PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 138, Number 12, December 2010, Pages 4387–4404
S 0002-9939(2010)10435-5
Article electronically published on May 27, 2010

COMPLEX EQUIANGULAR PARSEVAL FRAMES AND SEIDEL MATRICES CONTAINING pTH ROOTS OF UNITY

BERNHARD G. BODMANN AND HELEN J. ELWOOD

(Communicated by Michael T. Lacey)

Abstract. We derive necessary conditions for the existence of complex Seidel matrices containing pth roots of unity and having exactly two eigenvalues, under the assumption that p is prime. The existence of such matrices is equivalent to the existence of equiangular Parseval frames with Gram matrices whose off-diagonal entries are a common multiple of the pth roots of unity. Explicitly examining the necessary conditions for $p = 5$ and $p = 7$ rules out the existence of many such frames with a number of vectors less than 50, similar to previous results in the cube roots case. On the other hand, we confirm the existence of $p^2 \times p^2$ Seidel matrices containing pth roots of unity, and thus the existence of the associated complex equiangular Parseval frames, for any $p \geq 2$. The construction of these Seidel matrices also yields a family of previously unknown Butson-type complex Hadamard matrices.

1. Introduction

Orthonormal bases are a common tool for representing vectors or operators on Hilbert spaces. For certain tasks, however, it is preferable to use an overcomplete, nonorthogonal family of vectors instead of an orthonormal basis, and thereby incorporate redundancy in the representation. Frames are such families which provide stable embeddings of Hilbert spaces. More precisely, a family of vectors $\{f_j\}_{j\in J}$ is a frame for a Hilbert space H if the map from each vector in H to the sequence of its inner products with the frame vectors is bounded and has a bounded inverse on its range. If the map is an isometry, then we speak of a Parseval frame. Frames became popular in signal processing because of the inherent flexibility in their design [17, 18] which can be used, for example, for loss-insensitive data transmissions [11, 5, 14, 2, 16]. It has been shown that the special class of equiangular Parseval frames has certain optimality properties for this purpose [5, 14, 2]. Despite their applicability in various fields ranging from engineering [24, 23] to quantum communication [1, 20, 26], the last years have shown how challenging the construction of equiangular Parseval frames can be. For real Hilbert spaces, the seminal work of Seidel and collaborators [10, 19, 22] remains the standard source of constructions, while the few known examples in the complex case [13, 6, 7, 21, 12, 26] leave fundamental, unanswered questions such as whether maximal families of complex

Received by the editors September 21, 2009 and, in revised form, February 9, 2010.

2010 *Mathematics Subject Classification.* Primary 42C15, 52C17; Secondary 05B20.

This research was partially supported by NSF Grant DMS-0807399 and by NSF Grant DMS-0914021.

equiangular tight frames exist in any dimension and whether they can always be generated with a group action [27].

The existence of equiangular Parseval frames is known to be equivalent to the existence of a Seidel matrix with two eigenvalues [19], which has also been called a signature matrix [14]. A matrix Q is a Seidel matrix provided it is self-adjoint with diagonal entries all 0 and off-diagonal entries all of modulus 1. In the real case, the off-diagonal entries must all be ± 1; these matrices may then be viewed as Seidel adjacency matrices of graphs. A similar graph-theoretic description and related combinatorial techniques have been used to examine the existence of complex Seidel matrices with entries that are cube roots of unity [3]. In this paper, we study the existence of Seidel matrices with two eigenvalues and off-diagonal entries which are all pth roots of unity, where p is a prime, $p > 2$. The results presented here are a continuation of the efforts for the cube roots case. Essential for the derivation of our necessary conditions is again the use of switching equivalence to put Seidel matrices in a standard form and thus impose additional rigidity on their structure. This allows us to rule out the existence of many Seidel matrices with two eigenvalues and thus the existence of certain complex equiangular Parseval frames, with an argument depending only on the choice of p, the number of frame vectors and the dimension of the Hilbert space.

Apart from indicating the possible sizes of complex equiangular Parseval frames for $p = 5$ and $p = 7$, we confirm the existence of such frames with examples. We show the existence of equiangular Parseval frames of p^2 vectors in $p(p+1)/2$-dimensional complex Hilbert spaces, for any $p \geq 2$. The construction of these frames proceeds via Seidel matrices containing pth roots of unity, which also yields a previously unknown family of Butson-type complex Hadamard matrices [25, 28].

The remainder of this paper is organized as follows: After fixing notation and terminology in Section 2, we examine necessary conditions for the existence of complex Seidel matrices containing pth roots of unity and having only two eigenvalues in Section 3. The previously known consequences for $p = 3$ are summarized, and analogous results for $p = 5$ and $p = 7$ are developed in Section 4, which are complemented with examples in Section 5.

2. Preliminaries

2.1. **Equiangular Parseval frames.**

Definition 2.1. Given H, a real or complex Hilbert space, a finite family of vectors $\{f_1, f_2, ..., f_n\}$ in H is a *frame* for H if and only if there exist constants $A, B \in \mathbb{R}$ such that $A, B > 0$ and

$$A\|x\|^2 \leq \sum_{j=1}^{n} |\langle x, f_j\rangle|^2 \leq B\|x\|^2$$

for all $x \in H$. A frame is said to be an A-*tight frame* if we can choose $A = B$. A *normalized tight* frame, or *Parseval* frame, is a frame which admits $A = B = 1$. A frame $\{f_1, f_2, ..., f_n\}$ is called *equal norm* if there is $b > 0$ such that $\|f_j\| = b$. It is called *equiangular* if it is equal norm and if there is $c \geq 0$ such that $|\langle f_j, f_l\rangle| = c$ for all $j, l \in \{1, 2, \dots, n\}$ with $j \neq l$. Here, we are concerned mostly with equiangular Parseval frames for $\mathbb{C}^k$, equipped with the canonical inner product. We use the term (n, k)-*frame* to refer to a Parseval frame of n vectors for $\mathbb{C}^k$.

Our construction of equiangular Parseval frames makes use of an equivalence relation among frames [11, 14, 2].

Definition 2.2. Two frames, $\{f_1, f_2, ..., f_n\}$ and $\{g_1, g_2, ..., g_n\}$ for a real or complex Hilbert space H are said to be *unitarily equivalent* if there exists a unitary operator U on H such that $g_j = Uf_j$ for all $1 \leq j \leq n$. Furthermore, we say that they are *switching equivalent* if there exists a unitary operator U on H, a permutation π on $\{1, 2, ..., n\}$ and a set of unimodular constants $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ such that for each $j \in \{1, 2, \ldots, n\}$, $g_j = \alpha_j U f_{\pi(j)}$.

It is well known [8] that the definition of a Parseval frame is equivalent to the reconstruction identity

$$x = \sum_{j=1} \langle x, f_j \rangle f_j$$

for all $x \in H$. We note that switching a frame, meaning mapping all frame vectors with a unitary, permuting them and multiplying them with unimodular constants, leaves the reconstruction identity unchanged. From this point of view, it is very natural to identify two frames that can be obtained from each other by switching. We use switching equivalence to choose particular representatives of equivalence classes and derive essential properties of equiangular Parseval frames.

2.2. **Seidel matrices.** With a frame $F = \{f_1, f_2, \ldots, f_n\}$ for a real or complex Hilbert space H, we associate its analysis operator $V : H \to \ell^2(\{1, 2, \ldots, n\})$, which maps $x \in H$ to its frame coefficients, $(Vx)_j = \langle x, f_j \rangle$. Essential properties of the frame F are encoded in the Gram matrix VV^*, obtained from V and its Hilbert adjoint V^*. If F is equal norm, then the diagonal entries of the Gram matrix are identical, $(VV^*)_{j,j} = \|f_j\|^2 = b^2$ for some $b > 0$. If F is a Parseval frame, then V is an isometry and VV^* is an orthogonal projection. Consequently, for an equal-norm (n, k)-frame, $F = \{f_1, f_2, \ldots, f_n\}$, the trace of the Gram matrix is equal to its rank and thus $\|f_j\|^2 = k/n$ for all $1 \leq j \leq n$. Additionally, if F is an equiangular (n, k)-frame, then the Frobenius norm of the Gram matrix is equal to the square root of its rank, and $|\langle f_j, f_l \rangle| = c_{n,k} := \sqrt{\frac{k(n-k)}{n^2(n-1)}}$, for all $j \neq l$ ([24], [14]; see also [9]). This yields that the Gram matrix of an equiangular (n, k)-frame is of the form

$$VV^* = (\frac{k}{n})I_n + c_{n,k}Q,$$

where Q is a self-adjoint $n \times n$ matrix, with diagonal entries equal to 0, and off-diagonal entries all with modulus equal to 1. The matrix Q is called the *signature matrix* associated with the equiangular (n, k)-frame, $\{f_1, f_2, ..., f_n\}$. The following result characterizes the signature matrices of equiangular (n, k)-frames.

