+1$.

4 Argument Legendre fiducial vectors

Let p denote a prime number. For every $j \in \mathbb{Z}_p$ let $\left(\frac{j}{p}\right)$ denote the Legendre symbol, that is $\left(\frac{j}{p}\right)$ is 0 (respectively 1 or -1) if $j = 0$ (respectively if j is a quadratic or a non-quadratic residue).

Definition 4.1 *We say a fiducial vector $\mathbf{z} = (z_j) \in \mathbb{C}^p$ is argument Legendre* (AL) *if there exist $a, b, \theta \in \mathbb{R}$ such that*

$$z_j = \begin{cases} b & \textit{if } j = 0, \\ ae^{i\left(\frac{j}{p}\right)\theta} & \textit{if } j \neq 0. \end{cases}$$

Note that AL fiducial vectors are almost flat. Thus, by Theorem 3.1 and its succeeding remark, if $p > 3$ then we must have $a^2 = (1 - 1/\sqrt{p+1})/p$ and $b^2 = (1 + (p-1)/\sqrt{p+1})/p$. In fact, if an AL fiducial vector exists, then the value of θ is also determined in terms of p:

Proposition 4.2 *Let $p > 3$ such that $p \equiv 3 \pmod 4$. If $\mathbf{z} \in \mathbb{C}^p$ is an AL fiducial vector with parameters (a, b, θ) then*

$$\theta = \begin{cases} \cos^{-1}(1/\sqrt{2+\sqrt{p+1}}) & \textit{for } p \equiv 3 \pmod 8, \\ \cos^{-1}(-\sqrt{\frac{2+\sqrt{p+1}}{p+1}}) & \textit{for } p \equiv 7 \pmod 8. \end{cases} \tag{3}$$

The proof of this proposition is rather long and technical and is given in the Appendix. By using Theorem 2.2 it is easy to check that the vector $(\sqrt{2/3}, e^{i\pi/3}/\sqrt{6}, e^{-i\pi/3}/\sqrt{6})$ is an AL fiducial vector in $\mathbb{C}^3$. The construction of AL fiducial vectors in $\mathbb{C}^7$ and $\mathbb{C}^{19}$ is given by Appleby in [2]. However, a proof that the given vectors are in fact fiducial is not given in his work. One may interpret that the proofs are basic but require some extensive tedious algebra. We will give a short proof that Appleby's vectors [2] are fiducial:

Theorem 4.3 *AL fiducial vectors exist for $p = 7$ and $p = 19$.*

Proof Let $f_{s,t}(\mathbf{z})$ be as defined in Theorem 2.2. Recall from Theorem 2.2 (and the remark following it) that an AL fiducial vector $\mathbf{z} \in \mathbb{C}^p$ with parameters a, b, and $c = \cos\theta$ exists if and only if the system of equations

$$\begin{aligned} f_{0,0}(\mathbf{z}) - 2/(p+1) = f_{0,r}(\mathbf{z}) - 1/(p+1) = f_{s,t}(\mathbf{z}) = 0, \\ \text{where } 0 < r \le \lfloor p/2 \rfloor \text{ and } 0 < s \le t \le \lfloor p/2 \rfloor, \end{aligned} \tag{4}$$

has a solution. If $p = 7$, we may easily verify that

$$\begin{aligned} f_{0,0}(\mathbf{z}) &= 6a^4 + b^4, \\ f_{0,1}(\mathbf{z}) = f_{0,2}(\mathbf{z}) = f_{0,3}(\mathbf{z}) &= 5a^4 + 2a^2b^2, \\ f_{1,1}(\mathbf{z}) = f_{2,2}(\mathbf{z}) = f_{3,3}(\mathbf{z}) &= 4a^4c^2(4c^2-3) + a^2b^2 + 2a^3bc, \\ f_{1,2}(\mathbf{z}) = f_{1,3}(\mathbf{z}) = f_{2,3}(\mathbf{z}) &= 4a^4c^2 - a^4 + 4a^3bc(2c^2-1). \end{aligned}$$

It is therefore straightforward to check that the system (4) has a solution for $p = 7$ when

$$a = \sqrt{\tfrac{4-\sqrt{2}}{28}}, \quad b = \sqrt{\tfrac{2+3\sqrt{2}}{14}}, \quad c = \cos\theta = -\tfrac{\sqrt{\sqrt{2}+1}}{2}.$$

(the values of a, b, and θ are taken from Theorem 3.1 and Proposition 4.2.)

