Linear Algebra and its Applications 476 (2015) 98–123

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

Tight frames for cyclotomic fields and other rational vector spaces

Tuan-Yow Chien [a], Victor Flynn [b], Shayne Waldron [a,*]

[a] *Department of Mathematics, University of Auckland, Private Bag 92019, Auckland, New Zealand*
[b] *Mathematical Institute, Oxford University, United Kingdom*

ARTICLE INFO

Article history:
Received 16 December 2014
Accepted 16 February 2015
Available online xxxx
Submitted by R. Brualdi

MSC:
primary 11R18, 15A03, 41A65, 42C15

Keywords:
Finite tight frames
Vector spaces over the rationals
Gramian
Canonical coordinates
Cayley transform
Least squares (minimum norm) solutions
Cyclotomic fields

ABSTRACT

Here we consider the construction of tight frames for rational vector spaces. This is a subtle question, because the inner products on $\mathbb{Q}^d$ are not all isomorphic. We show that a tight frame for $\mathbb{C}^d$ can be arbitrarily approximated by a *tight* frame with vectors in $(\mathbb{Q}+i\mathbb{Q})^d$, and hence there are *many* tight frames for rational inner product spaces. We investigate the "minimal field" for which there is a tight frame with a given Gramian. We then consider the rational vector space given the cyclotomic field $\mathbb{Q}(\omega)$, with ω a primitive n-th root of unity. We give a simple formula for the unique inner product which makes the n-th roots $1,\omega,\omega^2,\dots,\omega^{n-1}$ into a tight frame for $\mathbb{Q}(\omega)$. From this, we conclude that the associated "canonical coordinates" have many nice properties, e.g., multiplication in $\mathbb{Q}(\omega)$ corresponds to convolution, which makes them well suited to computation. Along the way, we give a detailed description of the space of $\mathbb{Q}$-linear dependencies between the n-th roots, which includes a cyclically invariant tight frame.

* Corresponding author.
E-mail address: waldron@math.auckland.ac.nz (S. Waldron).

http://dx.doi.org/10.1016/j.laa.2015.02.021
0024-3795/

1. Introduction

Let $\mathcal{H}$ be a d-dimensional real or complex inner product space. A finite sequence of vectors $(f_j)_{j\in J}$ in $\mathcal{H}$ is a **tight frame** for $\mathcal{H}$ if (for some $A > 0$)

$$f = \frac{1}{A}\sum_{j\in J}\langle f, f_j\rangle f_j, \qquad \forall f \in \mathcal{H}. \tag{1.1}$$

These generalisations of orthonormal bases have recently found many applications, e.g., in signal analysis [12], quantum information theory [16] and orthogonal polynomials of several variables [19]. One of the key motivations is that for inner product spaces with additional structure it may be possible for a tight frame to have certain desirable properties which it is impossible for a basis to have. In the infinite dimensional setting, this has been played out in the theories of wavelets and Gabor systems [3,13], to construct systems with good time–frequency localisation.

The theory of finite tight frames is still in its foundational stages [4]. There is an ongoing effort to construct tight frames with certain properties. Most notably, a set of d^2 equiangular lines in $\mathbb{C}^d$ [17], i.e., d^2 unit vectors (f_j) in $\mathbb{C}^d$ with

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

Central to such constructions (Zauner's conjecture, the SIC problem, spherical 2-designs with the maximal number of vectors) is a description of a subfield of $\mathbb{C}$ in which the inner products lie.

The purpose of this paper is to investigate tight frames for inner product spaces where the field $\mathbb{F}$ is a subfield of $\mathbb{C}$, most notably the rationals $\mathbb{F} = \mathbb{Q}$. This is closely related to the above question of what is the smallest field that a unitary image of a given frame can lie in (so that symbolic calculations can be done). We motivate these questions, and our answers to them, by a careful consideration of the Mercedes-Benz frame (three equally spaced unit vectors in $\mathbb{R}^2$). Key results and observations include:

- Inner products on $\mathbb{Q}$-vector spaces may not be isomorphic (unlike those for $\mathbb{C}$ and $\mathbb{R}$). Nevertheless, a tight frame for a rational inner product space is still determined (up to unitary equivalence) by its Gramian.
- An $n \times n$ matrix Q with entries in a subfield $\mathbb{F} \subset \mathbb{C}$ is the Gramian of a tight frame of n vectors for a d-dimensional inner product space if and only if it is a positive scalar multiple of a rank d orthogonal projection matrix. Such a tight frame can be constructed
  1. In an $\mathbb{F}$-inner product space, by considering the columns of Q.
  2. In $\mathbb{E}^d$, with the Euclidean inner product, where $\mathbb{E}$ is possibly larger than $\mathbb{F}$, by considering the rows of Q.
- A tight frame for $\mathbb{C}^d$ can be arbitrarily approximated by one in $(\mathbb{Q} + i\mathbb{Q})^d$.

- We consider the minimal fields $\mathbb{E}$ for which there is a tight frame in $\mathbb{E}^d$ (with the Euclidean inner product) with a given Gramian. This may be larger than the field generated by the entries of the Gramian.
- We prove certain basic results about the tight frame for the cyclotomic field $\mathbb{Q}(\omega)$ (as a rational vector space) obtained from the canonical coordinates of [21].

2. Inner products on rational vector spaces

Rational vector spaces, and inner products on them [9,10] have important applications in algebraic systems theory [11]. Here we extend real and complex inner products to vector spaces over a subfield $\mathbb{F}$ of $\mathbb{C}$. We show that two such inner products may not be isomorphic, e.g., when $\mathbb{F} = \mathbb{Q}$.

Definition 2.1. An **inner product** on an $\mathbb{F}$-vector space $\mathcal{H}$ is a map $\langle \cdot, \cdot \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{F}$ satisfying

1. $\langle x, x\rangle \geq 0$, $\forall x \in \mathcal{H}$, with $\langle x, x\rangle = 0$ if and only if $x = 0$.
2. $\langle \alpha x + \beta y, z\rangle = \alpha\langle x, z\rangle + \beta\langle y, z\rangle$, $\forall \alpha, \beta \in \mathbb{F}$, $\forall x, y, z \in \mathcal{H}$.
3. $\overline{\langle x, y\rangle} = \langle y, x\rangle$, $\forall x, y \in \mathcal{H}$.

We say $\mathcal{H}$ is an **inner product space** over $\mathbb{F}$, or an $\mathbb{F}$**-inner product space**.

The conjugate-linearity in the second variable implies that $\overline{\mathbb{F}} = \mathbb{F}$ (when $\mathcal{H} \neq \{0\}$).

Example 2.1. The Euclidean inner product

$$\langle\!\langle x, y\rangle\!\rangle := x_1\overline{y_1} + \cdots + x_d\overline{y_d}, \qquad x, y \in \mathbb{C}^d$$

restricted to $\mathbb{F}^d$ is an inner product on the $\mathbb{F}$-vector space $\mathbb{F}^d$.

Definition 2.2. The **Gramian matrix** (or **Gram matrix** or **Gramian**) of a sequence of vectors $(v_1, \ldots, v_n)$ in an $\mathbb{F}$-inner product space $\mathcal{H}$ is the matrix

$$[\langle v_k, v_j\rangle]_{j,k=1}^n.$$

For the Euclidean inner product on $\mathbb{F}^d$, the Gramian is given by

$$V^*V = [\langle\!\langle v_k, v_j\rangle\!\rangle]_{j,k=1}^n,$$

where V is the **synthesis map**

$$V = [v_1, \ldots, v_n] : \mathbb{F}^n \to \mathcal{H} : a \mapsto a_1v_1 + \cdots + a_nv_n,$$

and V^* is the Hermitian transpose of the matrix V.

Here the term *positive (semi)definite matrix* is with respect to the Euclidean inner product.

Proposition 2.1. *All inner products on a d-dimensional $\mathbb{F}$-vector space $\mathcal{H}$ have the form*

$$\langle x, y\rangle = \langle\!\langle [x], M[y]\rangle\!\rangle, \tag{2.2}$$

where $M \in \mathbb{F}^{d\times d}$ is a positive definite matrix, $\langle\!\langle\cdot,\cdot\rangle\!\rangle$ is the Euclidean inner product, and

$$[x] = B^{-1}x, \qquad B : \mathbb{F}^d \to \mathcal{H} : a \mapsto a_1w_1 + \cdots a_dw_d,$$

are the coordinates of $x \in \mathcal{H}$ with respect to any fixed basis $(w_1, \ldots, w_d)$ for $\mathcal{H}$. In particular, the Gramian of a sequence of vectors in $\mathcal{H}$ is a positive semidefinite matrix.

Proof. Let $\mathbb{K}$ be the closure of $\mathbb{F}$ in $\mathbb{C}$, which is either $\mathbb{R}$ or $\mathbb{C}$. Let $\mathcal{K}$ be the extension of $\mathcal{H}$ to a d-dimensional $\mathbb{K}$-vector space (in the usual way), and

$$[x]_{\mathcal{K}} = B_{\mathcal{K}}^{-1}x, \qquad B_{\mathcal{K}} : \mathbb{K}^d \to \mathcal{K} : a \mapsto a_1w_1 + \cdots a_dw_d.$$

By a density argument, there is an extension of the inner product $\langle\cdot,\cdot\rangle$ to the $\mathbb{K}$-vector space $\mathcal{K}$, which we denote by $\langle\cdot,\cdot\rangle_{\mathcal{K}}$. Since $\mathbb{K}$ is $\mathbb{C}$ or $\mathbb{R}$, there is a unique positive definite matrix $M \in \mathbb{K}^{d\times d}$ with

$$\langle x, y\rangle_{\mathcal{K}} = \langle\!\langle [x]_{\mathcal{K}}, M[y]_{\mathcal{K}}\rangle\!\rangle, \qquad x, y \in \mathcal{K}.$$

Take $x = v_j = B_{\mathcal{K}}e_j$ and $y = v_k = B_{\mathcal{K}}e_k$, to obtain

$$\langle v_j, v_k\rangle = \langle v_j, v_k\rangle_{\mathcal{K}} = \langle\!\langle e_j, Me_k\rangle\!\rangle = \overline{m_{jk}} = m_{kj} \in \mathbb{F}.$$

Conversely, let $B : \mathbb{F}^d \to \mathcal{H}$ be a fixed basis map, then (2.2) defines a different inner product on $\mathcal{H}$ for each positive definite $M \in \mathbb{F}^{d\times d}$.