Theorem 2.3 (Proposition 3.2 and Theorem 3.3 of [14])**.** *Let Q be a self-adjoint $n \times n$ matrix with $Q_{j,j} = 0$ and $|Q_{j,l}| = 1$ for all $j \neq l$. Then the following three properties are equivalent:*

1. *Q is the signature matrix of an equiangular (n, k)-frame for some k;*
2. *$Q^2 = (n-1)I + \mu Q$ for some necessarily real number μ; and*
3. *Q has exactly two eigenvalues.*

Additionally, any matrix Q satisfying any of the three equivalent conditions has eigenvalues $\lambda_1 < 0 < \lambda_2$ for which the following five identities hold:

$$\mu = (n-2k)\sqrt{\frac{n-1}{k(n-k)}} = \lambda_1 + \lambda_2\,,$$
$$k = \frac{n}{2} - \frac{\mu n}{2\sqrt{4(n-1)+\mu^2}}\,,$$
$$\lambda_1 = -\sqrt{\frac{k(n-1)}{n-k}},\ \lambda_2 = \sqrt{\frac{(n-1)(n-k)}{k}}, \qquad \textit{and} \qquad n = 1 - \lambda_1\lambda_2\,.$$

When all of the entries of Q are real, Q must have diagonal entries equal to 0 and off-diagonal entries of ±1. It has been shown (Theorem 3.10 of [14]) that in this case there is a one-to-one correspondence between the switching equivalence classes of real equiangular Parseval frames and regular two-graphs [22].

When switching from a frame $F = \{f_1, f_2, \dots, f_n\}$ to $G = \{g_1, g_2, \dots, g_n\}$ given by $g_j = \alpha_j U f_{\pi(j)}$, then the signature matrix associated with G is obtained by conjugating the signature matrix of F with a diagonal unitary and with a permutation matrix. This motivates the following definition of switching equivalence for Seidel matrices.

Definition 2.4. Two Seidel matrices Q and Q' are said to be *switching equivalent* if they can be obtained from each other by conjugating with a diagonal unitary and with a permutation matrix. Furthermore, we say that a Seidel matrix Q is in standard form provided its first row and column contain all 1s, except on the diagonal (which must be 0). We say that Q is *trivial* if its standard form has all off-diagonal entries equal to 1 and *nontrivial* if at least one off-diagonal entry is not equal to 1.

Note that two switching equivalent Seidel matrices have the same spectrum, since they are related by conjugation with a unitary. As the equivalence class of any Seidel matrix contains a matrix in standard form we may focus on examining matrices of this form with two eigenvalues. The primary goal of this paper is to find necessary conditions for the existence of certain Seidel matrices with two eigenvalues and hence for the existence of equiangular Parseval frames. In the real case, Seidel and others [19, 22] established necessary and sufficient conditions in graph-theoretic terms. A similar graph-theoretic formulation was used to derive necessary conditions for complex equiangular Parseval frames when the the off-diagonal entries are cube roots of unity [3]. In this paper we explore nontrivial standard Seidel matrices with off-diagonal entries which are pth roots of unity, for p prime, $p > 2$. These cases will add to the description of families of complex equiangular tight frames, in analogy with previous results.

3. Conditions for signature matrices containing pth roots of unity

In this section, we consider nontrivial signature matrices whose off-diagonal entries are pth roots of unity. Let $p \in \mathbb{N}$, $\omega = e^{2\pi i/p}$, and accordingly $\{1, \omega, \omega^2, ..., \omega^{p-1}\}$ be the set of pth roots of unity. The overall strategy followed here mimics the treatment of $p = 3$ in [3], with some modifications that allow us to address the general pth roots case.

3.1. **Signature matrices in standard form.**

Definition 3.1. For $p \in \mathbb{N}$, a matrix Q is a pth root Seidel matrix if it is self-adjoint, with diagonal entries all equal to 0 and off-diagonal entries which are all pth roots of unity. If, in addition, Q has exactly two eigenvalues, then Q is the pth root signature matrix of an equiangular tight frame.

The following lemma is verbatim as in the cube roots case.

Lemma 3.2. *If Q' is an $n \times n$ pth root Seidel matrix, then it is switching equivalent to a pth root Seidel matrix of the form*

$$Q = \begin{pmatrix} 0 & 1 & \dots & \dots & 1 \\ 1 & 0 & * & \dots & * \\ \vdots & * & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & * \\ 1 & * & \dots & * & 0 \end{pmatrix},$$

where the entries marked with $*$ are pth roots of unity. Moreover, Q' is the signature matrix of an equiangular (n, k)-frame if and only if Q is the signature matrix of an equiangular (n, k)-frame.

Proof. Suppose that Q' is an $n \times n$ pth root Seidel matrix. So Q' is self-adjoint, $|Q_{j,l}| = 1$, for $j \neq l$, and $(Q')^2 = (n-1)I + \mu Q'$ for some $\mu \in \mathbb{R}$, by Theorem 2.3. Let U be the diagonal matrix with nonzero entries $U_{1,1} = 1$ and $U_{j,j} = Q'_{1,j}$, $j \in \{2, 3, \dots, n\}$. Then, U is a unitary matrix, as $|Q'_{j,l}| = 1$ when $j \neq l$. Define $Q = UQ'U^*$ and note that Q is a self-adjoint $n \times n$ matrix with $Q_{j,j} = 0$ and $|Q_{j,l}| = 1$ when $j \neq l$. The off-diagonal entries of Q are pth roots of unity and as $Q'_{j,l} = \overline{Q'_{l,j}}$, the off-diagonal entries of the first row and first column are 1's. Therefore Q has the proposed form. So Q is a pth root Seidel matrix that is unitarily equivalent to Q'. As Q and Q' have the same eigenvalues, if one of them is the signature matrix of an equiangular (n, k)-frame, then so is the other. □

Next we include a lemma concerning linear combinations of pth roots of unity with rational coefficients. This lemma is essential for deriving necessary conditions of pth root Seidel matrices having only two eigenvalues.

Lemma 3.3. *Let $\omega = e^{2\pi i/p}$, where p is prime. If $a_0, a_1, a_2, ..., a_{p-1} \in \mathbb{Q}$ and $a_0 1 + a_1\omega + a_2\omega^2 + ... + a_{p-1}\omega^{p-1} = 0$, then $a_0 = a_1 = a_2 = ... = a_{p-1}$.*

Proof. Suppose that $a_0, a_1, a_2, ..., a_{p-1} \in \mathbb{Q}$ and

$$a_0 1 + a_1\omega + a_2\omega^2 + ... + a_{p-1}\omega^{p-1} = 0. \tag{3.1}$$

First we show that we can reduce Equation (3.1) to an equation in terms of $\{1, \omega, \omega^2, \dots, \omega^{p-2}\}$. As $\omega^p = 1$, we know that $\omega^p - 1 = 0$, so $(\omega - 1)(\omega^{p-1} + \omega^{p-2} + \cdots + \omega^2 + \omega + 1) = 0$. Since $\omega \neq 1$, $1 + \omega + \omega^2 + \cdots + \omega^{p-1} = 0$, and therefore

$$a_{p-1} + a_{p-1}\omega + a_{p-1}\omega^2 + ... + a_{p-1}\omega^{p-1} = 0. \tag{3.2}$$

Subtracting Equation (3.2) from Equation (3.1), we see that

$$(a_0 - a_{p-1}) + (a_1 - a_{p-1})\omega + (a_2 - a_{p-1})\omega^2 + ... + (a_{p-2} - a_{p-1})\omega^{p-2} = 0. \tag{3.3}$$

But ω is a primitive pth root of unity, so the degree of $\mathbb{Q}(\omega)$ over $\mathbb{Q}$ is $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(p) = p - 1$, where φ is the Euler function (see Proposition 8.3, p. 299, in

[15]). Therefore the minimal irreducible polynomial of ω over $\mathbb{Q}$ has degree $p-1$. Specifically, this polynomial is the pth cyclotomic polynomial.

Since the degree of $f(x) = (a_0 - a_{p-1}) + (a_1 - a_{p-1})x + (a_2 - a_{p-1})x^2 + ... + (a_{p-2} - ap - 1)x^{p-2}$ is $p-2$, which is smaller than the degree of the minimal irreducible polynomial of ω, we conclude from Equation (3.3) that $f(x)$ must be the zero polynomial. Therefore $(a_0 - a_{p-1}), (a_1 - a_{p-1}), (a_2 - a_{p-1}), ..., (a_{p-2} - a_{p-1}) = 0$, and so $a_0 = a_1 = a_2 = ... = a_{p-1}$. □

Notice that this result implies that $\{1, \omega, \omega^2, \ldots, \omega^{p-1}\}$ is a linearly dependent set over the rational numbers whereas $\{1, \omega, \omega^2, \ldots, \omega^{p-2}\}$ is linearly independent.