Analogously for $p = 19$, we have

$$\begin{aligned} f_{0,0}(\mathbf{z}) &= 18a^4 + b^4, \\ f_{0,r}(\mathbf{z}) &= 17a^4 + 2a^2b^2, \\ f_{r,r}(\mathbf{z}) &= 16a^4c^2(2c^2-1) + a^2b^2 + 2a^3bc(4c^2-3), \\ f_{r,2r}(\mathbf{z}) = f_{r,7r}(\mathbf{z}) &= a^4(16c^4 - 4c^2 + 3) + 4a^3bc(2c^2-1), \\ f_{r,3r}(\mathbf{z}) = f_{r,4r}(\mathbf{z}) &= 4a^4c^2 - a^4 + 4a^3bc(2c^2-1), \end{aligned}$$

for all $r \in \mathbb{Z}_{19}$ such that $1 \le r \le 9$. A straightforward evaluation at

$$a=\sqrt{\tfrac{10-\sqrt{5}}{190}},\quad b=\sqrt{\tfrac{5+9\sqrt{5}}{95}},\quad c=\cos\theta=\sqrt{\tfrac{\sqrt{5}-1}{8}},$$

shows that the system (4) has a solution for $p=19$. □

Using MAPLE, Roy [14] confirms (numerically) that there are no other AL fiducial vectors for $p\le 400$. We conjecture that AL fiducial vectors only exist for $p\in\{3,7,19\}$. Except for a set of primes with density zero, we are able to confirm this conjecture:

Theorem 4.4 *There exists a set of primes $\mathcal{P}$ with zero density* (*in the set of all primes that are equal to* 3 *modulo* 4) *such that for all $p\notin\mathcal{P}$ there exists no AL fiducial vector in $\mathbb{C}^p$.*

In fact, in the proof of Theorem 4.4, we will see that $\mathcal{P}$ is the set of primes $p>7$ such that $a(p)=-3$ and $p\equiv 11$ or $19 \pmod{24}$, where $a(p)$ denotes the trace of the Frobenius endomorphism of the elliptic curve $y^2=x(x+1)(x+2)(x+3)$:

$$a(p)=-\sum_{x\in\mathbb{Z}_p}\left(\frac{x(x+1)(x+2)(x+3)}{p}\right).$$

The fact that the set $\mathcal{P}$ has density zero follows from Theorem 20 in [16].

5 Real fiducial vectors

We say a fiducial vector $\mathbf{z}$ of dimension d is *real* if $\mathbf{z}\in\mathbb{R}^d$.

Example 5.1 By Theorem 2.2, a vector $\mathbf{z}=(a,b,c)\in\mathbb{R}^3\subset\mathbb{C}^3$ is fiducial if and only if $a^4+b^4+c^4-1/2=a^2b^2+b^2c^2+c^2a^2-1/4=abc(a+b+c)=0$. It is easy to see that $(0,1/\sqrt{2},1/\sqrt{2})$ is a solution to this system and is thus a real fiducial vector.

It seems that real fiducial vectors rarely exist as the assumption $\mathbf{z}\in\mathbb{R}^d$ is rather strong. On the other hand, searching for such fiducial vectors should be easier since one needs to deal with less parameters. In fact, the number of unknown real parameters in a real fiducial vector in $\mathbb{C}^d$ is only d compared to the number of unknown real parameters in a general fiducial vector in $\mathbb{C}^d$ which is $2d-1$ (we may always assume $z_0\in\mathbb{R}$). Despite this fact, we are able to find real fiducial vectors in dimension 7 and 19 where the coordinates only take 3 distinct values.

It would be quite interesting to know whether real fiducial vectors in dimensions other than 3, 7, and 19 exist. In this section, we will discuss a special type of real fiducial vectors (called real Legendre) which have similar characteristics to the argument Legendre fiducial vectors.

5.1 Real Legendre fiducial vectors

Let p be a prime number. We call a fiducial vector $\mathbf{z}=(z_j)\in\mathbb{C}^p$ *real Legendre (RL)* if there exist $a,b,c\in\mathbb{R}$ such that

$$z_j=\begin{cases} a & \text{if } j=0,\\ b & \text{if } \left(\frac{j}{p}\right)=1,\\ c & \text{if } \left(\frac{j}{p}\right)=-1.\end{cases}$$

In the next two theorems, we will show that real Legendre fiducial vectors exist for $p\in\{7,19\}$.

Theorem 5.2 *Let* $\{\pm a\}$ *be the set of real roots of* $56x^4+8x^2-1$ *and let* $\{\pm b,\pm c\}$ *be the set of real roots of* $3136x^8-2240x^6+568x^4-56x^2+1$ *with* $a<0<b,c$. *Then the RL vector* $\mathbf{z}=(a,b,b,c,b,c,c)\in\mathbb{R}^7$ *is a fiducial vector in* $\mathbb{C}^7$.