The Gramian of a sequence of vectors $v_1, \ldots, v_n$ in $\mathcal{H}$ is

$$[\langle v_k, v_j\rangle] = [\langle\!\langle [v_k], M[v_j]\rangle\!\rangle] = [\langle\!\langle M^{\frac{1}{2}}B^{-1}v_k, M^{\frac{1}{2}}B^{-1}v_j\rangle\!\rangle] = W^*W,$$

where $W = [M^{\frac{1}{2}}B^{-1}v_1, \ldots, M^{\frac{1}{2}}B^{-1}v_n] \in \mathbb{F}^{d\times n}$, and hence is positive semidefinite. □

Definition 2.3. We say $\mathbb{F}$-inner product spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ with inner products $\langle\cdot,\cdot\rangle_j$ are **isomorphic** if there is an invertible $\mathbb{F}$-linear map $\sigma : \mathcal{H}_1 \to \mathcal{H}_2$ with

$$\langle f, g\rangle_1 = \langle \sigma f, \sigma g\rangle_2, \qquad \forall f, g \in \mathcal{H}_1.$$

Theorem 2.1. *Inner product spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ over a subfield $\mathbb{F}$ of $\mathbb{C}$ are isomorphic if and only if the Gramian matrices M_1 and M_2 for any choice of bases are $*$-conjugate, i.e.,*

$$M_1 = C^* M_2 C, \qquad C \in \mathbb{F}^{d\times d}.$$

In particular, $\mathcal{H}_1$ is isomorphic to $\mathbb{F}^d$ (with the Euclidean inner product) if and only if M_1 is the Gramian of a sequence of vectors in $\mathbb{F}^d$.

Proof. By Proposition 2.1, the inner products have the form

$$\langle x, y\rangle_\ell = \langle\!\langle B_\ell^{-1}x, M_\ell B_\ell^{-1}y\rangle\!\rangle,$$

where $B_\ell : \mathbb{F}^d \to \mathcal{H}_\ell$ is a basis map, and M_ℓ is positive definite with entries

$$(M_\ell)_{jk} = \langle\!\langle e_k, M_\ell e_j\rangle\!\rangle = \langle B_\ell e_k, B_\ell e_j\rangle \in \mathbb{F}.$$

These inner products are equivalent if and only if

$$\begin{aligned}\langle x, y\rangle_1 = \langle \sigma x, \sigma y\rangle_2 \quad &\iff \quad \langle\!\langle B_1^{-1}x, M_1 B_1^{-1}y\rangle\!\rangle = \langle\!\langle B_2^{-1}\sigma x, M_2 B_2^{-1}\sigma y\rangle\!\rangle \\ &\iff \quad M_1 = C^* M_2 C, \quad \text{where } C = B_2^{-1}\sigma B_1 \in \mathbb{F}^{d\times d},\end{aligned}$$

i.e., the Gramians M_1 and M_2 are $*$-conjugate (the term conjunctive is also used).

Now suppose $\mathcal{H}_2 = \mathbb{F}^d$ (with the Euclidean inner product). Take the standard orthonormal basis for $\mathcal{H}_2$, to obtain the condition $M_1 = C^* M_2 C = C^* I C = C^* C$, i.e., M_1 is the Gramian matrix of the columns of C. $\square$

Example 2.2. For $\mathbb{F}^1$, the $\mathbb{F}$-inner products have the form

$$\langle x, y\rangle_a = a\, x_1 \overline{y_1}, \qquad a > 0,\ a \in \mathbb{F}.$$

Two such inner products for $a = a_1, a_2$ are isomorphic via $C = [c_{11}]$ if and only if

$$a_1 = \overline{c_{11}} a_1 c_{11} = |c_{11}|^2 a_2,$$

i.e., $\mathbb{F}$ has an element with modulus $\sqrt{\frac{a_1}{a_2}}$. For example,

$$\langle x, y\rangle_1 = x_1 y_1, \qquad \langle x, y\rangle_2 = 2x_1 y_1$$

do not give isomorphic $\mathbb{Q}$-inner products.

Example 2.3. The inner product on $\mathbb{Q}^2$ given by

$$\langle u, v\rangle := \langle\!\langle u, Mv\rangle\!\rangle, \qquad M := \begin{pmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{pmatrix}$$

is not isomorphic to the Euclidean inner product, since

$$M = C^*C, \quad C = \begin{pmatrix} x & a \\ y & b \end{pmatrix} \quad \Longrightarrow \quad x = -\frac{a}{2} \pm \frac{\sqrt{3}}{2}b.$$

Proposition 2.2. *If $\mathbb{F} \cap \mathbb{R}$ is closed under taking square roots, then all $\mathbb{F}$-inner products on a d-dimensional space are isomorphic.*

Proof. Let $\mathcal{H}$ be a d-dimensional $\mathbb{F}$-vector space. For any inner product $\langle\cdot,\cdot\rangle$ on $\mathcal{H}$, the Gram–Schmidt process allows us to construct an orthogonal basis for $\mathcal{H}$, and this can be normalised, since for any $v \in \mathcal{H}$, $\langle v, v\rangle \in \mathbb{F} \cap \mathbb{R}$, and so $\|v\| = \sqrt{\langle v, v\rangle} \in \mathbb{F}$. Hence, for inner products $\langle\cdot,\cdot\rangle_1$ and $\langle\cdot,\cdot\rangle_2$ on $\mathcal{H}$, we can find orthonormal bases $(v_1, \dots, v_d)$ and $(w_1, \dots, w_d)$ for $\mathcal{H}$. The map $\sigma : v_j \mapsto w_j$ is an isomorphism between the inner product spaces given by $\langle\cdot,\cdot\rangle_1$ and $\langle\cdot,\cdot\rangle_2$. □

3. Tight frames and their construction from the Gramian

Here we show that $Q \in \mathbb{F}^{n\times n}$ is the Gramian of a tight frame for a d-dimensional $\mathbb{F}$-inner product space $\mathcal{H}$ if and only if Q is a positive scalar multiple of a rank d orthogonal projection matrix. We then show how to construct such a tight frame from the columns of Q, and how to construct a tight frame for $\mathbb{E}^d$, with the Euclidean inner product and $\mathbb{E}$ a field containing $\mathbb{F}$, with Gramian Q from the rows of Q.

Our results are motivated by a careful consideration of the **Mercedes-Benz** frame which consists of three equally spaced equal norm vectors in $\mathbb{R}^2$, e.g., the columns of

$$V = \begin{pmatrix} 1 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} \end{pmatrix}, \tag{3.3}$$

which has Gramian

$$V^*V = \begin{pmatrix} 1 & -\frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & 1 & -\frac{1}{2} \\ -\frac{1}{2} & -\frac{1}{2} & 1 \end{pmatrix}. \tag{3.4}$$

The tight frame definition (1.1) extends to an inner product space $\mathcal{H}$ over $\mathbb{F}$. By the polarisation identity, this is equivalent to the more standard definition

$$\|f\|^2 = \frac{1}{A}\sum_{j\in J} |\langle f, f_j\rangle|^2, \qquad \forall f \in \mathcal{H}.$$

It follows from (1.1) that a tight frame spans $\mathcal{H}$, and the **frame bound** A belongs to $\mathbb{F}$. When A is taken to be 1 (replace f_j by $\frac{f_j}{\sqrt{A}}$) a tight frame is said to be **normalised** (the term **Parseval tight frame** is also commonly used).

Remark 3.1. If $\mathbb{R} \not\subset \mathbb{F}$, then it may not be possible to normalise a tight frame (f_j), on account of $\sqrt{A}$ not being in $\mathbb{F}$. For example, the three equally spaced unit vectors (3.3) lie in $\mathbb{F}^2$, $\mathbb{F} = \mathbb{Q}(\sqrt{3})$, with $A = \frac{3}{2}$, so that $\sqrt{A} \notin \mathbb{F}$. Nevertheless, the tight frame expansion (1.1) allows the identity to be written as a linear combination of rank one orthogonal projections

$$I = \sum_{j \in J} c_j P_j, \qquad \forall f \in \mathcal{H}, \tag{3.5}$$

where $P_j = \frac{f_j f_j^*}{\|f_j\|^2}$, $c_j = \frac{\|f_j\|^2}{A}$. The pair $(c_j), (P_j)$ is known as a **fusion frame** [5]. For the three equally spaced unit vectors (3.5) gives

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{2}{3}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{2}{3}\begin{pmatrix} \frac{1}{4} & -\frac{\sqrt{3}}{4} \\ -\frac{\sqrt{3}}{4} & \frac{3}{4} \end{pmatrix} + \frac{2}{3}\begin{pmatrix} \frac{1}{4} & \frac{\sqrt{3}}{4} \\ \frac{\sqrt{3}}{4} & \frac{3}{4} \end{pmatrix}.$$

Remark 3.2. Tight frames $(f_j)_{j \in J}$ for $\mathcal{H}$ are characterised by the following variational condition [20]

$$\sum_{j \in J} \sum_{k \in J} |\langle f_j, f_k \rangle|^2 = \frac{1}{d}\Big(\sum_{j \in J} \langle f_j, f_j \rangle\Big)^2, \qquad d = \dim(\mathcal{H}), \tag{3.6}$$

where the constant A is given by

$$dA = \sum_{j \in J} \|f_j\|^2. \tag{3.7}$$

Thus a tight frame for an $\mathbb{F}$-inner product space $\mathcal{H}$ is tight frame for the $\mathbb{K}$-inner product space $\mathcal{K}$, $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$ (the closure of $\mathbb{F}$ in $\mathbb{C}$), as detailed in the proof of Proposition 2.1, and for the complexification of $\mathcal{K}$. For example, a tight frame for $\mathbb{Q}^d$ (with the Euclidean inner product) is a tight frame for $\mathbb{R}^d$ and $\mathbb{C}^d$.