Theorem 3.4. *Let Q be a nontrivial pth root Seidel matrix in standard form, where p is prime, and $Q^2 = (n-1)I + \mu Q$ for some $\mu \in \mathbb{R}$. Then $e := \frac{n-\mu-2}{p}$ is an integer, and for any l with $2 \le l \le n$, the lth column of Q (and similarly the lth row) contains e entries equal to ω, e entries equal to ω^2 ... and e entries equal to ω^{p-1}, and contains $e + \mu + 1 = \frac{n+(p-1)\mu+(p-2)}{p}$ entries equal to 1.*

Proof. For $2 \le j \le n$, p prime, define

$$\begin{aligned} x_{1,l} &:= \#\{i : Q_{j,l} = 1\}, \\ x_{2,l} &:= \#\{i : Q_{j,l} = \omega\}, \\ x_{3,l} &:= \#\{i : Q_{j,l} = \omega^2\}, \\ &\cdots \\ x_{p,l} &:= \#\{i : Q_{j,l} = \omega^{p-1}\}. \end{aligned}$$

Since the lth column of Q has $n-1$ nonzero entries (recall the zero on the diagonal), we have

$$x_{1,l} + x_{2,l} + ... + x_{p,l} = n - 1. \tag{3.4}$$

Also, since $Q^2 = (n-1)I + \mu Q$, and Q is in standard form, for $2 \le l \le n$,

$$\mu = \mu Q_{1,l} = [(n-1)I + \mu Q]_{1,l} = (Q^2)_{1,l} = (x_{1,l} - 1)1 + x_{2,l}\omega + x_{3,l}\omega^2 + ... + x_{p,l}\omega^{p-1}.$$

Therefore, $(x_{1,l} - \mu - 1) + x_{2,l}\omega + x_{3,l}\omega^2 + ... + x_{p,l}\omega^{p-1} = 0$, and so by Lemma 3.3,

$$x_{1,l} - \mu - 1 = x_{2,l} = x_{3,l} = ... = x_{p,l}. \tag{3.5}$$

Using these identities to eliminate $x_{j,l}$ with $j \ge 2$ in Equation (3.4) gives $x_{1,l} + (p-1)(x_{1,l} - \mu - 1) = n - 1$, and we conclude

$$x_{1,l} = \frac{n + (p-1)\mu + (p-2)}{p}. \tag{3.6}$$

Equation (3.5) hence shows that for all $2 \le j \le p$,

$$x_{j,l} = \frac{n - \mu - 2}{p}. \tag{3.7}$$

Since the quantities in (3.6) and (3.7) do not depend on l, they are valid for any column. In addition, since $Q = Q^*$ and $\overline{\omega^m} = \omega^{p-m}$ for all $1 \le m \le p$, the same equations hold for the rows of the Seidel matrix Q. □

3.2. **The structure of nontrivial pth root signature matrices.** Let Q be a pth root Seidel matrix, with p prime, and define

$$\alpha_{a,b} := \#\{k : Q_{j,k} = \omega^a \textit{ and } Q_{k,l} = \omega^{p-b}\},$$

for all $a, b \in \mathbb{Z}$. The implicit identity $\alpha_{a,b} = \alpha_{a,b\pm p}$ helps simplify notation in the computations below. We also define $R_t := \sum_{s=1}^{p} \alpha_{t,s}$ for $1 \leq t \leq p$, $C_t := \sum_{s=1}^{p} \alpha_{s,t}$ for $1 \leq t \leq p$, and $Z_t := \sum_{s=1}^{p}(\alpha_{s,s} - \alpha_{s,s-t})$ for $1 \leq t \leq p-1$.

Here and hereafter, we use modular arithmetic. If $q, r \in \mathbb{Z}$ and $p \in \mathbb{N}$, then $q \equiv r(mod\ p)$ means that $q - r$ is an integer multiple of p. On the other hand, when writing $q = r(mod\ p)$ it is implicit that $0 \leq q \leq p-1$.

Lemma 3.5. *Suppose that Q is a nontrivial pth root Seidel matrix, with p prime. Additionally suppose that Q is in standard form and satisfies $Q^2 = (n-1)I + \mu Q$. Then the following system of linear equations holds:*

(1) *$R_1 = e - 1$, $R_t = e$ for $2 \leq t \leq p-1$, and $R_p = e + \mu + 1$,*

(2) *$C_t = e$ for $1 \leq t \leq p-2$, $C_{p-1} = e - 1$, and $C_p = e + \mu + 1$,*

(3) *$Z_1 = -\mu$, and $Z_t = 0$ for $2 \leq t \leq p-1$.*

These $(3p-1)$ equations fix the values of the row sums of Q, the column sums of Q, and the difference computed by subtracting the sum of cyclic off-diagonals of Q from the main diagonal.

Proof. As Q is nontrivial, we know that $Q_{j,l} \neq 1$ for some $2 \leq j, l \leq n$ with $j \neq l$. Without loss of generality, let $Q_{j,l} = \omega$. Then the number of ωs in row j is $\alpha_{1,1} + \alpha_{1,2} + \cdots + \alpha_{1,p} + 1$ by the definition of α, with the $+1$ term coming from $\alpha_{j,l} = \omega$. We know that the number of ωs in row j is also equal to $e = \frac{n-\mu-2}{p}$ from Theorem 3.4. So $R_1 = \sum_{s=1}^{p} \alpha_{1,t} = e - 1$.

For $2 \leq t \leq p-1$, the number of ω^ts in row j is $\alpha_{t,1} + \alpha_{t,2} + \cdots + \alpha_{t,p}$, and by Theorem 3.4, the number of ω^ts in row j is e, so $R_t = \sum_{s=1}^{p} \alpha_{t,s} = e$.

Also, the number of 1s in row j is $\alpha_{p,1} + \alpha_{p,2} + \cdots + \alpha_{p,p}$ and by Theorem 3.4, the number of 1s in row j is $e + \mu + 1$, so $R_p = \sum_{s=1}^{p} \alpha_{p,s} = e + \mu + 1$.

As Theorem 3.4 holds for columns as well as for rows, we know that the number of $\omega^{(p-t)}$ in column l is $C_t = \sum_{s=1}^{p} \alpha_{s,t} = e$ for all $1 \leq l \leq p-2$.

The number of ωs in column l (remembering that $Q_{j,l} = \omega$) is $C_{(p-1)} = \sum_{s=1}^{p} \alpha_{s,(p-1)} = e - 1$, and the number of 1s in column l is $C_p = \sum_{s=1}^{p} \alpha_{s,p} = e + \mu + 1$.

Furthermore, since $Q^2 = (n-1)I + \mu Q$, we have that

$$\mu\omega = \mu Q_{i,j} = [(n-1)I + \mu Q]_{i,j} = (Q^2)_{i,j} = \sum_{k=1}^{n} Q_{i,k}Q_{k,j} = \sum_{j,l=1}^{p} (\alpha_{j,l})(\omega^j)(\omega^{p-l}).$$

Collecting powers of ω, we get $(\alpha_{1,1} + \alpha_{2,2} + \alpha_{3,3} + \cdots + \alpha_{p,p})1 + (\alpha_{1,p} + \alpha_{2,1} + \alpha_{3,2} + \cdots + \alpha_{p,(p-1)} - \mu)\omega + (\alpha_{1,(p-1)} + \alpha_{2,p} + \alpha_{3,1} + \ldots + \alpha_{p,(p-2)})\omega^2 + \cdots + (\alpha_{1,2} + \alpha_{2,3} + \alpha_{3,4} + \cdots + \alpha_{p,1})\omega^{p-1} = 0$.

That is, $\sum_{s=0}^{p-1} \sum_{t=1}^{p} (\alpha_{t,t-s}\omega^j) - \mu\omega = 0$.

It follows from Lemma 3.3 that

$$\begin{aligned}\alpha_{1,1}+\alpha_{2,2}+\alpha_{3,3}+\cdots+\alpha_{p,p} &= \alpha_{1,p}+\alpha_{2,1}+\alpha_{3,2}+\cdots+\alpha_{p,(p-1)}-\mu\\ &= \alpha_{1,(p-1)}+\alpha_{2,p}+\alpha_{3,1}+\cdots+\alpha_{p,(p-2)}\\ &\vdots\\ &= \alpha_{1,2}+\alpha_{2,3}+\alpha_{3,4}+\cdots+\alpha_{p,1}\end{aligned}$$

and therefore, the following $p-1$ equations hold:

$$Z_1=\alpha_{1,1}-\alpha_{1,p}+\alpha_{2,2}-\alpha_{2,1}+\alpha_{3,3}-\alpha_{3,2}+\cdots+\alpha_{p,p}-\alpha_{p,(p-1)}=-\mu,\ \text{and}$$
$$Z_t=\sum_{s=1}^{p}(\alpha_{s,s}-\alpha_{s,s-t})=0 \text{ for } 2\le t\le p-1\,. \qquad \square$$

So when the hypotheses of Lemma 3.5 are satisfied, we have a total of $(3p-1)$ equations in p^2 unknowns which must also be satisfied. We state some results exploring the consequences of this lemma.