Proof By Theorem 2.2, the vector $\mathbf{z}\in\mathbb{R}^7$ is fiducial if and only if (a,b,c) is a solution to the following system

$$\begin{aligned} f_{0,0}(\mathbf{z}) &= a^4+3(b^4+c^4)=1/4,\\ f_{0,1}(\mathbf{z})=f_{0,2}(\mathbf{z})=f_{0,3}(\mathbf{z}) &= a^2(b^2+c^2)+b^4+c^4+3b^2c^2=1/8,\\ f_{1,1}(\mathbf{z})=f_{2,2}(\mathbf{z})=f_{3,3}(\mathbf{z}) &= (2a(b+c)+b^2+c^2+bc)bc=0,\\ f_{1,2}(\mathbf{z})=f_{1,3}(\mathbf{z})=f_{2,3}(\mathbf{z}) &= a^2bc+a(b^3+c^3)+bc(b+c)^2=0.\end{aligned}$$

Let $I=\langle f_{0,0}(\mathbf{z})-1/4, f_{0,1}(\mathbf{z})-1/8, f_{1,1}(\mathbf{z}), f_{1,2}(\mathbf{z})\rangle$. Using a computer algebra system, such as MAPLE, we may find the Gröbner basis G_c of I with respect to the pure lexicographic monomial order induced by $a>b>c$. We observe that $G_c=\{h(c), b-f(c), a-g(c)\}$, where

$$\begin{aligned} h(x)&=3136x^8-2240x^6+568x^4-56x^2+1,\\ f(x)&=-8/23\,x(784x^6-707x^4+184x^2-14),\\ g(x)&=-1/23\,x(9408x^6-3976x^4+276x^2+39).\end{aligned}$$

Hence $h(c)\in I$ and we must have $h(c)=0$. Similarly, we get $h(b)=0$ and $56a^4+8a^2-1=0$. Now, since $h(0)=1>0$ and $h(1/4)<0$, we may assume $c\in(0,1/4)$. On the interval $(0,1/4)$, we have $f(x)>0$ and $g(x)<0$. Therefore $b=f(c)>0$ and $a=g(c)<0$. □

Remark. Since every fiducial vector has unit length, we have added the polynomial $a^2+3b^2+3c^2-1$ to the set of generators of I to reduce the degree of the polynomials in the Gröbner bases.

Theorem 5.3 *Let* $\{\pm a\}$ *be the set of real roots of* $76x^4+10x^2-5$ *and let* $\{\pm b,\pm c\}$ *be the set of real roots of* $144400x^8-34200x^6+3640x^4-160x^2+1$ *with* $b<0<a,c$. *Then the RL vector in* $\mathbb{C}^{19}$ *with parameters* (a,b,c) *is a fiducial vector.*

Proof The given RL vector $\mathbf{z} \in \mathbb{R}^{19}$ is fiducial if and only if (a, b, c) is a solution to the following system:

$$\begin{aligned}
f_{0,0}(\mathbf{z}) &= a^4 + 9(b^4 + c^4) = 1/10,\\
f_{0,1}(\mathbf{z}) &= a^2(b^2 + c^2) + 4(b^4 + c^4) + 9\,b^2c^2 = 1/20,\\
f_{1,1}(\mathbf{z}) &= abc(a + b + c) + 2(b + c)^2(b^2 + c^2) = 0,\\
f_{1,2}(\mathbf{z}) &= 2\,abc(b + c) + b^4 + 3\,b^3c + 7\,b^2c^2 + 3\,bc^3 + c^4 = 0,\\
f_{1,3}(\mathbf{z}) &= a(b + c)(b^2 + c^2) + 5bc(b^2 + bc + c^2) = 0.
\end{aligned}$$

The rest of the proof is similar to the proof of Theorem 5.2. □

Remark. As in dimension 7, adding the polynomial $a^2 + 9\,b^2 + 9\,c^2 - 1$ to the set of generators of I would reduce the degree of the polynomials in the Gröbner bases.

The following result is an analogous version of Theorem 4.4 for RL vectors:

Theorem 5.4 *There exists a set of primes $\mathcal{P}$ with zero density* (*in the set of all primes that are equal to* 3 *modulo* 4) *such that for all $p \notin \mathcal{P}$ there exists no RL fiducial vector in $\mathbb{C}^p$.*

Since the proof of the above theorem is similar to that of Theorem 4.4 and only involves some basic algebra, we have omitted the proof. However, in the proof of the Theorems 4.4 and 5.4, one can see that the exact same set $\mathcal{P}$ satisfies the conditions of these two theorems. This strongly suggests that one may find a one to one correspondence between the set of AL fiducial vectors and the set of RL fiducial vectors. If such a transformation is found then the proof of one of the mentioned theorems can be skipped. Now let us look at a crucial group for which a fiducial vector is invariant. We will discuss briefly why such a transformation (if any) cannot be in this group.