Theorem 3.1 *(Characterisation, column construction). An $n \times n$ matrix Q with entries in a subfield $\mathbb{F}$ of $\mathbb{C}$ is the Gramian of a tight frame for a d-dimensional inner product space $\mathcal{H}$ over $\mathbb{F}$ if and only if*

$$P = \frac{d}{\operatorname{trace}(Q)} Q$$

is an orthogonal projection matrix of rank d. Moreover, the vectors of the tight frame may be taken to be the columns of Q, where $\mathcal{H} = \operatorname{col}(Q) \subset \mathbb{F}^n$ with

$$\langle \cdot, \cdot \rangle = \frac{d}{\operatorname{trace}(Q)} \boldsymbol{\langle} \cdot, \cdot \boldsymbol{\rangle}.$$

Proof. ($\Longrightarrow$) Let (f_j) be a tight frame for a d-dimensional $\mathbb{F}$-inner product space $\mathcal{H}$, with Gramian Q. Take $f = f_\ell$ in (1.1), then the inner product with f_k, to get

$$f_\ell = \frac{1}{A}\sum_j \langle f_\ell, f_j\rangle f_j \quad \Longrightarrow \quad \langle f_k, f_\ell\rangle = \frac{1}{A}\sum_j \langle f_k, f_j\rangle\langle f_j, f_\ell\rangle,$$

i.e., $Q = \frac{1}{A}Q^2$. By (3.7), $dA = \operatorname{trace}(Q)$, and so $P^2 = P$, i.e., P (which is positive semidefinite) is an orthogonal projection matrix.

($\Longleftarrow$) Suppose that Q (of size n) has entries in $\mathbb{F}$, and $P = \frac{d}{\operatorname{trace}(Q)}Q$ is a rank d orthogonal projection matrix. Let $\mathcal{H}$ be the d-dimensional subspace of $\mathbb{F}^n$ spanned by (Qe_j) (the columns of Q), and define an $\mathbb{F}$-inner product on $\mathcal{H}$ by

$$\langle f, g\rangle := \frac{d}{\operatorname{trace}(Q)}\boldsymbol{\langle} f, g\boldsymbol{\rangle}, \qquad \forall f, g \in \mathcal{H}.$$

Since $f = Pf$, $f \in \mathcal{H}$, we can expand

$$f = Pf = P\Big(\sum_j \boldsymbol{\langle} Pf, e_j\boldsymbol{\rangle} e_j\Big) = \sum_j \boldsymbol{\langle} f, Pe_j\boldsymbol{\rangle} Pe_j = \frac{d}{\operatorname{trace}(Q)}\sum_j \langle f, Qe_j\rangle Qe_j.$$

Thus (Qe_j) is a tight frame for $\mathcal{H}$, whose Gramian matrix has entries

$$\langle Qe_j, Qe_k\rangle = \frac{d}{\operatorname{trace}(Q)}\boldsymbol{\langle} Qe_j, Qe_k\boldsymbol{\rangle} = \boldsymbol{\langle} Pe_j, Qe_k\boldsymbol{\rangle} = \boldsymbol{\langle} e_j, PQe_k\boldsymbol{\rangle} = \boldsymbol{\langle} e_j, Qe_k\boldsymbol{\rangle} = Q_{jk},$$

i.e., there is tight frame for $\mathcal{H}$ with Gramian Q. $\square$

Corollary 3.1. *If the Gramian of a tight frame has rational entries, then there is a $\mathbb{Q}$-inner product space and a tight frame for it which has this Gramian.*

Example 3.1. Let Q be the Gramian (3.4) of three equally spaced vectors in $\mathbb{R}^2$. This has rational entries, and so it columns

$$w_1 = \begin{pmatrix} 1 \\ -\frac{1}{2} \\ -\frac{1}{2} \end{pmatrix}, \quad w_2 = \begin{pmatrix} -\frac{1}{2} \\ 1 \\ -\frac{1}{2} \end{pmatrix}, \quad w_3 = \begin{pmatrix} -\frac{1}{2} \\ -\frac{1}{2} \\ 1 \end{pmatrix},$$

form an equiangular tight frame for $\mathcal{H} = \operatorname{span}_{\mathbb{Q}}\{w_1, w_2, w_3\}$ with the $\mathbb{Q}$-inner product $\langle\cdot,\cdot\rangle = \frac{2}{3}\boldsymbol{\langle}\cdot,\cdot\boldsymbol{\rangle}$, which has Gramian Q. For example,

$$\langle w_1, w_1\rangle = \frac{2}{3}\boldsymbol{\langle} \begin{pmatrix} 1 \\ -\frac{1}{2} \\ -\frac{1}{2} \end{pmatrix}, \begin{pmatrix} 1 \\ -\frac{1}{2} \\ -\frac{1}{2} \end{pmatrix} \boldsymbol{\rangle} = 1, \qquad \langle w_1, w_2\rangle = \frac{2}{3}\boldsymbol{\langle} \begin{pmatrix} 1 \\ -\frac{1}{2} \\ -\frac{1}{2} \end{pmatrix}, \begin{pmatrix} -\frac{1}{2} \\ 1 \\ -\frac{1}{2} \end{pmatrix} \boldsymbol{\rangle} = -\frac{1}{2}.$$

We can represent $\langle\cdot,\cdot\rangle$ as in inner product on $\mathbb{Q}^2$ using (2.2). Choose w_1, w_2 (the first two columns of Q) as a basis for $\mathcal{H}$, so that

$$B:\mathbb{Q}^2\to\mathcal{H}:a\mapsto a_1w_1+a_2w_2,\qquad [w_1]=\begin{pmatrix}1\\0\end{pmatrix},\quad [w_2]=\begin{pmatrix}0\\1\end{pmatrix},\quad [w_1]=\begin{pmatrix}-1\\-1\end{pmatrix},$$

and

$$\langle x,y\rangle=\langle\!\langle [x],M[x]\rangle\!\rangle,\qquad M=\begin{pmatrix}1 & -\frac{1}{2}\\ -\frac{1}{2} & 1\end{pmatrix},$$

where $[x]=B^{-1}x$, and M was calculated by

$$\langle w_j,w_k\rangle=\langle\!\langle [w_j],M[w_k]\rangle\!\rangle=\langle\!\langle e_j,Me_k\rangle\!\rangle=m_{jk},\qquad 1\le j,k\le 2.$$

We now show how to construct (realise) a tight frame with a given Gramian in Euclidean space.

Theorem 3.2 *(Row construction). Let $Q\in\mathbb{C}^{n\times n}$ be a positive scalar multiple of an orthogonal projection matrix of rank d. The columns of $V=[v_1,\dots,v_n]\in\mathbb{C}^{d\times n}$ are a tight frame for $\mathbb{C}^d$ with Gramian Q if and only if the rows of V are an orthogonal basis for the row space of Q and have length $\sqrt{A}$, $A=\operatorname{trace}(Q)/d$.*

Proof. Suppose that (v_j) is a tight frame. The tight frame condition (1.1) can be written in matrix form as $I=\frac{1}{A}VV^*$, i.e., the rows of V are orthogonal with length $\sqrt{A}$. The condition $VV^*=AI$ implies that the row space of the Gramian V^*V satisfies

$$\operatorname{row}(V^*V)\subset\operatorname{row}(VV^*V)=\operatorname{row}(AV)=\operatorname{row}(V)\subset\operatorname{row}(V^*V),$$

and hence is equal to the row space of V.

Conversely, suppose that Q is a nonzero scalar multiple of an orthogonal projection of rank d, and V has orthogonal rows of length $\sqrt{A}$, $A=\frac{1}{d}\operatorname{trace}(Q)$ which span $\operatorname{row}(Q)$. Then

$$(\frac{1}{A}V^*V)^2=\frac{1}{A^2}V^*(VV^*)V=\frac{1}{A^2}V^*(AI)V=\frac{1}{A}V^*V,$$

so that $\frac{1}{A}V^*V$ is an orthogonal projection matrix, with the same row space, and hence column space, as the orthogonal projection $P=\frac{1}{A}Q$, and hence they are equal, i.e., $Q=V^*V$. $\square$

If $Q\in\mathbb{C}^{n\times n}$ is a positive scalar multiple of an orthogonal projection matrix, then we call any $V=[v_1,\dots,v_n]\in\mathbb{C}^{d\times n}$ (or the tight frame given by its columns) with $Q=V^*V$ a **realisation** of the “Gramian” Q (in the field $\mathbb{E}$ generated by the entries of V).

Example 3.2. Let Q be the Gramian (3.4) of three equally spaced vectors in $\mathbb{R}^2$. Then applying Gram–Schmidt to the first two rows $(1, -\frac{1}{2}, -\frac{1}{2})$, $(-\frac{1}{2}, 1, -\frac{1}{2})$ of Q gives

$$V = \begin{bmatrix} 1 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} \end{bmatrix}, \tag{3.8}$$

with $Q = V^*V$. Here the entries of the vectors lie in the field $\mathbb{Q}(\sqrt{3})$.