Theorem 3.6. *For $p\in\mathbb{N}$ prime, $p>2$, let Q be a nontrivial pth root signature matrix of an equiangular (n,k)-frame, satisfying $Q^2=(n-1)I+\mu Q$. Then the following assertions hold:*

1. *The value μ is an integer and $\mu\equiv(p-2)(mod\ p)$.*
2. *The integer n satisfies $n\equiv 0(mod\ p)$.*
3. *If $\lambda_1<0<\lambda_2$ are the eigenvalues of Q, then λ_1 and λ_2 are integers with $\lambda_1\equiv(p-1)(mod\ p)$ and $\lambda_2\equiv(p-1)(mod\ p)$.*
4. *The integer $4(n-1)+\mu^2$ is a perfect square and $4(n-1)+\mu^2\equiv 0(mod\ p^2)$.*

Proof. Using the same notation as in Lemma 3.5,

$$R_p=\alpha_{p,1}+\alpha_{p,2}+\alpha_{p,3}+...+\alpha_{p,p}=e+\mu+1$$

implies that $(\alpha_{p,1}+\alpha_{p,2}+\alpha_{p,3}+...+\alpha_{p,p})$ is an integer and e is an integer, so μ must also be an integer.

To prove the first assertion, we define $q=\frac{p-1}{2}$ and introduce the following coefficients:

$$r_t=\begin{cases}\frac{2-t}{p} & \text{for } 1\le t\le q+2,\\ \frac{p+2-t}{p} & \text{for } q+3\le t\le p;\end{cases}$$
$$c_t=\begin{cases}\frac{t-1}{p} & \text{for } 1\le t\le q+1,\\ \frac{t-1-p}{p} & \text{for } q+2\le t\le p;\end{cases}$$
$$z_t=\begin{cases}\frac{1-t}{p} & \text{for } 1\le t\le q+1,\\ \frac{p+1-t}{p} & \text{for } q+2\le t\le p-1.\end{cases}$$

Applying Lemma 3.5, we see that

$$\begin{aligned}\sum_{t=1}^{p} r_t R_t + \sum_{t=1}^{p} c_t C_t + \sum_{t=1}^{p-1} z_t Z_t &= [\frac{1}{p}(e-1) - \frac{1}{p}(e) - \frac{2}{p}(e) - \frac{3}{p}(e) - \cdots - \frac{q}{p}(e) \\ &\quad + \frac{q}{p}(e) + \frac{q-1}{p}(e) + \frac{q-2}{p}(e) + \cdots + \frac{3}{p}(e) \\ &\quad + \frac{2}{p}(e+\mu+1)] + [\frac{1}{p}(e) + \frac{2}{p}(e) + \frac{3}{p}(e) + \cdots \\ &\quad + \frac{q}{p}(e) - \frac{q}{p}(e) - \frac{q-1}{p}(e) - \frac{q-2}{p}(e) - \cdots - \frac{3}{p}(e) \\ &\quad - \frac{2}{p}(e-1) - \frac{1}{p}(e+\mu+1)] \\ &\quad + [-\frac{1}{p}(0) - \frac{2}{p}(0) - \frac{3}{p}(0) - \cdots - \frac{q}{p}(0) \\ &\quad + \frac{q}{p}(0) + \frac{q-1}{p}(0) + \frac{q-2}{p}(0) + \cdots + \frac{2}{p}(0)] \\ &= \frac{\mu}{p} + \frac{2}{p}.\end{aligned}$$

Now we define $\{b_{j,l}\}_{j,l=1}^{p}$ to be the coefficients of $\{\alpha_{j,l}\}_{j,l=1}^{p}$ in the expression

$$\sum_{j,l=1}^{p} b_{j,l}\alpha_{j,l} = \sum_{t=1}^{p} r_t R_t + \sum_{t=1}^{p} c_t C_t + \sum_{t=1}^{p-1} z_t Z_t. \tag{3.8}$$

By the definition of R_t, C_t and Z_t, the expression (3.8) is a rational linear combination of $\{\alpha_{j,l}\}_{j,l=1}^{p}$. Our goal is to show that, in fact, it is a linear combination with integer coefficients $\{b_{j,l}\}_{j,l=1}^{p}$. As each $\alpha_{j,l}$ is an integer, this would show that the expression (3.8) is an integer.

To accomplish this, we consider five main cases of coefficients $\{b_{j,l}\}_{j,l=1}^{p}$: Case 1: $j = l$; Case 2: $j \neq l$, $1 \leq j \leq q+2$, $1 \leq l \leq q+1$; Case 3: $j \neq l$, $1 \leq j \leq q+2$, $p \geq l > q+1$; Case 4: $j \neq l$, $p \geq j > q+2$, $1 \leq l \leq q+1$; Case 5: $j \neq l$, $p \geq j > q+2, p \geq l > q+1$. Distinguishing these cases is necessary because of the piecewise definition of r_t, c_t and z_t. To simplify notation when computing contributions from Z_t in expression (3.8), we define $s = (j-l)(mod\ p)$ and recall that our convention for modular arithmetic implies $0 \leq s \leq p-1$.

Case 1: We first consider the case when $j = l$. If $j = l = 1$, then as $\alpha_{1,1}$ appears in R_1, C_1, and in Z_t for all $1 \leq t \leq p-1$, the coefficient $b_{1,1}$ in expression (3.8) is $\frac{1}{p} + 0 + \sum_{t=2}^{q+1} \frac{1-t}{p} + \sum_{t=q+2}^{p-1} \frac{p+1-t}{p} = \frac{1}{p} + 0 - \frac{1}{p} = 0$.

If $j = l$ and $1 < j < q+2$, then $\alpha_{j,j}$ appears in R_j, C_j, and in Z_t for all $1 \leq t \leq p-1$, so the coefficient of $\alpha_{j,j}$ in expression (3.8) is $b_{j,j} = \frac{2-j}{p} + \frac{j-1}{p} + \frac{-1}{p} = 0$, whereas if $j \neq 1$ and $j = l > q+2$, then the coefficient is $b_{j,j} = \frac{p+2-j}{p} + \frac{j-p-1}{p} - \frac{1}{p} = 0$.

Finally, if $j = l = q+2$, then the coefficient of $\alpha_{j,l} = \alpha_{q+2,q+2}$ in expression (3.8) is $b_{q+2,q+2} = -\frac{q}{p} - \frac{q}{p} - \frac{1}{p} = -1$.

We conclude that if $j = l$, then the coefficient $b_{j,l}$ is an integer.

Case 2: For the remainder of the proof we focus on the coefficient of $\alpha_{j,l}$, where $j \neq l$. Note as $j \neq l$, $s \in \{1, 2, 3, ..., (p-1)\}$.

Let $1 \leq j \leq q+2, 1 \leq l \leq q+1$. Now suppose that $1 \leq s \leq q+1$. Then the coefficient of $\alpha_{j,l}$ in expression (3.8) is $b_{j,l} = \frac{2-j}{p} + \frac{l-1}{p} + \frac{-(1-s)}{p} = \frac{l-j+s}{p} \in \mathbb{Z}$ as $s = (j-l)(mod\ p)$. If instead, $q+2 \leq s < p$, then $b_{j,l} = \frac{2-j}{p} + \frac{l-1}{p} + \frac{-(p+1-s)}{p} = \frac{j-l+s-p}{p} \in \mathbb{Z}$ as $s = (j-l)(mod\ p)$. Thus, for $1 \leq j \leq q+2, 1 \leq l \leq q+1$, the coefficient of $\alpha_{j,l}$ in expression (3.8) is an integer.

Case 3: Now let $1 \leq j \leq q+2, q+1 < l \leq p$. Suppose that $1 \leq s \leq (q+1)$. Then $b_{j,l} = \frac{2-j}{p} + \frac{l-p-1}{p} + \frac{-(1-s)}{p} = \frac{l-j+s-p}{p} \in \mathbb{Z}$ as $s = (j-l)(mod\ p)$. If instead, $q+2 \leq s < p$, then $b_{j,l} = \frac{2-j}{p} + \frac{l-p-1}{p} + \frac{-(p+1-s)}{p} = \frac{l-j+s-2p}{p} \in \mathbb{Z}$ as $s = (j-l)(mod\ p)$. Therefore, when $1 \leq j \leq q+2$, $q+1 < l \leq p$, we have that the coefficient $b_{j,l}$ is an integer.

Case 4: Next, let $q+2 < j \leq p, 1 \leq l \leq q+1$ Suppose that $1 \leq s \leq q+1$. Then $b_{j,l} = \frac{p+2-j}{p} + \frac{(l-1)}{p} + \frac{-(1-s)}{p} = \frac{l-j+s+p}{p} \in \mathbb{Z}$ as $s = (j-l)(mod\, p)$. If instead, $q+2 \leq s < p$, then the coefficient of $\alpha_{j,l}$ is $b_{j,l} = \frac{p+2-j}{p} + \frac{(l-1)}{p} + \frac{-(p+1-s)}{p} = \frac{l-j+s}{p} \in \mathbb{Z}$ as $s = (j-l)(mod\ p)$. Thus, if $q+2 < j \leq p$ and $1 \leq l \leq q+1$, then $b_{j,l}$ is an integer.