Let $\mathrm{C}(d)$ denote the *Clifford group*, the group of all unitary operations $\mathbf{U}$ which normalize the generalized Pauli group $\mathrm{GP}(d)$, i.e. $\mathbf{U}\,\mathrm{GP}(d)\,\mathbf{U}^* = \mathrm{GP}(d)$. Let $\mathbf{J}$ be the mapping that maps $(z_j) \in \mathbb{C}^d$ to $(\bar{z_j})$. The *extended Clifford group* is the group consisting of $\mathrm{C}(d)$ and all elements of the form $\mathbf{JU}$, where $\mathbf{U} \in \mathrm{C}(d)$. This group is denoted by $\mathrm{EC}(d)$. The relevance of the (extended) Clifford group to the set of equiangular lines arising from $\mathrm{GP}(d)$ has been discussed by several authors (for example see [2, 10]). Note that if $\mathbf{z}$ is a fiducial vector and $\mathbf{U} \in \mathrm{EC}(d)$ then $\mathbf{Uz}$ is also a fiducial vector. Therefore $\mathrm{EC}(d)$ lies in the automorphism group of the set of fiducial vectors in $\mathbb{C}^d$. Appleby [2] proves that for odd d the group $\mathrm{EC}(d)$ modulo its centre $\mathrm{I}(d)$ is isomorphic to the group $\mathrm{ESL}(2, \mathbb{Z}_d) \wr (\mathbb{Z}_d \times \mathbb{Z}_d)$, where $\mathrm{ESL}(2, \mathbb{Z}_d)$ denotes the group of all 2×2 matrices over $\mathbb{Z}_d$ with determinant equal to ± 1 and $\wr$ denotes the wreath product. On page 17 in [2], Appleby also describes a method to find the stability group of a given fiducial vector $\mathbf{z} \in \mathbb{C}^d$, the set of all $\mathbf{U} \in \mathrm{EC}(d)/\mathrm{I}(d)$ for which $\mathbf{z}$ is eigenvector. Applying the same method, it turns out that the stability group of the RL fiducial vector in dimension 7 (from Theorem 5.2) is isomorphic to the order 3 subgroup generated by

$$\left[\begin{pmatrix} -3 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} -3 \\ 0 \end{pmatrix}\right].$$

But the stability group of the AL fiducial vector in dimension 7 (from Theorem 4.3) is isomorphic to the order 6 subgroup (see [2]) generated by

$$[\begin{pmatrix} -2 & 0 \\ 0 & -3 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix}],$$

and therefore the two AL and RL fiducial vectors in dimension 7 do not belong to the same orbit under the action of the extended Clifford group. Therefore, the transformation discussed in the previous paragraph cannot be found in $\mathrm{EC}(d)$. Similar argument shows that the two AL and RL fiducial vectors in dimension 19 do not belong to the same orbit under the action of the extended Clifford group. In fact, the stability group of the RL fiducial vector in dimension 19 (from Theorem 5.3) is isomorphic to the order 9 subgroup generated by

$$[\begin{pmatrix} 9 & 0 \\ 0 & -2 \end{pmatrix}, \begin{pmatrix} 11 \\ 0 \end{pmatrix}],$$

whereas the stability group of the AL fiducial vector in dimension 19 (from Theorem 4.3) is isomorphic to the order 18 subgroup (see [2]) generated by

$$[\begin{pmatrix} -9 & 0 \\ 0 & -2 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix}].$$

6 Periodic fiducial vectors

We say that a sequence $(a_j)_{j\in\mathbb{Z}_d}$ is *periodic* if there exists $p \in \mathbb{Z}_d \setminus \{0\}$ such that $a_{j+p} = a_j$ for every $j \in \mathbb{Z}_d$. The smallest such p is called the *period* of the sequence.

Proposition 6.1 *There exists no fiducial vector in $\mathbb{C}^d$ such that the absolute values of its coordinates form a periodic sequence.*

Proof Towards a contradiction assume that such a fiducial vector, namely $\mathbf{z} = (z_j)$, exists. Let p be the period of the sequence $(|z_j|^2)_{j\in\mathbb{Z}_d}$ and let $d = pk$ for some integer $k > 1$. For $j = 0 \ldots p-1$, let $R_j = |z_j|^2$. It follows from Corollary 2.3 that

$$\sum_{j=0}^{p-1} R_j R_{j+s} = \begin{cases} \frac{1}{k(pk+1)} & \text{for } 1 \le s \le p-1, \\ \frac{2}{k(pk+1)} & \text{for } s = 0. \end{cases}$$

We also know that $\sum_{j=0}^{p-1} R_j = 1/k$. By substituting the above values in the identity $(\sum_j R_j)^2 = \sum_j R_j^2 + \sum_{i\neq j} R_i R_j$, we get

$$\frac{1}{k^2} = \frac{2}{k(pk+1)} + (p-1)\cdot\frac{1}{k(pk+1)}.$$

Simplifying the above equation, we get $k = 1$, which is a contradiction. □

Acknowledgements The author thanks Petr Lisoněk for fruitful discussions and acknowledges Noam Elkies for his valuable comments. The author also thanks the referees for their useful remarks.