Example 3.3. Consider the four equiangular unit vectors in $\mathbb{C}^2$ given by the columns of

$$V = [v, Sv, \Omega v, S\Omega],$$

where

$$v := \frac{1}{\sqrt{6}} \begin{bmatrix} \sqrt{3+\sqrt{3}} \\ \frac{1}{\sqrt{2}}(1+i)\sqrt{3-\sqrt{3}} \end{bmatrix}, \qquad S := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \Omega := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

This tight frame has Gramian

$$Q = \begin{bmatrix} 1 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & -\frac{i}{\sqrt{3}} \\ \frac{1}{\sqrt{3}} & 1 & -\frac{i}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{3}} & \frac{i}{\sqrt{3}} & 1 & -\frac{1}{\sqrt{3}} \\ \frac{i}{\sqrt{3}} & \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{3}} & 1 \end{bmatrix}.$$

Applying Gram–Schmidt to the first two rows of Q gives the tight frame

$$W = \begin{bmatrix} 1 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & -\frac{i}{\sqrt{3}} \\ 0 & \frac{\sqrt{2}}{\sqrt{3}} & -\frac{i}{\sqrt{2}} - \frac{1}{\sqrt{2}\sqrt{3}} & \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}\sqrt{3}} \end{bmatrix},$$

which has Gramian Q. The entries of the vectors lie in the field

$$\mathbb{Q}(\sqrt{3}, i, \sqrt{2}) = \mathbb{Q}(\sqrt{3}, i, \sqrt{3+\sqrt{3}}) = \mathbb{Q}(\sqrt{d}, a), \qquad d = 2, \quad a = \sqrt{(d-3)(d+1)} = \sqrt{-3}.$$

The presentation $\mathbb{Q}(\sqrt{d}, a)$ fits into the general theory for SICs proposed by [1].

There is no tight frame of three equally spaced unit vectors in $\mathbb{Q}^2$ with the Euclidean inner product, i.e., having the Gramian (3.4). This follows, since if (a, b) and (x, y) are equally spaced unit vectors (in $\mathbb{Q}^2$), then

$$\left\langle \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} x \\ y \end{pmatrix} \right\rangle = ax + by = -\frac{1}{2} \quad \Longrightarrow \quad x = -\frac{a}{2} \pm \frac{\sqrt{3}}{2} b. \tag{3.9}$$

Thus the smallest field $\mathbb{F}$ for which there are three equally spaced unit vectors in $\mathbb{F}^2$ is $\mathbb{Q}(\sqrt{3})$, we will investigate this "minimal field" next (Section 4). We will also show that there are tight frames in $\mathbb{Q}^2$ which arbitrarily approximate the three equally spaced unit vectors (Section 5).

4. The minimal field of a tight frame

Given a d-dimensional tight frame with $n \times n$ Gramian Q, we call the field generated by its inner products (the entries of Q) the **Gramian field**. If $\mathbb{F}$ is the Gramian field, then there exist an inner product on $\mathbb{F}^n$ and vectors in $\mathbb{F}^n$ with this Gramian (Theorem 3.1). Scaling the vectors in a frame can change the Gramian field. The **base field** of a tight frame is the Gramian field of the associated normalised tight frame, which has Gramian

$$P = \frac{d}{\operatorname{trace}(Q)} Q.$$

The base field is

- The unique smallest Gramian field that can be obtained by multiplying a frame by a nonzero scalar.
- The field generated by the ratios of the entries of the Gramian (which are invariant under scaling).
- The Gramian field when any entry of the Gramian is rational.

For the three equally space unit vectors with Gramian

$$\begin{pmatrix} 1 & -\frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & 1 & -\frac{1}{2} \\ -\frac{1}{2} & -\frac{1}{2} & 1 \end{pmatrix},$$

the Gramian field and the base field are $\mathbb{Q}$.

We define a **minimal field** for a d-dimensional frame with Gramian Q to be a smallest field $\mathbb{E}$ for which there is a realisation of Q, i.e., a $V \in \mathbb{E}^{d\times n}$ with

$$Q = V^* V.$$

We observe that

- Minimal fields exist, and they contain the base field (Theorem 3.2).
- Minimal fields need not be unique, e.g., if $Q = [2]$, then $V = [\sqrt{2}]$ and $V = [1 + i]$ are realisations of Q, which give minimal fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i)$.

Example 4.1. For the three equally spaced unit vectors, the calculation (3.9) shows that the base field is $\mathbb{Q}$, and that there is a unique minimal field $\mathbb{Q}(\sqrt{3})$.

This argument extends to the $n \geq 3$ equally spaced unit vectors in $\mathbb{R}^2$ given by the columns of

$$V = \begin{bmatrix} 1 & \cos\theta & \cos 2\theta & \cdots & \cos(n-1)\theta \\ 0 & \sin\theta & \sin 2\theta & \cdots & \sin(n-1)\theta \end{bmatrix}, \qquad \theta := \frac{2\pi}{n}.$$

Since $\cos j\theta \cos k\theta + \sin j\theta \sin k\theta = \cos(j-k)\theta$, the Gramian matrix is given by

$$Q = V^*V = [\cos(j-k)\theta]_{j,k=1}^{n}, \tag{4.10}$$

and so the base field is $\mathbb{Q}(\cos\theta)$. For unit vectors (a,b) and (x,y), we have

$$\left\langle \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} x \\ y \end{pmatrix} \right\rangle = ax + by = \cos\theta \quad \Longrightarrow \quad x = (\cos\theta)a \pm (\sin\theta)b, \tag{4.11}$$

and so a minimal field for the n equally spaced vectors is $\mathbb{Q}(\cos\theta, \sin\theta)$, $\theta = \frac{2\pi}{n}$.

Example 4.2. For the four equiangular unit vectors of Example 3.3, the base field is $\mathbb{Q}(\sqrt{3}, i)$, and since V and W give realisations, a minimal field is contained within $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i)$. Left multiplying W by the unitary matrix $U = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}}(1+i) \end{pmatrix}$ gives the realisation

$$UW = \begin{bmatrix} 1 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & -\frac{i}{\sqrt{3}} \\ 0 & \frac{1+i}{\sqrt{3}} & \frac{1-i}{2} - \frac{1+i}{2\sqrt{3}} & \frac{1+i}{2} + \frac{i-1}{2\sqrt{3}} \end{bmatrix},$$

and so we conclude that the base field $\mathbb{Q}(\sqrt{3}, i)$ is the unique minimal field. This realisation of the $d = 2$ SIC is new: all the other known realisations are in $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i)$.

Example 4.2 shows that a realisation of some Q obtained by Gram–Schmidt orthogonalisation of its rows need not give a minimal field, even if it is unique. This is still the case if symmetric (Löwdin) Gram–Schmidt is used, e.g., applying this to the first two rows of the W in Example 4.2 gives the realisation

$$\frac{1}{6}\begin{bmatrix} \sqrt{18+6\sqrt{6}} & \sqrt{18-6\sqrt{6}} & \sqrt{9+3\sqrt{6}} + i\sqrt{9-3\sqrt{6}} & -\sqrt{9-3\sqrt{6}} - i\sqrt{9+3\sqrt{6}} \\ \sqrt{18-6\sqrt{6}} & \sqrt{18+6\sqrt{6}} & -\sqrt{9-3\sqrt{6}} - i\sqrt{9+3\sqrt{6}} & \sqrt{9+3\sqrt{6}} + i\sqrt{9-3\sqrt{6}} \end{bmatrix}$$

The following is another example.

Example 4.3. Consider the harmonic frame [8] of three vectors for $\mathbb{C}^2$ given by the columns of

$$W = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \end{bmatrix}, \qquad \omega := e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i.$$

Gram–Schmidt applied to the Gramian

$$Q = W^*W = \begin{bmatrix} 2 & \omega+1 & -\omega \\ -\omega & 2 & \omega+1 \\ \omega+1 & -\omega & 2 \end{bmatrix}$$

gives the realisation

$$V = \begin{bmatrix} \sqrt{2} & \frac{\omega+1}{\sqrt{2}} & \frac{-\omega}{\sqrt{2}} \\ 0 & \frac{\sqrt{3}}{\sqrt{2}} & \frac{\sqrt{3}}{\sqrt{2}}(\omega+1) \end{bmatrix}.$$

The entries of V generate the field $\mathbb{Q}(\sqrt{2}, \omega)$, which is *not* a minimal field, since the entries of W generate the base field $\mathbb{Q}(\omega)$, which is therefore the unique minimal field.

In view of these examples, finding a minimal field amounts to finding an orthogonal basis of vectors (of a fixed length $\sqrt{A}$) for the d-dimensional subspace row(Q) of $\mathbb{C}^n$ with components in as small as possible field. This appears to be a difficult problem in general.

It is interesting to observe that Gram–Schmidt applied to the rows of the Gramian gives the minimal field for n equally spaced unit vectors.

Example 4.4. Applying Gram–Schmidt to the first two rows

$$w_1 = (1, \cos\theta, \cos 2\theta, \ldots), \qquad w_2 = (\cos\theta, 1, \cos\theta, \cos 2\theta, \ldots),$$

of the Gramian (4.10) for n equally spaced unit vectors gives the following row which is orthogonal to w_1

$$w_2' := w_2 - (\cos\theta)w_1 = (0, 1 - \cos\theta\cos\theta, \cos\theta - \cos\theta\cos 2\theta, \cos 2\theta - \cos\theta\cos 3\theta, \ldots).$$

Since $1 - \cos^2\theta = \sin^2\theta$ and $(w_2)_1 = 0$, the rows w_1 and $(1/\sin\theta)w_2'$ are an orthogonal basis for col(Q) with length $\sqrt{A}$. The corresponding V with these rows has components in $\mathbb{Q}(\cos\theta, \sin\theta)$, which is a minimal field.

5. The density of rational frames

The variational condition (3.6) implies that the $V = [v_1, \ldots, v_d] \in \mathbb{C}^{d\times n}$ giving tight frames form an algebraic variety [7]. The subvariety obtained by imposing the equal norm condition $\|v_1\| = \cdots = \|v_n\|$ is of particular interest for applications, e.g., Cahill et al. [6] consider its path connectedness.

Here we show that the rational points are dense on the algebraic variety of tight frames, i.e., each tight frame of n vectors for $\mathbb{C}^d$ can be arbitrarily well approximated by a *tight* frame with vectors in $(\mathbb{Q} + i\mathbb{Q})^d$. This a nontrivial result, since the perturbation of a tight frame is not a tight frame (in general).

In view of Theorems 3.1 and 3.2, up to a scalar, a tight frame $V = [v_1, \ldots, v_n] \in \mathbb{C}^{d\times n}$ is equal to a $d \times n$ submatrix of an $n \times n$ unitary matrix. Thus to approximate a tight frame by one with entries in $\mathbb{Q}$, it suffices to approximate an appropriate unitary matrix by one with entries in $\mathbb{Q}$. This can be done using the Cayley transform (cf. [15]).