Case 5: Lastly, let $q+2 < j \leq p$ and $q+1 < l \leq p$. Now suppose that $1 \leq s \leq (q+1)$. Then $b_{j,l} = \frac{p+2-j}{p} + \frac{l-1-p}{p} + \frac{-(1-s)}{p} = \frac{l-j+s}{p} \in \mathbb{Z}$ as $s = (j-l)(mod\ p)$. If instead, $q+2 \leq s < p$, then the coefficient is $b_{j,l} = \frac{p+2-j}{p} + \frac{l-1-p}{p} + \frac{-(p+1-s)}{p} = \frac{l-j+s-p}{p} \in \mathbb{Z}$ as $s = (j-l)(mod\ p)$. Therefore, if $q+2 < j \leq p$ and $q+1 < l \leq p$, then the coefficient of $\alpha_{j,l}$ in expression (3.8) is an integer.

Having covered all cases, we conclude that the expression (3.8) is indeed an integer linear combination of $\{\alpha_{j,l}\}_{j,l=1}^{p}$, and as each $\alpha_{j,l}$ is an integer, so is the entire expression (3.8). Recalling that $\sum_{t=1}^{p}(r_t R_t + c_t C_t) + \sum_{t=1}^{p-1} z_t Z_t = (\mu+2)/p$, we see that $\mu + 2 \equiv 0(mod\ p)$, and therefore, $\mu \equiv (p-2)(mod\ p)$.

To prove assertion (2) of this theorem, note that as $Q^2 = (n-1)I + \mu Q$, by Theorem 3.4, we have that $e = \frac{n-\mu-2}{p}$ is an integer. So $n - \mu - 2 \equiv 0(mod\ p)$, and since $\mu \equiv (p-2)(mod\ p), n \equiv \mu + 2(mod\ p) \equiv 0(mod\ p)$.

For assertion (3), we recall the equations in Theorem 2.3, $\mu = (n-2k)\sqrt{\frac{(n-1)}{k(n-k)}} = \lambda_1 + \lambda_2$. Since μ is an integer by assertion (1), we have $\sqrt{\frac{(n-1)}{k(n-k)}} \in \mathbb{Q}$ and $\lambda_1 = -\sqrt{\frac{k(n-1)}{(n-k)}} = -k\sqrt{\frac{(n-1)}{k(n-k)}} \in \mathbb{Q}$. In addition we know that $\lambda_2 = \frac{1-n}{\lambda_1} \in \mathbb{Q}$. Therefore, λ_1 and λ_2 are both rational. Since $Q^2 = (n-1)Q + \mu Q$, the polynomial $p(x) = x^2 - \mu x - (n-1)$ annihilates Q. So the minimal polynomial of Q divides $p(x)$, and λ_1 and λ_2 are rational roots of $p(x)$. However, the coefficients of $p(x)$ are all integers and the leading coefficient is 1, so by the Rational Root Theorem (see Lemma 6.11 in [15]), λ_1 and λ_2 are integers. Now, $\lambda_1 + \lambda_2 = \mu \equiv (p-2)(mod\ p)$ by part(1), and $\lambda_1\lambda_2 = 1 - n \equiv 1(mod\ p)$ by part (2) and the equations in Theorem 2.3, with $\lambda_1(mod\ p), \lambda_2(mod\ p) \in \{0, 1, 2, 3, \ldots, (p-1)\}$. So $\lambda_2 = (p-2) - \lambda_1$, and $\lambda_1\lambda_2 = \lambda_1[(p-2)-\lambda_1] = 1$. Therefore, $\lambda_1 p - 2\lambda_1 - \lambda_1^2 = -2\lambda_1 - \lambda_1^2 = 1$. So, $\lambda_1^2 + 2\lambda_1 + 1 = 0$; that is, $\lambda_1^2 + 2\lambda_1 + 1 = mp$, for some $m \in \mathbb{Z}$. Using the quadratic formula, the roots of $\lambda_1^2 + 2\lambda_1 + (1-mp) = 0$ are $\lambda_1 = \frac{-2 \pm \sqrt{4-4(1)(1-mp)}}{2} = -1 \pm \sqrt{mp}$. $\sqrt{mp}$ must be an integer, as $\lambda_1 \in \mathbb{Z}$. Since p is prime, m must therefore be a multiple of p, say $m = lp$, where l is a perfect square. So $\lambda_1 = -1 \pm \sqrt{mp} = -1 \pm \sqrt{l}p$ with $\sqrt{l} \in \mathbb{Z}$, and therefore $\lambda_1 \equiv (p-1)(mod\ p)$. Finally, $\lambda_2 = (p-2) - \lambda_1 \equiv ((p-2)-(p-1))(mod\ p) \equiv (p-1)(mod\ p)$.

To prove assertion (4) we use the fact that $k = \frac{n}{2} - \frac{\mu n}{2\sqrt{4(n-1)+\mu^2}}$ from the Theorem 2.3 equations. Therefore, $\sqrt{4(n-1)+\mu^2} = \frac{\mu n}{n-2k} \in \mathbb{Q}$ by part (1). $n, \mu \in \mathbb{Z}$, so $(4(n-1)+\mu^2) \in \mathbb{Z}$. Thus $\sqrt{4(n-1)+\mu^2} \in \mathbb{Q}$ if and only if $\sqrt{4(n-1)+\mu^2} \in \mathbb{Z}$. So $\sqrt{4(n-1)+\mu^2} = m \in \mathbb{Z}$, and therefore $4(n-1)+\mu^2 = m^2$; that is, $4(n-1)+\mu^2$ is a perfect square. Furthermore, since $4(n-1)+\mu^2 = m^2$ and $\mu \equiv (p-2)(mod\ p)$, $n \equiv 0(mod\ p)$, by parts (1) and (2) we see that $4(n-1)+\mu^2 \equiv 0(mod\ p)$. So $m^2 = 0(mod\ p)$. Therefore p divides m^2, but since p is prime, p must divide m, and therefore p^2 divides $m^2 = 4(n-1)+\mu^2$ and $4(n-1)+\mu^2 \equiv 0(mod\ p^2)$. □

Corollary 3.7. *For p prime, $p > 2$, let Q be a nontrivial pth root signature matrix of an equiangular (n,k)-frame such that $Q^2 = (n-1)I + \mu Q$. Then there is $m \in \{0,1,2,\ldots,(p-1)\}$ such that $n \equiv mp\ (mod\ p^2)$, and $\mu \equiv (mp-2)\ (mod\ p^2)$.*

Proof. By Theorem 3.6(2), $n \equiv 0\ (mod\ p)$, so the equivalence class of $n(mod\ p^2)$ must have a representative in the set $\{0, p, 2p, 3p, \ldots, (p-1)p\}$. So $n \equiv mp\ (mod\ p^2)$ where $m \in \{0,1,2,3,...,(p-1)\}$. We also know by Theorem 3.6 (1) that $\mu \equiv (p-2)\ (mod\ p)$, so the equivalence class of $\mu(mod\ p^2)$ has a representative in the set $\{(p-2),(2p-2),(3p-2),...,(p^2-2)\}$, so $\mu \equiv (rp-2)\ (mod\ p^2)$, where $r \in \{0,1,2,...,(p-1)\}$. Additionally, by Theorem 3.1(d), we have that $4(n-1)+\mu^2 \equiv 0\ (mod\ p^2)$, so

$$4(n-1)+\mu^2 = 4(mp-1)+(rp-2)^2 \equiv 4p(m-r)(modp) \equiv 0\ (mod\ p^2),$$

and therefore $m \equiv r\ (mod\ p)$, as p is a prime with $p > 2$. But $m, r \in \{0,1,2,\ldots,(p-1)\}$, so $m = r$. That is, $n \equiv mp\ (mod\ p^2)$, and $\mu \equiv (mp-2)\ (mod\ p^2)$, where $m \in \{0,1,2,...,(p-1)\}$. □

The case of complex equiangular tight frames with the maximal number of frame vectors has received much attention in the literature on quantum information theory [21, 12, 26]; see also [13, 6, 7]. The necessary conditions derived in the preceding theorem rule out the “simplest” candidate for a construction of equiangular Parseval frames with Seidel matrices containing pth roots of unity, the case of p^2 vectors in a p-dimensional Hilbert space when p is prime.

Corollary 3.8. *Let $p > 3$ be prime. Then there exists no equiangular (p^2,p)-frame with a pth root signature matrix.*

Proof. By Theorem 3.6 (1), $\mu = (p-2)\sqrt{p+1}$ is an integer, and thus invoking the Rational Root Theorem again, $p+1$ is a perfect square; that is, $p = (r+1)(r-1)$ for some integer r, which contradicts the assumption that p is prime and $p > 3$. □

Even in the case of $p = 3$ there is no equiangular $(9,3)$-frame with a cube root signature matrix. This was shown in [3], along with results that we have generalized here to signature matrices containing pth roots.