Appendix

Here we present the technical, yet interesting, details that were skipped throughout the paper. In Section A we provide some necessary tools and state some properties of the Legendre symbol which will be used in the proof of theorems presented in Section B.

A Properties of the Legendre symbol

For every $j \in \mathbb{Z}_p$ recall that $\left(\frac{j}{p}\right)$ denotes the Legendre symbol. The basic properties of the Legendre symbol can be found in almost any introductory number theory textbook (for example see [1]). Also recall that $a(p)$ denotes the trace of the Frobenius endomorphism of the elliptic curve $y^2 = x(x+1)(x+2)(x+3)$:

$$a(p) = -\sum_{j\in\mathbb{Z}_p}\left(\frac{j(j+1)(j+2)(j+3)}{p}\right).$$

The following lemma is quite straightforward, but we include it for the sake of completeness:

Lemma A.1 *For every prime p such that $p \equiv 3 \pmod 4$, we have*

(i) $\sum_{j\in\mathbb{Z}_p}\left(\frac{j}{p}\right) = 0$,

(ii) $\sum_{j\in\mathbb{Z}_p}\left(\frac{j(j+\epsilon)}{p}\right) = -1$ *for every fixed* $\epsilon \in \mathbb{Z}_p \setminus \{0\}$,

(iii) $\sum_{j\in\mathbb{Z}_p}\left(\frac{(j-\epsilon)j(j+\epsilon)}{p}\right) = 0$ *for every fixed* $\epsilon \in \mathbb{Z}_p$.

Proof Since $p \equiv 3 \pmod 4$ we have $\left(\frac{-x}{p}\right) = -\left(\frac{x}{p}\right)$. This immediately implies (i) and (iii). Since the Legendre symbol is multiplicative we get $\sum_{j\in\mathbb{Z}_p}\left(\frac{j(j+\epsilon)}{p}\right) = \sum_{j\in\mathbb{Z}_p\setminus\{0\}}\left(\frac{1+\epsilon j^{-1}}{p}\right) = -\left(\frac{1}{p}\right) = -1$ by (i). □

In the next three lemmas, we count the number of fixed points of certain maps on $\mathbb{Z}_p$ that involve the Legendre symbol $\left(\frac{j}{p}\right)$. The lemmas are very similar, but none of them quite implies another one and therefore we have included them all. However, since the proofs are similar, we have only presented one of the proofs. The key idea in all of them is to count the number of elements of the set $\{j \in \mathbb{Z}_p : (\left(\frac{j}{p}\right), \left(\frac{j+1}{p}\right), \ldots, \left(\frac{j+t-1}{p}\right)) = C\}$ for every given constant $C \in \{-1, 1\}^t$. We will do this for $t = 2$, $t = 3$, and $t = 4$, respectively, in the next three lemmas.

Lemma A.2 *For every prime p such that $p \equiv 3 \pmod 4$, and $j \in \mathbb{Z}_p$, let*

$$\kappa(j) = \left(\frac{j}{p}\right) - \left(\frac{j+1}{p}\right).$$

Also let $K(c)=|\{j:\kappa(j)=c\}|$. *Then*

$$K(0)=\tfrac{1}{2}(p-3),\quad K(2)=\tfrac{1}{4}(p+1),\quad K(-2)=\tfrac{1}{4}(p-3).$$

Proof For every $\alpha=(\alpha_0,\alpha_1)\in\{-1,1\}\times\{-1,1\}$, let

$$k_p(\alpha)=\frac{1}{4}\sum_{j\in\mathbb{Z}_p\setminus\{0,-1\}}\left(\alpha_0\left(\frac{j}{p}\right)+1\right)\left(\alpha_1\left(\frac{j+1}{p}\right)+1\right).$$

By applying Lemma A.1, we get

$$\begin{aligned}4k_p(\alpha)&=(p-\alpha_0\alpha_1)-\left(\alpha_1\left(\frac{1}{p}\right)+1\right)-\left(\alpha_0\left(\frac{-1}{p}\right)+1\right)\\&=p-2-\alpha_0\alpha_1+\alpha_0-\alpha_1.\end{aligned}\tag{5}$$