Let $A \in \mathbb{C}^{n\times n}$ be *skew Hermitian*, i.e.,

$$A^* = -A.$$

Then $A + I$ is invertible, and

$$U := \frac{I - A}{I + A}$$

is a unitary matrix, called the **Cayley transform** of A. If U is unitary, and does not have -1 as an eigenvalue (so that $I + U$ is invertible), then

$$A := \frac{I - U}{I + U}$$

is skew Hermitian. These maps are inverses of each other, and so the unitary matrices (without eigenvalue -1) can be parametrised by the skew Hermitian matrices. Cayley's original presentation (1846) was in the real case, where the skew Hermitian matrices are called skew symmetric matrices, and unitary matrices are called orthogonal matrices.

Theorem 5.1 *(Density). Each tight frame $V = [v_1, \ldots, v_n]$ for $\mathbb{C}^d$ can be approximated arbitrary closely by one with vectors in $(\mathbb{Q} + i\mathbb{Q})^d$.*

Proof. Suppose, without loss of generality, that V is normalised (so that its rows are orthonormal). Extend the orthonormal rows of V to obtain a unitary matrix U.

Since the rational points on the unit circle are dense (this classical result is the special case $d = 1$ and $n = 1$, incidently), we may multiply U by a unit modulus scalar in $\mathbb{Q}+i\mathbb{Q}$ so that U does not have -1 as an eigenvalue.

Let A be the (inverse) Cayley transform of U. Since A is skew Hermitian, it can be parametrised by its $\frac{1}{2}n(n-1)$ strictly upper triangular entries, and its n purely imaginary diagonal entries. In the case of real matrices (A is skew symmetric) this reduces to $\frac{1}{2}n(n-1)$ real parameters. Taking the Cayley transform of such a parametrised matrix gives a unitary matrix with entries in the same field as the parameters. We can therefore approximate the parameters as closely as desired by elements in $\mathbb{Q} + i\mathbb{Q}$ (which is dense in $\mathbb{C}$), and the transform of the skew Hermitian matrix $\tilde{A}$ given by these approximate parameters is a unitary matrix $\tilde{U}$, which arbitrarily approximates the unitary matrix U. If the first d rows of U are a normalised tight frame V, then the first d rows $\tilde{U}$ are a normalised tight frame $\tilde{V} \in (\mathbb{Q} + i\mathbb{Q})^{d\times n}$, which arbitrarily closely approximates V. □

We now illustrate the proof of Theorem 5.1 for the tight frame of three equally spaced vectors. The 3×3 skew symmetric matrices A have three real parameters

$$A = \begin{pmatrix} 0 & a & b \\ -a & 0 & c \\ -b & -c & 0 \end{pmatrix}, \qquad a, b, c \in \mathbb{R}.$$

The Cayley transform is the symmetric matrix

$$U = \frac{I-A}{I+A} = \begin{bmatrix} \frac{1-a^2-b^2+c^2}{1+a^2+b^2+c^2} & \frac{-2(a+bc)}{1+a^2+b^2+c^2} & \frac{2(ac-b)}{1+a^2+b^2+c^2} \\ \frac{2(a-bc)}{1+a^2+b^2+c^2} & \frac{1-a^2+b^2-c^2}{1+a^2+b^2+c^2} & \frac{-2(c+ab)}{1+a^2+b^2+c^2} \\ \frac{2(ac+b)}{1+a^2+b^2+c^2} & \frac{-2(ab-c)}{1+a^2+b^2+c^2} & \frac{1+a^2-b^2-c^2}{1+a^2+b^2+c^2} \end{bmatrix}. \tag{5.12}$$

Taking any 2×3 submatrix V of the above U gives a parametrisation by $(a, b, c) \in \mathbb{R}^3$ of the normalised tight frames of three vectors for $\mathbb{R}^2$. Conversely, starting with the particular normalised tight frame V of three equally spaced vectors, we may extend it to a unitary U, as follows

$$V = \frac{\sqrt{2}}{\sqrt{3}} \begin{pmatrix} 1 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} \end{pmatrix} \quad \longrightarrow \quad U = \begin{pmatrix} \frac{\sqrt{2}}{\sqrt{3}} & -\frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{6}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \end{pmatrix}.$$

Applying the (inverse) Cayley transform to U gives the parameter values

$$a = -2 - \sqrt{3} + \sqrt{2}\sqrt{3} + \sqrt{2}, \qquad b = \sqrt{3} - \sqrt{2}, \qquad c = \sqrt{2} - 1.$$

We can approximate these to 5 decimal places by rationals

$$\tilde{a} \approx \frac{13\,165}{100\,000}, \qquad \tilde{b} \approx \frac{31\,784}{100\,000}, \qquad \tilde{c} \approx \frac{41\,421}{100\,000}.$$

The corresponding skew symmetric matrix and its Cayley transform are

$$\tilde{A} = \begin{bmatrix} 0 & \frac{2633}{20\,000} & \frac{3973}{12\,500} \\ -\frac{2633}{20\,000} & 0 & \frac{41\,421}{100\,000} \\ -\frac{3973}{12\,500} & -\frac{41\,421}{100\,000} & 0 \end{bmatrix},$$

$$\tilde{U} = \begin{pmatrix} \frac{5\,266\,079\,680}{6\,449\,619\,561} & -\frac{2\,633\,025\,064}{6\,449\,619\,561} & -\frac{2\,633\,092\,535}{6\,449\,619\,561} \\ -\frac{25\,064}{6\,449\,619\,561} & \frac{4\,560\,603\,095}{6\,449\,619\,561} & -\frac{4\,560\,536\,360}{6\,449\,619\,561} \\ \frac{3\,723\,707\,465}{6\,449\,619\,561} & \frac{3\,723\,663\,640}{6\,449\,619\,561} & \frac{3\,723\,697\,664}{6\,449\,619\,561} \end{pmatrix}.$$

Taking the first two rows of $\tilde{U}$ gives the tight frame

$$\tilde{V} = \begin{bmatrix} \frac{5\,266\,079\,680}{6\,449\,619\,561} & -\frac{2\,633\,025\,064}{6\,449\,619\,561} & -\frac{2\,633\,092\,535}{6\,449\,619\,561} \\ -\frac{25\,064}{6\,449\,619\,561} & \frac{4\,560\,603\,095}{6\,449\,619\,561} & -\frac{4\,560\,536\,360}{6\,449\,619\,561} \end{bmatrix}, \tag{5.13}$$

which approximates the three equally spaced vectors of V to 5 decimal places.

Given Theorem 5.1, a natural question is whether the tight frames with rational entries are dense in the algebraic varieties of equal norm and unit norm tight frames. The answer for real frames is no, as we now explain. Up to multiplication of the vectors by ± 1, all tight frames of three vectors for $\mathbb{R}^2$ are given by the 2×3 submatrix V of the U of (5.12) given by its first two rows. These vectors have equal norms if and only if the entries of the third row of U have equal moduli. Imposing this condition implies that these entries must be $\pm\frac{1}{\sqrt{3}}$. This in turn implies that V is given by a finite number of choices, each indexed by a single variable a, e.g.,

$$V = \begin{bmatrix} \frac{a^2-4a+2\sqrt{3}a-1}{(-3+\sqrt{3})(1+a^2)} & \frac{-2a^2+\sqrt{3}a^2+2*a+2-\sqrt{3}}{(-3+\sqrt{3})(1+a^2)} & \frac{-(2a-1+a^2)(\sqrt{3}-1)}{(-3+\sqrt{3})(1+a^2)} \\ \frac{-2a^2+\sqrt{3}a^2-2a+2-\sqrt{3}}{(-3+\sqrt{3})(1+a^2)} & \frac{a^2+4a-2\sqrt{3}a-1}{(-3+\sqrt{3})(1+a^2)} & \frac{-(a^2-2a-1)(\sqrt{3}-1)}{(-3+\sqrt{3})(1+a^2)} \end{bmatrix}.$$

For each one of these, the inner product between the vectors (scaled to unit length) is $\pm\frac{1}{2}$, and so it follows by a variation of (3.9b) that a cannot be chosen so that V has all entries rational. Thus tight frames with rational entries are not dense in the equal norm and unit norm tight frames of three vectors for $\mathbb{R}^2$. Alternatively, the above calculation shows that there is just one equal norm tight frames of three vectors for $\mathbb{R}^2$ up to projectively unitary equivalence, namely the three equally spaced vectors, which we already know do not have $\mathbb{Q}$ as a minimal field.

6. Canonical coordinates for cyclotomic fields

Let ω be the primitive n-th root of unity

$$\omega := e^{\frac{2\pi i}{n}}.$$

The *cyclotomic field* $\mathbb{Q}(\omega)$ is a $\mathbb{Q}$-vector space of dimension $d = \varphi(n)$, where φ is the *Euler Phi* function. The number of primitive n-th roots is $\varphi(n)$, but they do not form a basis for $\mathbb{Q}(\omega)$ in general, e.g., the primitive 4-th roots are $\pm i$, which are $\mathbb{Q}$-linearly dependent. For n square free the primitive n-th roots are a basis. When the primitive roots are not a basis, bases with additional properties can be constructed in a noncanonical way. Most prominently used are the *integral bases* (each element of the ring of integers has its coefficients in $\mathbb{Z}$), and *power bases* (these have the form $\{1, z, z^2, \cdots, z^{d-1}\}$).

A natural spanning sequence for $\mathbb{Q}(\omega)$ is given by the n-th roots themselves. Here we outline how $\mathbb{Q}(\omega)$ can be endowed with a unique $\mathbb{Q}$-inner product for which the n-th roots are a tight frame. The corresponding coordinates naturally inherit the geometric structure of the roots, e.g., multiplication by ω corresponds to a cyclic shift.