Remark 3.9. The previous theorem is a generalization of the cube root case established in Proposition 3.4 of [3]. That result stated that if a nontrivial cube root signature matrix Q of an equiangular (n,k)-frame satisfies $Q^2 = (n-1)I + \mu Q$, then either $n \equiv 0$ $(mod\ 9)$ and $\mu \equiv 7$ $(mod\ 9)$ or $n \equiv 3$ $(mod\ 9)$ and $\mu \equiv 1$ $(mod\ 9)$ or $n \equiv 6$ $(mod\ 9)$ and $\mu \equiv 4$ $(mod\ 9)$. This is the $p = 3$ case of Corollary 3.7. Here $m \in \{0, 1, 2\}$, producing three possibilities: $n = 0p \equiv 0$ $(mod\ 9)$, and $\mu \equiv (0p - 2)$ $(mod\ 9) \equiv 7$ $(mod\ 9)$, or $n = 1p \equiv 3$ $(mod\ 9)$, and $\mu \equiv (1p - 2)$ $(mod\ 9) \equiv 1$ $(mod\ 9)$, or $n = 2p \equiv 6$ $(mod\ 9)$, and $\mu \equiv (2p - 2)$ $(mod\ 9) \equiv 4$ $(mod\ 9)$.

4. pth root signature matrices

In Sections 3.1 and 3.2 we derived some conditions which the parameters of a nontrivial pth root Seidel matrix must satisfy in order to be the signature matrix of an equiangular (n, k)-frame. We now consider a few cases for small p values to illustrate the use of these conditions.

4.1. **Cube root signature matrices.** A search for possible cube root signature matrices was carried out in [3]. The calculations for possible cube root signature matrices yielded eight potential (n, k) pairs for $n < 100$: $(9, 6), (33, 11)$, $(36, 21), (45, 12)$, $(51, 34), (81, 45)$, $(96, 76)$, and $(99, 33)$. Two of these pairs, $(9, 6)$ and $(81, 45)$, were confirmed to exist in Theorems 6.1 and 6.3 of that paper.

4.2. **Fifth root signature matrices.** Next we go through the calculations of possible (n, k) values for $2 \leq k < n \leq 50$ with $p = 5$. As $5e = n - \mu - 2$ by Theorem 3.4, and $\mu = (n - 2k)\sqrt{\frac{n-1}{k(n-k)}} \in \mathbb{Z}$ by the Theorem 2.3 equations, we have that $5e = n - 2 - \sqrt{q}(n - 2k)$, where $q = \frac{n-1}{k(n-k)}$, and $\sqrt{q} \in \mathbb{Q}$. So, our strategy will be to begin with a multiple of 5 as our n value. Step 1 is to check for values of k where $\sqrt{q} = \sqrt{\frac{n-1}{k(n-k)}} \in \mathbb{Q}$. Step 2 is to calculate μ for any k satisfying step 1. We know that $\mu \in \mathbb{Z}$ and that for $n \equiv 5m$ $(mod\ 25), m \in \{0, 1, 2, 3, 4\}$, we must have that $\mu \equiv 5m - 2$ $(mod\ 25)$.

n = 5: Step 1: Since $k = 2, 3$, or 4, $q = \frac{n-1}{k(n-k)} = \frac{4}{6}, \frac{4}{6}$, or $\frac{4}{4}$, and $\sqrt{q}$ must be in $\mathbb{Q}$, $k \neq 2$. Step 2: $\mu = (n - 2k)\sqrt{q} = \frac{-2}{3}, -3$ for $k = 2$ and 3 respectively. As neither of these yields $\mu \equiv 3(mod\ 25)$, there are no possible solutions for $n = 5$.

n = 10: Step 1: For $2 \leq k \leq 9$, we examine each $q = \frac{n-1}{k(n-k)}$ and see that $\sqrt{q}$ is not in $\mathbb{Q}$ when $k = 3, 4, 6$, or 7. Step 2: Now, $\mu = \frac{9}{2}, 0, \frac{-9}{2}, -8$ for $k = 2, 5, 8$, and 9 respectively. As none of these yields $\mu \equiv 8$ $(mod\ 25)$, there are no possible solutions for $n = 10$.

n = 15: Step 1: Checking each q value for $2 \leq k \leq 14$, $\sqrt{q} = \sqrt{\frac{n-1}{k(n-k)}} \in \mathbb{Q}$ for $k = 7$ and 8 only. Step 2: $\mu = \frac{1}{2}, \frac{-1}{2}$ for these values and as neither is equivalent to 13 $(mod\ 25)$, there are no possible solutions for $n = 15$.

n = 20: Step 1: For $2 \leq k \leq 19$, we check each $q = \frac{n-1}{k(n-k)}$ and note that $\sqrt{q} \in \mathbb{Q}$ only when $n = 19$. Step 2: This yields a μ value of -18 which is not equivalent to 18 $(mod\ 25)$, so there are no possible solutions for $n = 20$.

n = 25: Step 1: Looking at each q value for $2 \leq k \leq 24$, we see that $\sqrt{q} = \sqrt{\frac{n-1}{k(n-k)}} \in \mathbb{Q}$ when $k = 10,\ 15$, or 24. Step 2: These lead to μ values of $2, -2, -23$ respectively. $\mu = -2 \equiv 23$ $(mod\ 25)$, and neither 2 nor -23 has the same property. Therefore a $(25, 15)$-frame is the only possible solution for $n = 25$.

- $\mathbf{n = 30}$**:** Step 1: For $2 \leq k \leq 29$, we can see that $\sqrt{q} \in \mathbb{Q}$ only when $k = 29$. Step 2: When $k = 29$, $\mu = -28$, which is not equivalent to 28 $(mod\ 49)$. Thus, there are no possible solutions for $n = 30$.
- $\mathbf{n = 35}$**:** Step 1: Checking each q value for $2 \leq k \leq 34$, $\sqrt{q} = \sqrt{\frac{n-1}{k(n-k)}} \in \mathbb{Q}$ for $k = 17, 18$, and 34 only. Step 2: These three k values correspond to $\mu = \frac{1}{3}, \frac{-1}{3}$, and -33, none of which satisfies $\mu \equiv 10\ (mod\ 25)$, so there are no possible solutions for $n = 35$.
- $\mathbf{n = 40}$**:** Step 1: For $2 \leq k \leq 39$, we examine each $q = \frac{n-1}{k(n-k)}$ and see that $\sqrt{q} \in \mathbb{Q}$ for $k = 39$ only. Step 2: When $k = 39$, then $\mu = -38 \equiv 12\ (mod\ 25) \not\equiv 13\ (mod\ 25)$. Therefore, there are no possible solutions for $n = 40$.
- $\mathbf{n = 45}$**:** Step 1: Looking at each q value for $2 \leq k \leq 44$, we see that $\sqrt{q} = \sqrt{\frac{n-1}{k(n-k)}} \in \mathbb{Q}$ when $k = 12$, 33, or 44. Step 2: These lead to μ values of $7, -7, -43$ respectively. Since $n \equiv 20\ (mod\ 25)$, we know that $\mu \equiv 18\ (mod\ 25)$. Neither 7 nor -43 has this property, but $\mu = -7$ does. Therefore a $(45, 33)$-frame is the only possible solution for $n = 45$.
- $\mathbf{n = 50}$**:** Step 1: Checking each q value for $2 \leq k \leq 49$, we note that $\sqrt{q} \in \mathbb{Q}$ for $k = 5, 10, 18, 25, 32, 40$, and 45. Step 2: These seven k values yield $\mu = \frac{56}{3}, \frac{21}{2}, \frac{49}{12}, 0, \frac{-49}{12}, \frac{-21}{2}$, and $\frac{-56}{3}$. Only 0 is an integer, and as $\mu \equiv 0\ (mod\ 25) \not\equiv 23\ (mod\ 25)$, there are no possible solutions for $n = 50$.

Our search has so far yielded two potential fifth root signature matrices belonging to an equiangular $(25, 15)$-frame and a $(45, 33)$-frame among the Parseval frames of $n \leq 50$ vectors.

4.3. **Seventh root signature matrices.** Now we go through the calculations of possible (n, k) values for $2 \leq k < n \leq 50$ with $p = 7$. Again, our strategy will be to begin with a multiple of 7 as our n value. Step 1 is to check for values of k where $\sqrt{q} = \sqrt{\frac{n-1}{k(n-k)}} \in \mathbb{Q}$. Step 2 is to calculate μ for any k satisfying step 1. We know that $\mu \in \mathbb{Z}$ and that for $n \equiv 7m\ (mod\ 49), m \in \{0, 1, 2, \ldots, 6\}$, we must have that $\mu \equiv 7m - 2\ (mod\ 49)$.