On the other hand, for every $\delta\in\{-1,1\}$ and $x\neq 0$, the value of the expression $(1/2)\left(\delta\left(\frac{x}{p}\right)+1\right)$ is equal to 1 if $\left(\frac{x}{p}\right)=\delta$ and 0 otherwise. Therefore $k_p(\alpha)=|\{j\in\mathbb{Z}_p:\left(\frac{j}{p}\right)=\alpha_0,\left(\frac{j+1}{p}\right)=\alpha_1\}|$. Hence $K(0)=k_p(1,1)+k_p(-1,-1)$, $K(2)=k_p(1,-1)$, and $K(-2)=k_p(-1,1)$. The result follows immediately using (5). □

Lemma A.3 *For every prime* p *such that* $p\equiv 3\pmod 4$, *and* $j\in\mathbb{Z}_p$, *let*

$$\mu(j)=2\left(\frac{j}{p}\right)-\left(\frac{j-1}{p}\right)-\left(\frac{j+1}{p}\right).$$

Also let $M(c)=|\{j:\mu(j)=c\}|$. *Then*

$$M(0)=\begin{cases}\frac{1}{4}(p-3) & \textit{for } p\equiv 3\pmod 8,\\[2ex] \frac{1}{4}(p-7) & \textit{for } p\equiv 7\pmod 8,\end{cases}$$

$$M(2)=M(-2)=\frac{1}{4}(p-3),$$

$$M(4)=M(-4)=\begin{cases}\frac{1}{8}(p-3) & \textit{for } p\equiv 3\pmod 8,\\[2ex] \frac{1}{8}(p+1) & \textit{for } p\equiv 7\pmod 8.\end{cases}$$

Remark. Note that the equality $k_p(\alpha_0,\alpha_1)=m_p(1,\alpha_0,\alpha_1)+m_p(-1,\alpha_0,\alpha_1)$ does not necessarily hold, where

$$m_p(\beta,\alpha_0,\alpha_1)=\frac{1}{8}\sum_{j\in\mathbb{Z}_p\setminus\{0,\pm1\}}\left(\beta\left(\frac{j-1}{p}\right)+1\right)\left(\alpha_0\left(\frac{j}{p}\right)+1\right)\left(\alpha_1\left(\frac{j+1}{p}\right)+1\right).$$

This is why Lemma A.2 can not be implied from Lemma A.3.

Lemma A.4 *For every prime p such that $p \equiv 3 \pmod 4$, and $j \in \mathbb{Z}_p$, let*

$$\nu(j) = \left(\frac{j+3}{p}\right) - \left(\frac{j+2}{p}\right) - \left(\frac{j+1}{p}\right) + \left(\frac{j}{p}\right).$$

Also let $N(c) = |\{j : \nu(j) = c\}|$. Then

$$N(0) = \frac{1}{8}\left(3p - 10 - 3a(p) - 2(\left(\frac{2}{p}\right) + 1)(\left(\frac{3}{p}\right) + 1)\right),$$

$$N(2) = N(-2) = \frac{1}{4}(p - 4 + a(p)),$$

$$N(4) = N(-4) = \frac{1}{16}\left(p - 6 - a(p) + 2(\left(\frac{2}{p}\right) + 1)(\left(\frac{3}{p}\right) + 1)\right),$$

where

$$a(p) = -\sum_{j\in\mathbb{Z}_p}\left(\frac{j(j+1)(j+2)(j+3)}{p}\right).$$

B The proofs

Proof of Theorem 3.2 By letting $s = 0$ in Corollary 2.3 and the fact that $\mathbf{z}$ is a unit vector, it follows that

$$kb^2 + (d-k)a^2 = 1, \qquad kb^4 + (d-k)a^4 = 2/(d+1).$$

It is easy to see that if $k = 0$ then no a and b exist. Thus $k \geq 1$ and $d \geq 2$. Solving for a^2 and b^2, we get

$$a^2 = \frac{1}{d}\left(1 \mp \sqrt{\frac{k(d-1)}{(d+1)(d-k)}}\right), \qquad b^2 = \frac{1}{d}\left(1 \pm \sqrt{\frac{(d-k)(d-1)}{k(d+1)}}\right).$$

Hence

$$(a^2 - b^2)^2 = \frac{d-1}{d^2(d+1)}\left(\frac{k}{d-k} + \frac{d-k}{k} + 2\right) = \frac{d-1}{(d+1)(d-k)k}. \tag{6}$$