Given a finite spanning set $\Phi = (v_j)$ for an $\mathbb{F}$-vector space X, a vector $x \in X$ may be written as a linear combination

$$x = c_1 v_1 + \cdots + c_n v_n, \qquad c_1, \ldots, c_n \in \mathbb{F}.$$

The set of such (c_j) is an affine subspace of $\mathbb{F}^n$, which consists of a single point (the coordinates) when (v_j) is a basis, and infinitely many points otherwise. We call $a \in \mathbb{F}^n$ a *dependence of* Φ, for short $a \in \text{dep}(\Phi)$ if

$$a_1 v_1 + \cdots + a_n v_n = 0.$$

For $\mathbb{F}$ a subfield $\mathbb{C}$ which is closed under conjugation, Waldron [21] showed that there is a unique choice of (c_j) with minimal ℓ_2-norm, called the **canonical coordinates**, denoted by $c(x) = c^\Phi(x)$. We now investigate these coordinates for the spanning sequence

$$\Phi = (\omega^j)_{j\in\mathbb{Z}_n} = (1, \omega, \omega^2, \cdots, \omega^{n-1}),$$

for the $\mathbb{Q}$-vector space $\mathbb{Q}(\omega)$, which we refer to as "the canonical coordinates for $\mathbb{Q}(\omega)$".

For simplicity, we index the canonical coordinates $c_j(z)$ of $z \in \mathbb{Q}(\omega)$ by $j \in \mathbb{Z}_n$. For

$$z = a_0 + a_1\omega + \cdots + a_{n-1}\omega^{n-1}, \qquad a_0, \ldots, a_{n-1} \in \mathbb{Q},$$

we have

$$\omega z = a_0\omega + a_1\omega^2 + \cdots + a_{n-1}\omega^n, \qquad \bar{z} = a_0 + a_1\omega^{n-1} + \cdots + a_{n-1}\omega,$$

and so the canonical coordinates satisfy

$$c_j(\omega z) = c_{j+1}(z), \tag{6.14}$$

$$c_j(\bar{z}) = c_{-j}(z), \tag{6.15}$$

i.e., multiplication by ω corresponds to a *forward cyclic shift* of coordinates, and complex conjugation to the permutation $j \mapsto -j$ of the indices.

Let μ be the *Möbius Function*

$$\mu(n) := \begin{cases} 1, & n = 1; \\ (-1)^n, & n \text{ is square free}; \\ 0, & \text{otherwise} \end{cases}$$

which satisfies

$$\sum_{j\in\mathbb{Z}_n^*} \omega^j = \mu(n). \tag{6.16}$$

Here $\mathbb{Z}_n^*$ is the group of units in $\mathbb{Z}_n$ (and the primitive n-th roots of unity have the form ω^j, $j \in \mathbb{Z}_n^*$).

Theorem 6.1 *(Calculation). Suppose that $a \in \mathbb{Q}^n$ are coordinates for $z \in \mathbb{Q}(\omega)$ with respect to $\Phi = (1, \omega, \omega^2, \cdots, \omega^{n-1})$, i.e.,*

$$z = a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{n-1}\omega^{n-1},$$

then the canonical coordinates are given by

$$c(z) = c^\Phi(z) = P_\Phi a,$$

where P_Φ is the rank $d = \varphi(n)$ orthogonal projection matrix, with kernel $\operatorname{dep}(\Phi)$, *given by*

$$P_\Phi = \frac{1}{n}\sum_{j\in\mathbb{Z}_n^*} \chi_j\chi_j^*, \qquad \chi_j := (1, \omega^j, \omega^{2j}, \dots, \omega^{(n-1)j})^T, \tag{6.17}$$

which has entries

$$(P_\Phi)_{jk} = \frac{1}{n}\sum_{a\in\mathbb{Z}_n^*} \omega^{a(j-k)} = \frac{1}{n}\varphi(g)\mu\Big(\frac{n}{g}\Big), \qquad g := \gcd(j-k, n).$$

Proof. In [21], it was shown that such a P_Φ is given by

$$P_\Phi = (\Lambda V)^+\Lambda V, \qquad V : \mathbb{Q}^n \to \mathbb{Q}(\omega) : a \mapsto a_1 + a_1\omega + \cdots + a_{n-1}\omega^{n-1},$$

where $\Lambda = (\lambda_k)_{k=1}^m : \mathbb{Q}(\omega) \to \mathbb{Q}^m$ is any injective linear map, i.e., $\lambda_1, \dots, \lambda_m$ span the algebraic dual of $\mathbb{Q}(\omega)$, and A^+ is the pseudoinverse of A. Without giving an explicit basis for $\mathbb{Q}(\omega)$, it is not immediately obvious what the $\mathbb{Q}$-linear functionals on $\mathbb{Q}(\omega)$ are, and so we show that P_Φ must have the form suggested.

Since the columns of P_Φ are the canonical coordinates of $1, \omega, \dots, \omega^{n-1}$, respectively, it follows from (6.14) that P_Φ is a circulant matrix, and hence it is diagonalisable by the Fourier matrix (characters of the cyclic group of order n), i.e.,

$$P_\Phi = \frac{1}{n}\sum_{j\in\mathbb{Z}_n} \lambda_j\chi_j\chi_j^*,$$

where λ_j are the eigenvalues. Since P_Φ is a rank d orthogonal projection, exactly d of the eigenvalues are 1, with the others being 0. This motivates the formula in (6.17), indeed it gives a rank d orthogonal projection, and it only remains to show it has the same kernel as P_Φ, i.e., $\operatorname{dep}(\Phi)$. Suppose that $a \in \operatorname{dep}(\Phi)$, i.e.,

$$\chi_{-1}^* a = a_0 + a_1\omega + \cdots a_{n-1}\omega^{n-1} = 0,$$

then applying the Galois action $\omega^{-1} \mapsto \omega^j$, $j \in \mathbb{Z}_n^*$, which fixes $\mathbb{Q}$, gives

$$\chi_j^* a = a_0 + a_1\omega^{-j} + \cdots + a_{n-1}\omega^{-(n-1)} = 0,$$

and so we have

$$\ker(P_\Phi) = \operatorname{dep}(\Phi) \subset \ker\Big(\frac{1}{n}\sum_{j\in\mathbb{Z}_n^*} \chi_j\chi_j^*\Big).$$

Both of the subspaces above have dimension $n - d$, so they are equal, which establishes the formula (6.17).

Evaluating entries gives the *Ramanujan sum*

$$(P_\Phi)_{jk} = e_j^* \frac{1}{n} \sum_{a \in \mathbb{Z}_n^*} \chi_a \chi_a^* e_k = \frac{1}{n} \sum_{a \in \mathbb{Z}_n^*} \omega^{-ak} e_j^* \chi_a = \frac{1}{n} \sum_{a \in \mathbb{Z}_n^*} \omega^{a(j-k)}.$$

Using (6.16), and $\varphi(n) = \varphi(g)\varphi(\frac{n}{g})$, this can be simplified to

$$\frac{1}{n} \sum_{a \in \mathbb{Z}_n^*} \omega^{ag\frac{j-k}{g}} = \frac{1}{n} \sum_{a \in \mathbb{Z}_n^*} \omega^{ag} = \frac{1}{n}\varphi(g) \sum_{b \in \mathbb{Z}_{n/g}^*} (\omega^g)^b = \frac{1}{n}\varphi(g)\mu\left(\frac{n}{g}\right). \qquad \square$$

The argument above shows that the complementary orthogonal projection Q_Φ, onto $\operatorname{dep}(\Phi)$, is given by

$$Q_\Phi = I - P_\Phi = \frac{1}{n} \sum_{j \notin \mathbb{Z}_n^*} \chi_j \chi_j^*. \tag{6.18}$$

Example 6.1. For $n = 2^k$ the canonical decomposition of ω^j is

$$\omega^j = \frac{1}{2}\omega^j - \frac{1}{2}\omega^{j+\frac{n}{2}}.$$

More generally, for $n = p^k$, p a prime, the canonical decomposition of ω^j is

$$\omega^j = \frac{1}{p}\left\{(p-1)\omega^j - \omega^{j+\frac{n}{p}} - \omega^{j+2\frac{n}{p}} - \cdots - \omega^{j+(p-1)\frac{n}{p}}\right\}.$$

These canonical coordinates have norm

$$\|c(\omega^j)\|_2 = \frac{1}{p}\sqrt{(p-1)^2 + (p-1)} = \sqrt{1 - \frac{1}{p}} < 1.$$

Proposition 6.1. *The canonical coordinates satisfy*

$$c(\alpha x + \beta y) = \alpha c(x) + \beta c(y), \qquad \alpha, \beta \in \mathbb{Q}, \quad x, y \in \mathbb{Q}(\omega), \tag{6.19}$$

$$c(xy) = c(x) * c(y), \qquad x, y \in \mathbb{Q}(\omega), \tag{6.20}$$

where $a * b$ is the **cyclic convolution** *of a and b over $\mathbb{Z}_n$, which is given by*

$$(a * b)_k := \sum_{j=0}^{n-1} a_j b_{k-j}.$$

Proof. The first is immediate. For the second, observe that if M is a circulant matrix (such as P_Φ), then

$$M(a * b) = (Ma) * b = a * (Mb).$$

Let $a, b \in \mathbb{Q}^n$ be coordinates for x, y, then

$$xy = \Big(\sum_s a_s\omega^s\Big)\Big(\sum_r b_r\omega^r\Big) = \sum_s\sum_r a_s b_r \omega^{s+r} = \sum_k\sum_j a_j b_{k-j}\omega^k = \sum_k (a*b)_k\omega^k,$$

so that $a*b$ are coordinates for xy, and we have

$$c(xy) = P_\Phi(a*b) = (P_\Phi a)*b = c(x)*b = c(x)*c(y),$$

where for the last equality, we made the particular choice $b = c(y)$. $\square$

Example 6.2. The orthogonal projection matrices P_Φ for $n = 3, 4, 5$ are

$$\frac{1}{3}\begin{bmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{bmatrix}, \quad \frac{1}{4}\begin{bmatrix} 2 & 0 & -2 & 0 \\ 0 & 2 & 0 & -2 \\ -2 & 0 & 2 & 0 \\ 0 & -2 & 0 & 2 \end{bmatrix}, \quad \frac{1}{5}\begin{bmatrix} 4 & -1 & -1 & -1 & -1 \\ -1 & 4 & -1 & -1 & -1 \\ -1 & -1 & 4 & -1 & -1 \\ -1 & -1 & -1 & 4 & -1 \\ -1 & -1 & -1 & -1 & 4 \end{bmatrix}.$$

We can now define a $\mathbb{Q}$-inner product on $\mathbb{Q}(\omega)$ which makes the n-th roots of unity a tight frame.