- $\mathbf{n = 7}$**:** Step 1: Since $2 \leq k \leq 6$, $q = \frac{n-1}{k(n-k)} = \frac{6}{10}, \frac{6}{12}, \frac{6}{12}, \frac{6}{10}$, or $\frac{6}{6}$, and $\sqrt{q}$ must be in $\mathbb{Q}$, so $k = 6$. Step 2: $\mu = (n - 2k)\sqrt{q} = -5 \equiv 44\ (mod\ 49)$ for $k = 6$. But $n = 7$ implies that $\mu \equiv 5\ (mod\ 49)$, so there are no possible solutions for $n = 7$.
- $\mathbf{n = 14}$**:** Step 1: Checking q values for $2 \leq k \leq 13$, we find that $\sqrt{q} = \sqrt{\frac{n-1}{k(n-k)}} \in \mathbb{Q}$ for $k = 13$ only. Step 2: As $k = 13$ implies that $\mu = -12 \equiv 37\ (mod\ 49) \not\equiv 12\ (mod\ 49)$, so there are no possible solutions for $n = 14$.
- $\mathbf{n = 21}$**:** Step 1: For $2 \leq k \leq 20$, we examine each $q = \frac{n-1}{k(n-k)}$ and see that $\sqrt{q} \in \mathbb{Q}$ for $k = 5, 16$, and 20. Step 2: These k values correspond to $\mu = \frac{11}{2}, \frac{-11}{2}$, and -19 respectively. However, as $n = 21$, we know that $\mu \equiv 19\ (mod\ 49)$, so there are no possible solutions for $n = 21$.
- $\mathbf{n = 28}$**:** Step 1: Now, for $2 \leq k \leq 27$, we examine each $q = \frac{n-1}{k(n-k)}$ and see that $\sqrt{q} \in \mathbb{Q}$ for $k = 3, 7, 12, 14, 16, 21$, and 27. Step 2: These k values correspond to $\mu = \frac{27}{2}, 6, \frac{3}{2}, 0, \frac{-3}{2}, -6, \frac{-27}{2}$, and -26 respectively. However,

as $n = 28$, we know that $\mu \equiv 26$ $(mod\ 49)$, so there are no possible solutions for $n = 28$.

$\mathbf{n} = \mathbf{35}$: Step 1: Checking q values for $2 \leq k \leq 34$, we find that $\sqrt{q} = \sqrt{\frac{n-1}{k(n-k)}} \in \mathbb{Q}$ for $k = 34$ only. Step 2: As $k = 34$ implies that $\mu = -33 \equiv 16$ $(mod\ 49) \not\equiv 33$ $(mod\ 49)$, so there are no possible solutions for $n = 35$.

$\mathbf{n} = \mathbf{42}$: Step 1: Looking at each q value for $2 \leq k \leq 41$, we see that $\sqrt{q} = \sqrt{\frac{n-1}{k(n-k)}} \in \mathbb{Q}$ when $k = 21$ or 41. Step 2: These lead to μ values of $0, -40$ respectively. Since $n \equiv 42$ $(mod\ 49)$, we know that $\mu \equiv 40$ $(mod\ 49)$. Neither 0 nor -40 has this property, so there are no possible solutions for $n = 42$.

$\mathbf{n} = \mathbf{49}$: Step 1: For $2 \leq k \leq 48$, we examine each $q = \frac{n-1}{k(n-k)}$ and see that $\sqrt{q} \in \mathbb{Q}$ for $k = 21, 28$, and 48. Step 2: These k values correspond to $\mu = 2, -2, -19$ respectively. However, as $n \equiv 0$ $(mod\ 49)$, we know that $\mu \equiv 47$ $(mod\ 49)$. Therefore a $(49, 28)$-frame is the only possible solution for $n = 49$.

Here our search has located one potential seventh root signature matrix belonging to an equiangular $(49, 28)$-frame among the Parseval frames with $n \leq 50$ vectors.

5. Examples of pth root signature matrices with two eigenvalues

As mentioned earlier, the existence of cube root signature matrices satisfying $Q^2 = (n-1)I - \mu Q$ was confirmed in [3]. The first example, corresponding to a $(9, 6)$-frame, is listed here in our notation. To facilitate the display of signature matrices, we only present the exponents of the pth root ω appearing in Q in a matrix A. This means that the entries of Q are $Q_{j,l} = \omega^{A_{j,l}} - \delta_{j,l}$, where $\delta_{j,l} = 0$ if $j \neq l$ and $\delta_{j,j} = 1$ for $j, l \in \{1, 2, \ldots, n\}$.

Example 5.1 (Theorem 6.1 in [3])**.** The matrix

$$A := \begin{pmatrix} 000000000 \\ 000111222 \\ 000222111 \\ 021012012 \\ 021201120 \\ 021120201 \\ 012021021 \\ 012210102 \\ 012102210 \end{pmatrix}$$

gives rise to a 9×9 nontrivial cube root signature matrix Q belonging to an equiangular $(9, 6)$-frame with entries $Q_{j,l} = \omega^{A_{j,l}} - \delta_{j,l}$. The fact that Q has two eigenvalues can be verified explicitly by confirming the matrix identity $Q^2 = 8I - 2Q$.

Based on our analysis of the necessary conditions in the previous section, a nontrivial fifth root Seidel matrix could exist for $n = 25$ and $k = 15$. This is indeed the case.

Example 5.2. Let

$$A := \begin{pmatrix}
0000000000000000000000000\\
0000011111222223333344444\\
0000044444333332222211111\\
0000022222444441111133333\\
0000033333111114444422222\\
0413201234012340123401234\\
0413240123123402340134012\\
0413234012234014012312340\\
0413223401340121234040123\\
0413212340401233401223401\\
0321404321043210432104321\\
0321443210104322104332104\\
0321432104210434321010432\\
0321421043321041043243210\\
0321410432432103210421043\\
0234103142031420314242031\\
0234142031142032031420314\\
0234131420203144203103142\\
0234120314314201420331420\\
0234114203420313142014203\\
0142302413024131302402413\\
0142341302130243024130241\\
0142330241241300241313024\\
0142324130302412413041302\\
0142313024413024130224130
\end{pmatrix},$$

let $\omega = e^{2\pi i/5}$, and, for $j, l \in \{1, 2, \dots, 25\}$, define the matrix Q by $Q_{j,l} := \omega^{A_{j,l}} - \delta_{j,l}$. Then Q is a 25×25 nontrivial fifth root signature matrix of an equiangular $(25, 15)$-frame.

The matrix Q was found by performing an enumerative search in Matlab. To confirm that Q is a signature matrix, one needs only to check that $Q^2 = 24I - 2Q$. This has been verified using the symbolic computation package Mathematica.

The $p^2 \times p^2$ signature matrices in the above two examples have $\mu = -2$, and so $B = Q + I$ gives a corresponding Butson-type Hadamard matrix satisfying $B^2 = p^2 I$ ([4], [25]; see also the online catalogue [28]) for $p \in \{3, 5\}$. We construct such complex $p^2 \times p^2$ Hadamard matrices for any $p \geq 2$. First note that while Lemma 3.3 cannot be extended to values of p which are not prime, the converse holds for primes and nonprimes alike.

Lemma 5.3. *If $\omega \in \mathbb{C}$ such that $\omega \neq 1$, and $\omega^r = 1$ for some $r \in \mathbb{N}$, $r \geq 2$, then $\Sigma_{j=0}^{r-1} \omega^j = 0$.*

Proof. As $\omega^r = 1$ implies that $\omega^r - 1 = 0$, we see that $(\omega - 1)(\Sigma_{j=0}^{r-1} \omega^j) = 0$. Since $\omega \neq 1$, it must be that $\Sigma_{j=0}^{r-1} \omega^j = 0$. □

Theorem 5.4. *For any $p \in \mathbb{N}$, $p \geq 2$, let $\omega = e^{2\pi i/p}$. Define B to be a $p^2 \times p^2$ matrix composed of $p \times p$ blocks where for $1 \leq j \leq p$, $1 \leq l \leq p$, $B_{j,l} = (\omega^{(1-l)(x-1)+(j-1)(y-1)})_{x,y=1}^{p}$, where x and y denote the row and column within the $p \times p$ block $B_{j,l}$. This matrix satisfies $B = B^*$ and $B^2 = p^2 I$.*

Proof. To begin with, we define the diagonal unitary $p \times p$ matrix D with nonzero entries $D_{j,j} = \omega^{j-1}$. The definition of the blocks in B is then simply expressed by

$$B_{j,l} = D^{1-l} J D^{j-1},$$

where J is the $p \times p$ matrix containing only 1's.

With the unitarity of D it is straightforward to verify that $B^*_{j,l} = B_{l,j}$ and thus B is self-adjoint.