Let $N_s(x, y) = |\{i \in \mathbb{Z}_d : |z_i| = x, |z_{i+s}| = y\}|$. Since there are k coordinates that have absolute value b and $d-k$ coordinates that have absolute value a, we have

$$N_s(b,b) + N_s(b,a) = \quad k \quad = N_s(b,b) + N_s(a,b). \tag{7}$$

$$N_s(a,a) + N_s(a,b) = d-k = N_s(a,a) + N_s(b,a). \tag{8}$$

On the other hand, by Corollary 2.3 we have

$$N_s(a,a)a^4 + N_s(b,b)b^4 + (N_s(a,b) + N_s(b,a))a^2b^2 = \frac{1}{d+1}$$

for every $s \in \mathbb{Z}_d \setminus \{0\}$. Thus, by using identities (7) and (8), this can be rewritten as $(N_s(b,b)-k)(a^2-b^2)^2 = -1/(d+1)$. Substituting identity (6) implies that

$$N_s(b,b) = k - \frac{(d-k)k}{d-1} = \frac{k(k-1)}{d-1} := \lambda$$

is independent of s. By definition of D and $N_s(b,b)$, this means that every $s \in \mathbb{Z}_d \setminus \{0\}$ can be represented as a difference of two distinct elements of D in exactly λ different ways. □

Proof of Proposition 4.2 Let $c = \cos\theta$, $\delta = \sqrt{p+1}$, and $\psi = \sqrt{\delta+2}$. By Theorem 3.1, we have $a = 1/\sqrt{\delta(\delta+1)}$ and $b = \psi/\sqrt{\delta(\delta+1)}$. By definition, we must have $|\sum_{j\in\mathbb{Z}_p} z_j \bar{z}_{j+1}|^2 = 1/(p+1)$. Using Lemma A.2 and Lemma A.3, we may rewrite this as

$$(2bc + (p-1)ac^2 - a)^2 + 4(1-c^2)(b-ac)^2 = 1/a^2(p+1).$$

By making the above substitutions for a, b, p, and δ and factoring out the non-zero terms, the previous expression can be written as

$$(\psi c - 1)\left((\psi^2-2)c+\psi\right)\left((\psi^2-2)(\psi^2-4)c^2 + 2\psi c + \psi^2 - 6\right) = 0. \qquad (9)$$

Let $f_{s,t}(\mathbf{z})$ be as defined in Theorem 2.2. Using Lemma A.3 and Lemma A.4, we get

$$f_{1,-1}(\mathbf{z}) = \begin{cases} a^4(p-3)c^2(2c^2-1) + 2a^3b(4c^3-3c) + a^2b^2 & \text{for } p \equiv 3 \pmod 8 \\ a^4c^2(p(2c^2-1)+2c^2-5) + 2a^3bc + a^2b^2 & \text{for } p \equiv 7 \pmod 8 \end{cases}$$

Note that $f_{1,-1}(\mathbf{z}) = 0$ by Theorem 2.2. As before, both polynomials on the left hand side can be factored in $\mathbb{R}[\psi]$. After factoring out the non-zero terms, we get the following: If $p \equiv 3 \pmod 8$ then

$$(\psi c - 1)\left(2(\psi^2-4)c^3 + 2\psi c^2 - (\psi^2-6)c - \psi\right) = 0. \qquad (10)$$

It is easy to check that for $p > 3$, the only common root of the equations (9) and (10) is $c = 1/\psi$. Therefore $\theta = \cos^{-1}(1/\sqrt{2+\sqrt{p+1}})$, as desired. If $p \equiv 7 \pmod 8$ then

$$\left((\psi^2-2)c+\psi\right)\left(2(\psi^2-2)c^3 - 2\psi c^2 - (\psi^2-4)c + \psi\right) = 0. \qquad (11)$$

The only common root of the equations (9) and (11) is $c = -\psi/(\psi^2-2)$ and therefore we must have $\theta = \cos^{-1}(-\sqrt{\frac{2+\sqrt{p+1}}{p+1}})$ in this case. □

Remark. For $p > 19$ the quadratic factor in equation (9) is always positive. Therefore equation (9) simplifies to $(\psi c - 1)\left((\psi^2-2)c+\psi\right) = 0$ for $p > 19$.

Proof of Theorem 4.4 Let $\mathbf{z} = (z_j)$ be an AL fiducial vector in $\mathbb{C}^p$ with parameters $a, b, c = \cos\theta$. We already know that such vector exists for $p = 3$ and $p = 7$. So assume $p > 7$. As in the proof of Proposition 4.2, by letting $\delta = \sqrt{p+1}$, and $\psi = \sqrt{\delta + 2}$ we get $a = 1/\sqrt{\delta(\delta+1)}$ and $b = \psi a$. Also, by Proposition 4.2 we have $c = 1/\psi$ if $p \equiv 3 \pmod 8$ and $c = -\psi/(\psi^2 - 2)$ if $p \equiv 7 \pmod 8$. Now, by letting $q = a(p)$ and using Lemma A.3 and Lemma A.4 we get the following: If $p \equiv 23 \pmod{24}$ then

$$f_{1,2}(\mathbf{z}) = (p + 2 - q)a^4c^4 + 2(q-3)a^4c^2 + 4a^3bc - qa^4$$

and if $p \not\equiv 23 \pmod{24}$ then

$$f_{1,2}(\mathbf{z}) = (p - 6 - q)a^4c^4 + 8a^3bc^3 + 2(q+1)a^4c^2 - 4a^3bc - qa^4.$$