Proposition 6.2 *(Normalised tight frame). The unique inner product on $\mathbb{Q}(\omega)$ for which the n-th roots Φ are a normalised tight frame is given by*

$$\langle x, y\rangle := \langle\!\langle c(x), c(y)\rangle\!\rangle, \tag{6.21}$$

i.e., the Euclidean inner product between the canonical coordinates. This satisfies

$$\langle xy, z\rangle = \langle y, \bar{x}z\rangle, \tag{6.22}$$

$$\langle z, z\rangle = \frac{\varphi(n)}{n}|z|^2. \tag{6.23}$$

In particular, multiplication by any $z \in \mathbb{Q}(\omega)$ of unit modulus is a unitary operation.

Proof. The existence of a unique inner product on $\mathbb{Q}(\omega)$ making the n-th roots into a normalised tight frame, which is given by (6.21), follows from [21, Theorem 4.9].

We now prove (6.22) and (6.23). In view of (6.15) and (6.20), the first amounts to showing

$$\langle\!\langle a*b, w\rangle\!\rangle = \langle\!\langle b, \tilde{a}*w\rangle\!\rangle, \qquad \tilde{a} = (a_{-j}),$$

where $a = c(x)$, $b = c(y)$ and $w = c(z)$. This holds for all a, b, w by direct calculation:

$$\langle\!\langle a*b, w\rangle\!\rangle = \sum_k\Big(\sum_j a_j b_{k-j}\Big)w_k = \sum_j\sum_k a_j b_{k-j} w_k,$$

$$\langle\!\langle b, \tilde{a}*w\rangle\!\rangle = \sum_k b_k\Big(\sum_j a_{-j}w_{k-j}\Big) = \sum_j\sum_k a_j b_k w_{k+j} = \sum_j\sum_k a_j b_{k-j} w_k.$$

Finally, since $|z|^2 \in \mathbb{Q}$, we have

$$\langle z, z\rangle = \langle \bar{z}z, 1\rangle = \langle |z|^2 1, 1\rangle = |z|^2\langle 1, 1\rangle.$$

In particular, all the n-roots have the same norm, and so the condition (3.7) for the normalised tight frame Φ ($A = 1$) gives

$$\dim(\mathbb{Q}(\omega)) = \varphi(n) = \sum_j \langle \omega^j, \omega^j\rangle = n\langle 1, 1\rangle.$$

Combining these gives (6.23). $\square$

Remark 6.1. In general, this inner product is different from the one induced by viewing the n-th roots of unity as vectors in $\mathbb{R}^2$ (with the Euclidean inner product), which gives a tight frame for $\mathbb{R}^2$. For example, when $d = 5$

$$\langle 1, \omega\rangle = -\frac{1}{5}, \qquad \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} \cos\frac{2\pi}{5} \\ \sin\frac{2\pi}{5} \end{pmatrix} \right\rangle = \cos\frac{2\pi}{5} \notin \mathbb{Q}.$$

Here the coordinates for 1 with the Euclidean norm (minimising $\langle c, c\rangle$ over $c \in \mathbb{R}^n$), the canonical coordinates (minimising $\langle c, c\rangle$ over $c \in \mathbb{Q}^n$), and coordinates given by $1 = 1 \cdot 1 + 0 \cdot \omega + \cdots + 0 \cdot \omega^{n-1}$ are

$$\begin{pmatrix} \frac{2}{5} \\ \frac{2}{5}\cos\frac{2\pi}{5} \\ \frac{2}{5}\cos\frac{4\pi}{5} \\ \frac{2}{5}\cos\frac{6\pi}{5} \\ \frac{2}{5}\cos\frac{8\pi}{5} \end{pmatrix}, \qquad c(1) = \begin{pmatrix} \frac{4}{5} \\ -\frac{1}{5} \\ -\frac{1}{5} \\ -\frac{1}{5} \\ -\frac{1}{5} \end{pmatrix}, \qquad \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

which have norms

$$\frac{2}{5}\sqrt{1 + 2\cos^2\frac{2\pi}{5} + 2\cos^2\frac{4\pi}{5}} \approx 0.63246, \qquad \frac{2}{\sqrt{5}} \approx 0.89442, \qquad 1.$$

Example 6.3. We observe that

$$\omega^j \text{ is orthogonal to } \omega^k \quad\iff\quad \mu\Big(\frac{n}{g}\Big) = 0, \quad g = \gcd(j-k, n),$$

and so two n-th roots cannot be orthogonal if n is square free.

Canonical bases for $\mathbb{Q}(\omega)$ for efficient computation were considered in [2]. In particular, from these representations it is immediately apparent what is the small cyclotomic field an element lies in. The following example indicates how similar conclusions can be drawn from our canonical coordinates.

Example 6.4. Let $n = 8$, $\omega = \sqrt{i} = e^{\frac{2\pi i}{8}}$. Then $\mathbb{Q}(\omega)$ is 4-dimensional, with cyclotomic subspaces

$$\mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{Q}(\sqrt{i}).$$

We have the canonical coordinates

$$c(1) = \begin{pmatrix} \frac{1}{2} \\ 0 \\ 0 \\ 0 \\ \frac{1}{2} \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad c(i) = c(\omega^2) = \begin{pmatrix} 0 \\ 0 \\ \frac{1}{2} \\ 0 \\ 0 \\ 0 \\ \frac{1}{2} \\ 0 \end{pmatrix},$$

$$c(\sqrt{i}) = c(\omega) = \begin{pmatrix} 0 \\ \frac{1}{2} \\ 0 \\ 0 \\ 0 \\ \frac{1}{2} \\ 0 \\ 0 \end{pmatrix}, \quad c(i\sqrt{i}) = c(\omega^3) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \frac{1}{2} \\ 0 \\ 0 \\ 0 \\ \frac{1}{2} \end{pmatrix}.$$

Therefore one can determine what is the smallest cyclotomic subfield of $\mathbb{Q}(\sqrt{i})$ a given element lies in by considering which of its canonical coordinates are zero.

Theorem 6.2 *(Irreducibility). For any nonzero $z \in \mathbb{Q}(\omega)$, the vectors $(z, \omega z, \ldots, \omega^{n-1} z)$ are a tight frame for $\mathbb{Q}(\omega)$, i.e.,*

$$x = \frac{1}{|z|^2} \sum_{j \in \mathbb{Z}_n} \langle x, \omega^j z \rangle \omega^j z, \qquad \forall x \in \mathbb{Q}(\omega). \tag{6.24}$$

In particular, the natural action of the cyclic group $C_n = \langle a \rangle$ on $\mathbb{Q}(\omega)$ on the $\mathbb{Q}$-vector space $\mathbb{Q}(\omega)$ given by $a \cdot \omega^j = \omega^{j+1}$ is irreducible.

Proof. Using (6.22) and the fact $(1, \omega, \ldots, \omega^{n-1})$ is a normalised tight frame, we calculate

$$\sum_j \langle x, \omega^j z \rangle \omega^j z = \Big(\sum_j \langle \bar{z} x, \omega^j \rangle \omega^j \Big) z = (\bar{z} x) z = |z|^2 x.$$

Thus every C_n-orbit of $z \neq 0$ spans $\mathbb{Q}(\omega)$, i.e., the action is irreducible. □

Let S be the (*forward*) *cyclic shift* operator on $\mathbb{Q}^n$, which is given by

$$Se_j := e_{j+1}, \qquad j \in \mathbb{Z}_n,$$

and defines a natural action of $C_n = \langle a \rangle$ on $\mathbb{Q}^n$ via

$$a \cdot v = Sv.$$

The condition (6.14) for canonical coordinates can be written

$$c(\omega z) = Sc(z).$$

We denote by $\operatorname{can}(\Phi)$ the subspace $\mathbb{Q}^n$ given by the canonical coordinates

$$\operatorname{can}(\Phi) := \operatorname{ran}(P_\Phi) = \{c^\Phi(x) : x \in \mathbb{Q}(\omega)\}.$$

The canonical coordinates $\operatorname{can}(\Phi)$ and the dependencies $\operatorname{dep}(\Phi)$ are orthogonal shift invariant subspaces of $\mathbb{Q}^n$. It follows from (6.24), that the action of S on $\operatorname{can}(\Phi)$ is irreducible.

Corollary 6.1. *The shifts of any nonzero $b \in \operatorname{can}(\Phi)$ are a tight frame for $\operatorname{can}(\Phi)$, i.e.,*

$$a = \frac{\varphi(n)}{n} \frac{1}{\langle b, b \rangle} \sum_{j \in \mathbb{Z}_n} \langle a, S^j b \rangle S^j b, \qquad \forall a \in \operatorname{can}(\Phi).$$

The structure of the space $\operatorname{dep}(\Phi)$ of linear dependencies between the n-roots is more complicated than that of $\operatorname{can}(\Phi)$. For n not a prime, the there is a proper 1-dimensional shift invariant subspace spanned by $(1, 1, \dots, 1)$. Nevertheless, we are able to give a single linear dependence a_Φ whose shifts give a tight frame for $\operatorname{dep}(\Phi)$.