Next, we notice that for $x \in \mathbb{Z}_p$ such that $x \neq 0$, $\omega^x \neq 1$ and $(\omega^x)^p = 1$. Thus by Lemma 5.3, $\sum_{j=0}^{p-1} \omega^{jx} = \sum_{j=0}^{p-1} (\omega^x)^j = 0$. Consequently, $JD^xJ = 0$ if $x \neq 0$. This simplifies computing the $p \times p$ blocks of the square $S := B^2$:

$$\begin{aligned} S_{j,l} &= \Sigma_{k=1}^{p} B_{j,k} B_{k,l} \\ &= \Sigma_{k=1}^{p} D^{1-k} J D^{j-1} D^{1-l} J D^{k-1} \\ &= \Sigma_{k=1}^{p} D^{1-k} J D^{j-l} J D^{k-1} \\ &= \begin{cases} 0 & \text{for } j \neq l, \\ p^2 I & \text{for } j = l. \end{cases} \end{aligned}$$

In the last step we use that when $j = l$, each (a, b)-entry of

$$\Sigma_{k=1}^{p} D_{1-k} J J D_{k-1} = p \Sigma_{k=1}^{p} D_{1-k} J D_{k-1} = p \Sigma_{k=1}^{p} B_{k,k}$$

is

$$\omega^0 + \omega^{a-b} + \omega^{2(a-b)} + \ldots + \omega^{(p-2)(a-b)} + \omega^{(p-1)(a-b)} = \begin{cases} 0 & \text{for } a \neq b, \\ p & \text{for } a = b, \end{cases}$$

as $(a - b)$ $(mod\ p) \neq 0$ implies that $\omega^{a-b} \neq 1$. This together with the fact that $\omega^p = 1$ by definition allows us to apply Lemma 5.3 to obtain the desired result. Thus $S_{j,l} = p^2 I$ for $j = l$, and as $S_{j,l} = 0$ for $j \neq l$, we then have that $S = B^2 = p^2 I$. □

If $B = Q + I$ and $B^2 = (Q + I)^2 = p^2 I$, then $Q^2 = (p^2 - 1)I - 2Q$. The matrix Q is by the definition of B in standard form and nontrivial. It is the signature matrix of an equiangular (p^2, k)-frame, with $k = p(p + 1)/2$ following from $\mu = -2$ and Theorem 2.3. We summarize this consequence.

Corollary 5.5. *Let $p \in \mathbb{N}$, $p \geq 2$ and let B be as in the preceding theorem. Then $Q = B - I$ is the $p^2 \times p^2$ nontrivial pth root signature matrix of an equiangular $(p^2, \frac{p(p+1)}{2})$-frame.*

Another consequence of the identity $(Q + I)^2 = nI$ implicit in this construction is that the above examples can be used to obtain signature matrices for $n = p^{2m}$, $m \in \mathbb{N}$, by a tensorization argument as in the cube roots case [3]. Moreover, one can take tensor products of Butson-type Hadamard matrices $Q_1 + I$ and $Q_2 + I$ belonging to different values p_1, p_2. This gives a signature matrix $Q = (Q_1 + I) \otimes (Q_2 + I) - I \otimes I$ containing roots of unity belonging to $p = p_1 p_2$, which is not prime, and thus the necessary conditions derived here do not apply without appropriate modifications. Combinatorial techniques for the case when ω is a primitive pth root of unity but p is not prime deserve to be studied further. Perhaps the most interesting case would be a combinatorial technique for the construction of equiangular Parseval frames with $n = p^2$ vectors in $k = p$ dimensions. Corollary 3.8 shows that the case of p prime will not yield any examples. We hope that this paper may pave the way to conditions for the existence of Seidel matrices in the nonprime case, and that it provides concepts which could serve as an alternative to group-related constructions.

Acknowledgment

The authors would like to thank the anonymous referee for suggesting Corollary 3.8.

References

[1] D. M. Appleby, *Symmetric informationally complete-positive operator valued measures and the extended Clifford group*, J. Math. Phys. **46** (2005), no. 5, 052107, 29. MR2142983 (2006i:81008)

[2] B. G. Bodmann and V. I. Paulsen, *Frames, graphs and erasures*, Linear Algebra Appl. **404** (2005), 118–146. MR2149656 (2006a:42047)

[3] B. G. Bodmann, V. I. Paulsen, and Mark Tomforde, *Equiangular tight frames from complex Seidel matrices containing cube roots of unity*, Linear Algebra and its Applications **430** (2009), 396–417. MR2460526 (2010b:42040)

[4] A.T. Butson, *Generalised Hadamard matrices*, Proceedings of the American Mathematical Society **13** (1962), 894–898. MR0142557 (26:126)

[5] P. Casazza and J. Kovačević, *Equal-norm tight frames with erasures*, Adv. Comp. Math. **18** (2003), 387–430. MR1968127 (2004e:42046)

[6] B. Et-Taoui, *Equiangular lines in C^r*, Indagationes Mathematicae **11** (2) (2000), 201–207. MR1813161 (2002a:51022)

[7] B. Et-Taoui, *Equiangular lines in C^r (part (II))*, Indagationes Mathematicae **13** (4) (2002), 483–486. MR2015832 (2004j:51013)

[8] O. Christensen, *An introduction to frames and Riesz bases*, Birkhäuser, Boston, 2003. MR1946982 (2003k:42001)

[9] C. Godsil and A. Roy, *Equiangular lines, mutually unbiased bases, and spin models*, European J. Combin. **30** (2009), no. 1, 246–262. MR2460230 (2009j:05028)

[10] J.-M. Goethals and J. J. Seidel, *Strongly regular graphs derived from combinatorial designs*, Can. J. Math. **22** (1970), 597–614. MR0282872 (44:106)

[11] V. K. Goyal, J. Kovačević, and J. A. Kelner, *Quantized frame expansions with erasures*, Appl. Comput. Harmon. Anal. **10** (2001), 203–233. MR1829801 (2002h:94012)

[12] M. Grassl, *Tomography of quantum states in small dimensions*, Proceedings of the Workshop on Discrete Tomography and its Applications (Amsterdam), Electron. Notes Discrete Math., vol. 20, Elsevier, 2005, pp. 151–164 (electronic). MR2301093

[13] S. G. Hoggar, *64 lines from a quaternionic polytope*, Geom. Dedicata **69** (1998), no. 3, 287–289. MR1609397 (98m:51013)

[14] R. Holmes and V. I. Paulsen, *Optimal frames for erasures*, Linear Algebra Appl. **377** (2004), 31–51. MR2021601 (2004j:42028)

[15] Thomas W. Hungerford, *Algebra*, Holt, Rinehart and Winston, New York, 1974. MR0354211 (50:6693)

[16] D. Kalra, *Complex equiangular cyclic frames and erasures*, Linear Algebra Appl. **419** (2006), 373–399. MR2277977 (2007j:42024)

[17] J. Kovačević and A. Chebira, *Life beyond bases: The advent of frames (part I)*, IEEE Signal Processing Magazine **24** (2007), no. 4, 86–104.

[18] ———, *Life beyond bases: The advent of frames (part II)*, IEEE Signal Processing Magazine **24** (2007), no. 5, 115–125.

[19] P. W. H. Lemmens and J. J. Seidel, *Equiangular lines*, J. Algebra **24** (1973), 494–512. MR0307969 (46:7084)

[20] J. M. Renes, *Equiangular spherical codes in quantum cryptography*, Quantum Inf. Comput. **5** (2005), no. 1, 81–92. MR2123901 (2005i:81029)

[21] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, *Symmetric informationally complete quantum measurements*, J. Math. Phys. **45** (2004), no. 6, 2171–2180. MR2059685 (2004m:81043)

[22] J. J. Seidel, *A survey of two-graphs*, Colloquio Internazionale sulle Teorie Combinatorie (Proceedings, Rome, 1973), vol. I, Accademia Nazionale dei Lincei, 1976, pp. 481–511. MR0550136 (58:27659)

[23] T. Strohmer, *A note on equiangular tight frames*, Linear Algebra Appl. **429** (2008), no. 1, 326–330. MR2419160 (2009d:42091)

[24] T. Strohmer and R. Heath, *Grassmannian frames with applications to coding and communications*, Appl. Comput. Harmon. Anal. **14** (2003), 257–275. MR1984549 (2004d:42053)

[25] W. Tadej and K. Zyczkowski, *A concise guide to complex Hadamard matrices*, Open Systems and Information Dynamics **13** (2006), 133–177. MR2244963 (2007f:15020)

[26] W. K. Wootters, *Quantum measurements and finite geometry*, Found. Phys. **36** (2006), no. 1, 112–126, Special issue of invited papers dedicated to Asher Peres on the occasion of his seventieth birthday. MR2234897 (2007i:81049)

[27] G. Zauner, *Quantendesigns - Grundzüge einer nichtkommutativen Designtheorie*, Ph.D. thesis, Universität Wien, 1999.

[28] K. Zyczkowski and W. Tadej, http://chaos.if.uj.edu.pl/∼karol/hadamard/index.php, 2009.

Department of Mathematics, University of Houston, Houston, Texas 77204-3008
E-mail address: bgb@math.uh.edu

Department of Mathematics, University of Houston, Houston, Texas 77204-3008
E-mail address: helwood@math.uh.edu