By Theorem 2.2, we must have $f_{1,2}(\mathbf{z}) = 0$. Since a, b, c and p can be described in terms of ψ, we can describe $f_{1,2}(\mathbf{z})$ in terms of q and ψ. Solving for q, we get:

$$q = a(p) = \begin{cases} -3 & \text{for } p \equiv 11 \text{ or } 19 \pmod{24} \\ -\psi^2(3\psi^2 - 8)/(\psi^2 - 4)^2 & \text{for } p \equiv 23 \pmod{24} \\ \psi^2(5\psi^2 - 24)/(\psi^2 - 4)^2 & \text{for } p \equiv 7 \pmod{24} \end{cases}$$

For $p \equiv 23 \pmod{24}$ we can easily check that q is not an integer (in fact, if $p = 24\ell + 23$ and $\ell > 13$ then $-4 < q < -3$). This is impossible since $q = a(p)$ is an integer by definition. Similarly, the case $p \equiv 7 \pmod{24}$ when $p \neq 7$ is excluded. Thus the set

$$\mathcal{P} = \{p : p \text{ is prime}, p \equiv 11 \text{ or } 19 \pmod{24},\ p > 7,\ a(p) = -3\}$$

has the desired properties. As mentioned before, the fact that the set $\mathcal{P}$ has density zero follows from Theorem 20 in [16]. □

Remark. By considering the identity $f_{1,4}(\mathbf{z}) = 0$ in the previous theorem, we may further restrict the forbidden set $\mathcal{P}$ to its proper subset $\{p \in \mathcal{P} | a'(p) = -3\}$, where $a'(p) = -\sum_{j \in \mathbb{Z}_p} \left(\frac{j(j+1)(j+4)(j+5)}{p}\right)$. Since this subset of $\mathcal{P}$ is still non-empty and has the same density as $\mathcal{P}$, namely zero, we have skipped the details.

References

1. Andrews, G.E.: Number Theory. Dover, New York (1994)
2. Appleby, D.M.: Symmetric informationally complete-positive operator valued measures and the extended Clifford group. J. Math. Phys. **46**(5), 052107 (2005)
3. Appleby, D.M., Dang, H.B., Fuchs, C.A.: Physical significance of symmetric informationally-complete sets of quantum states. Preprint arXiv:0707.2071v1 (2007)
4. Baumert, L.D., Gordon, D.M.: On the existence of cyclic difference sets with small parameters. In: High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams. Fields Inst. Commun., vol. 41, pp. 61–68. Amer. Math. Soc., Providence (2004)
5. Caves, C.M., Fuchs, C.A., Schack, R.: Unknown quantum states: the quantum de finetti representation. J. Math. Phys. **43**, 4537–4559 (2002)
6. Delsarte, P., Goethals, J.M., Seidel, J.J.: Spherical codes and designs. Geom. Dedicata **6**(3), 363–388 (1977)

7. Flammia, S.T.: On SIC-POVMs in prime dimensions. J. Phys. A **39**(43), 13483–13493 (2006)
8. Fuchs, C.A., Sasaki, M.: Squeezing quantum information through a classical channel: measuring the “quantumness” of a set of quantum states. Quantum Inf. Comput. **3**(5), 377–404 (2003)
9. Godsil, C., Roy, A.: Equiangular lines, mutually unbiased bases, and spin models. Preprint arXiv:quant-ph/0511004 v2 (2005)
10. Grassl, M.: On SIC-POVMs and MUBs in dimension 6. Preprint arXiv:quant-ph/0406175v1 (2004)
11. Grassl, M.: Tomography of quantum states in small dimensions. Electron. Notes Discrete Math. **20**, 151–164 (2005)
12. Hoggar, S.G.: 64 lines from a quaternionic polytope. Geom. Dedicata **69**(3), 287–289 (1998)
13. Renes, J.M., Blume-Kohout, R., Scott, A.J., Caves, C.M.: Symmetric informationally complete quantum measurements. J. Math. Phys. **45**(6), 2171–2180 (2004)
14. Roy, A.: Complex lines with restricted angles. PhD thesis, University of Waterloo (2005)
15. Scott, A.J., Walgate, J., Sanders, B.C.: Optimal fingerprinting strategies with one-sided error. Preprint arXiv:quant-ph/0507048 v3 (2006)
16. Serre, J.-P.: Quelques applications du theoreme de densite de Chebotarev. Publ. Math. lIHES **54**, 123–201 (1981)
17. Zauner, G.: Quantum designs–Foundations of a non-commutative theory of designs. PhD thesis, University of Vienna (1999) (in German)