Theorem 6.3. *Let $a_\Phi \in \mathbb{Z}^n$ be n times the first column of Q_Φ, the orthogonal projection matrix onto $\operatorname{dep}(\Phi)$, i.e.,*

$$a_\Phi = \sum_{j \notin \mathbb{Z}_n^*} \chi_j \chi_j^*.$$

Then the shifts of a_Φ are a tight frame for $\operatorname{dep}(\Phi)$, i.e.,

$$x = \frac{n - \varphi(n)}{n} \frac{1}{\langle a_\Phi, a_\Phi \rangle} \sum_{j \in \mathbb{Z}_n} \langle x, S^j a_\Phi \rangle S^j a_\Phi, \qquad \forall x \in \operatorname{dep}(\Phi). \tag{6.25}$$

Proof. By (6.18), Q_Φ is the circulant matrix given by

$$\frac{1}{n} \sum_{j \notin \mathbb{Z}_n^*} \chi_j \chi_j^* = \frac{1}{n} [a_\Phi, Sa_\Phi, S^2 a_\Phi, \dots, S^{n-1} a_\Phi].$$

By Theorem 3.1, its columns are a normalised tight frame for its range dep(Φ), i.e.,

$$x = \frac{1}{n^2} \sum_{j \in \mathbb{Z}_n} \langle x, S^j a_\Phi \rangle S^j a_\Phi, \qquad \forall x \in \operatorname{dep}(\Phi).$$

The condition (3.7) for normalised tight frames gives

$$\dim(\operatorname{dep}(\Phi)) = n - \varphi(n) = \sum_{j \in \mathbb{Z}_n} \left\langle \frac{1}{n} S^j a_\Phi, \frac{1}{n} S^j a_\Phi \right\rangle = \frac{1}{n} \langle a_\Phi, a_\Phi \rangle.$$

Combining these gives (6.25). □

Calculations suggest that the first $n - \phi(n)$ columns of Q_Φ are a basis for dep(Φ).

There is a large body of research on the dependencies (over $\mathbb{Z}$) of the n-th roots of unity, largely concerned with finding *vanishing sums* with minimal numbers of terms (cf. [14,18]). To the best of our knowledge the spanning sequence $\{S^j a_\Phi\}_{j \in \mathbb{Z}_n}$ is new.

Example 6.5. For $n = 6$, $\mathbb{Z}_6^* = \{1, 5\}$, and so $P_\Phi = \frac{1}{6}(\chi_1 \chi_1^* + \chi_5 \chi_5^*)$ and $Q_\Phi = I - P_\Phi$ are given by

$$P_\Phi = \frac{1}{6} \begin{pmatrix} 2 & 1 & -1 & -2 & -1 & 1 \\ 1 & 2 & 1 & -1 & -2 & -1 \\ -1 & 1 & 2 & 1 & -1 & -2 \\ -2 & -1 & 1 & 2 & 1 & -1 \\ -1 & -2 & -1 & 1 & 2 & 1 \\ 1 & -1 & -2 & -1 & 1 & 2 \end{pmatrix}, \quad Q_\Phi = \frac{1}{6} \begin{pmatrix} 4 & -1 & 1 & 2 & 1 & -1 \\ -1 & 4 & -1 & 1 & 2 & 1 \\ 1 & -1 & 4 & -1 & 1 & 2 \\ 2 & 1 & -1 & 4 & -1 & 1 \\ 1 & 2 & 1 & -1 & 4 & -1 \\ -1 & 1 & 2 & 1 & -1 & 4 \end{pmatrix}.$$

Thus $a_\Phi = (4, -1, 1, 2, 1, -1)^T$, and the dependencies between the roots can be expressed as

$$4\omega^j - \omega^{j+1} + \omega^{j+2} + 2\omega^{j+3} + \omega^{j+4} - \omega^{j+5} = 0, \qquad 0 \le j < 6.$$

The shift invariant subspace dep(Φ) can be decomposed if n is not prime, e.g., for $n = 6$, this 4-dimensional subspace of $\mathbb{Q}^6$ decomposes into two 1-dimensional and one 2-dimensional orthogonal shift invariant subspaces generated by

$$(1, 1, 1, 1, 1, 1)^T, \quad (1, -1, 1, -1, 1, -1)^T, \quad (0, 1, -1, 0, 1, -1)^T,$$

respectively. The $a = a_\Phi$ of Example 6.5 can be decomposed as follows

$$a = \begin{pmatrix} 4 \\ -1 \\ 1 \\ 2 \\ 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} + \begin{pmatrix} 2 \\ -1 \\ -1 \\ 2 \\ -1 \\ -1 \end{pmatrix}.$$

Theorem 6.18 of [19] shows that, up to a scalar multiple, all the vectors $v \in \operatorname{dep}(\Phi)$ for which $(S^j v)_{j\in\mathbb{Z}_n}$ is a tight frame for $\operatorname{dep}(\Phi)$ are given by

$$v = \begin{pmatrix}1\\1\\1\\1\\1\\1\end{pmatrix} \pm \begin{pmatrix}1\\-1\\1\\-1\\1\\-1\end{pmatrix} + \alpha \begin{pmatrix}2\\-1\\-1\\2\\-1\\-1\end{pmatrix} + \beta \begin{pmatrix}0\\1\\-1\\0\\1\\-11\end{pmatrix}, \qquad \begin{array}{c}\alpha,\beta\in\mathbb{Q},\\ 3\alpha^2+\beta^2=3.\end{array} \tag{6.26}$$

As an example, taking $+$, $\alpha = \frac{1}{7}$, $\beta = \frac{12}{7}$ gives $v = \frac{1}{7}(16, 11, 1, 2, 25, -13)^T$.

The usual way to study $\operatorname{dep}(\Phi)$ is to observe that each $a \in \operatorname{dep}(\Phi)$ corresponds to a polynomial p given by

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1},$$

where $p(\omega) = 0$. All such p have the form

$$p = Q_n r,$$

where Q_n is the n-**cyclotomic polynomial** (which has integer coefficients)

$$Q_n(x) = \prod_{j\in\mathbb{Z}_n^*} (x - \omega^j),$$

r has degree $n - \varphi(n) - 1$. By taking r from some basis for the polynomials of degree $n - \varphi(n) - 1$, one obtains a basis for $\operatorname{dep}(\Phi)$. For $n = 6$,

$$Q_6(x) = x^2 - x + 1,$$

and taking r to be the monomials $1, x, x^2, x^3$ gives the basis

$$(1,-1,1,0,0,0)^T, \quad (0,1,-1,1,0,0)^T, \quad (0,0,1,-1,1,0)^T, \quad (0,0,0,1,-1,1)^T$$

for $\operatorname{dep}(\Phi)$. This consists of some of the shifts of a single dependence. In view of (6.26), the set of all shifts is not a tight frame for $\operatorname{dep}(\Phi)$.

References

[1] D.M. Appleby, Hulya Yadsan-Appleby, Gerhard Zauner, Galois automorphisms of a symmetric measurement, Quantum Inf. Comput. 13 (7–8) (2013) 672–720.
[2] Wieb Bosma, Canonical bases for cyclotomic fields, Appl. Algebra Engrg. Comm. Comput. 1 (2) (1990) 125–134.
[3] Ole Christensen, An Introduction to Frames and Riesz Bases, Appl. Numer. Harmon. Anal., Birkhäuser Boston, Inc., Boston, MA, 2003.

[4] Peter G. Casazza, Gitta Kutyniok (Eds.), Finite Frames: Theory and Applications, Appl. Numer. Harmon. Anal., Birkhäuser/Springer, New York, 2013.
[5] Peter G. Casazza, Gitta Kutyniok, Shidong Li, Fusion frames and distributed processing, Appl. Comput. Harmon. Anal. 25 (1) (2008) 114–132.
[6] J. Cahill, D.G. Mixon, N. Strawn, Connectivity and irreducibility of algebraic varieties of finite unit norm tight frames, arXiv e-prints, November 2013.
[7] Jameson Cahill, Nate Strawn, Algebraic geometry and finite frames, in: Finite Frames, in: Appl. Numer. Harmon. Anal., Birkhäuser/Springer, New York, 2013, pp. 141–170.
[8] Tuan-Yow Chien, Shayne Waldron, A classification of the harmonic frames up to unitary equivalence, Appl. Comput. Harmon. Anal. 30 (3) (2011) 307–318.
[9] C.J. Everett, H.J. Ryser, Rational vector spaces. I, Duke Math. J. 16 (1949) 553–570.
[10] C.J. Everett, H.J. Ryser, Rational vector spaces. II, Duke Math. J. 17 (1950) 135–145.
[11] G. David Forney Jr., Minimal bases of rational vector spaces, with applications to multivariable linear systems, SIAM J. Control 13 (1975) 493–520.
[12] Vivek K. Goyal, Jelena Kovačević, Jonathan A. Kelner, Quantized frame expansions with erasures, Appl. Comput. Harmon. Anal. 10 (3) (2001) 203–233.
[13] Karlheinz Gröchenig, Foundations of Time–Frequency Analysis, Appl. Numer. Harmon. Anal., Birkhäuser Boston, Inc., Boston, MA, 2001.
[14] T.Y. Lam, K.H. Leung, On vanishing sums of roots of unity, J. Algebra 224 (1) (2000) 91–109.
[15] Hans Liebeck, Anthony Osborne, The generation of all rational orthogonal matrices, Amer. Math. Monthly 98 (2) (1991) 131–133.
[16] Joseph M. Renes, Robin Blume-Kohout, A.J. Scott, Carlton M. Caves, Symmetric informationally complete quantum measurements, J. Math. Phys. 45 (6) (2004) 2171–2180.
[17] A.J. Scott, M. Grassl, Symmetric informationally complete positive-operator-valued measures: a new computer study, J. Math. Phys. 51 (4) (2010), 042203, 16.
[18] John P. Steinberger, Minimal vanishing sums of roots of unity with large coefficients, Proc. Lond. Math. Soc. (3) 97 (3) (2008) 689–717.
[19] Richard Vale, Shayne Waldron, Tight frames and their symmetries, Constr. Approx. 21 (1) (2005) 83–112.
[20] Shayne Waldron, Generalized Welch bound equality sequences are tight frames, IEEE Trans. Inform. Theory 49 (9) (2003) 2307–2309.
[21] Shayne Waldron, Frames for vector spaces and affine spaces, Linear Algebra Appl. 435 (1) (2011) 77–94.