Appl. Comput. Harmon. Anal. 48 (2020) 46–63

Contents lists available at ScienceDirect

Applied and Computational Harmonic Analysis

www.elsevier.com/locate/acha

On the number of harmonic frames

Simon Marshall [a], Shayne Waldron [b,*]

[a] Department of Mathematics, University of Wisconsin–Madison, 480 Lincoln Drive, Madison, WI 53706, USA
[b] Department of Mathematics, University of Auckland, Private Bag 92019, Auckland, New Zealand

ARTICLE INFO

Article history:
Received 21 November 2016
Received in revised form 17 October 2017
Accepted 6 February 2018
Available online 8 February 2018
Communicated by Zuowei Shen

MSC:
primary 42C15, 94A12
secondary 11Z05, 20C15, 94A15, 20F28

Keywords:
Finite tight frames
Harmonic frames
Finite abelian groups
Character theory
Pontryagin duality
Mordell–Lang conjecture
Projective unitary equivalence

ABSTRACT

There is a finite number $h_{n,d}$ of tight frames of n distinct vectors for $\mathbb{C}^d$ which are the orbit of a vector under a unitary action of the cyclic group $\mathbb{Z}_n$. These *cyclic harmonic frames* (or *geometrically uniform tight frames*) are used in signal analysis and quantum information theory, and provide many tight frames of particular interest. Here we investigate the conjecture that $h_{n,d}$ grows like n^{d-1}. By using a result of Laurent which describes the set of solutions of algebraic equations in roots of unity, we prove the asymptotic estimate

$$h_{n,d} \approx \frac{n^d}{\varphi(n)} \geq n^{d-1}, \qquad n \to \infty.$$

By using a group theoretic approach, we also give some exact formulas for $h_{n,d}$, and estimate the number of cyclic harmonic frames up to projective unitary equivalence.

1. Introduction

Tight frames of n vectors for $\mathbb{C}^d$ have numerous applications (see the surveys [4], [5]). These include signal transmission with erasures [10], [14], [2] and quantum information theory [16], [20].

Many tight frames of practical and theoretical interest are G-frames (the orbit of a unitary action of a group G) [22]. Most notable are the *harmonic frames* (G is abelian) and *SICs*, i.e., d^2 equiangular lines in $\mathbb{C}^d$ (for a projective action of the abelian group $\mathbb{Z}_d^2$). The main result of this paper is a precise statement about how numerous the harmonic frames of n vectors for $\mathbb{C}^d$ are (Theorem 3.1). By way of comparison, SICs are known to exist only for certain values of d, and there is strong evidence for *Zauner's conjecture* that they exist for all values of d (see [20], [25]).

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

https://doi.org/10.1016/j.acha.2018.02.004

We now provide some background on harmonic frames, and then detail our approach (precise definitions are given in §2). What we will call a *cyclic harmonic frame* for $\mathbb{C}^d$ was first introduced as a $d \times n$ submatrix $[v_1, \ldots, v_n]$ of the Fourier matrix (character table for $\mathbb{Z}_n$)

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \cdots & \omega^{(n-1)(n-1)} \end{bmatrix}, \qquad \omega := e^{\frac{2\pi i}{n}}, \tag{1.1}$$

obtained by selecting d of the rows (characters of $\mathbb{Z}_n$). See [11], [13], [3] (who use the term *harmonic frame* for when the first d rows are taken), [6] (who use the term a *Fourier ensemble*), and [19] (who show a matrix with its columns given by a random cyclic harmonic frame is a RIP (restricted isometry property) matrix with high probability). These tight frames can be viewed as $\mathbb{Z}_n$-frames (called *geometrically uniform frames* in [9]). This construction generalises, with $\mathbb{Z}_n$ replaced by an abelian group G of order n [21], to give what we call a *harmonic frame* (it is *cyclic* if G can be taken to be $\mathbb{Z}_n$). It follows from the character table construction (and the fact there are a finite number of abelian groups of order n) that there is a finite number of harmonic frames of n vectors for $\mathbb{C}^d$.

A computer study [24] of the harmonic frames of n vectors for $\mathbb{C}^d$ suggested the following behaviour:

- The number of harmonic frames (up to unitary equivalence) grows like n^{d-1}, and it is influenced by the prime factors of n.
- The majority of harmonic frames are cyclic.

In this paper, we show that for fixed d the number $h_{n,d}$ of cyclic harmonic frames grows like

$$h_{n,d} \approx \frac{n^d}{\varphi(n)} \geq n^{d-1}, \qquad n \to \infty.$$

The key points of our argument are

- Cyclic harmonic frames correspond to d-element subsets $J \subset \mathbb{Z}_n$.
- When cyclic harmonic frames given by $J, K \subset \mathbb{Z}_n$ are unitarily equivalent, usually $K = \sigma J$ for some automorphism. When this is not the case, we say they are *exceptional*.
- The automorphisms of $\mathbb{Z}_n$ are easy to describe (as the units $\mathbb{Z}_n^*$).
- A pair of unitarily equivalent cyclic harmonic frames determines a torsion point on the $(2d)$-torus $\mathbb{T}^{2d}$.
- By using results about the torsion point solutions of algebraic equations, we show that the number of exceptional harmonic frames grows slower than the number which aren't.
- The nonexceptional cyclic harmonic frames are counted by Burnside enumeration.

We carry out this argument in §4–§5. We give examples and some numerical data in §6. In §7 we show that there are no exceptional equivalences when n is prime, and together with Burnside enumeration this allows us to give an exact formula for $h_{n,d}$ in this case, which we break down into lifted and unlifted, and into real and complex harmonic frames.

In the final section, we use our techniques to investigate the number $p_{n,d}$ of harmonic frames of n vectors for $\mathbb{C}^d$ up to *projective unitary equivalence*. For $d \geq 4$, this gives the lower estimate

$$p_{n,d} \approx \frac{n^{d-1}}{\varphi(n)} \geq n^{d-2}, \qquad n \to \infty.$$

2. Harmonic frames

A sequence of n vectors (v_j) in $\mathbb{C}^d$ is a **tight frame** for $\mathbb{C}^d$ if for some $A > 0$

$$A\|f\|^2 = \sum_{j=1}^{n} |\langle f, v_j\rangle|^2, \qquad \forall f \in \mathbb{C}^d.$$

By the polarisation identity, this is equivalent to the redundant "orthogonal expansion"

$$f = \frac{1}{A}\sum_{j=1}^{n} \langle f, v_j\rangle v_j, \qquad \forall f \in \mathbb{C}^d. \tag{2.2}$$

We say that tight frames (v_j) and (w_k) are **unitarily equivalent** (up to a reindexing) if there is a unitary map U and a bijection $\sigma : j \to k$ (a reindexing) between their index sets for which

$$v_j = U w_{\sigma j}, \qquad \forall j. \tag{2.3}$$

If (v_j) is unitarily equivalent to a frame $(w_j) \subset \mathbb{R}^d$, then we say it is a **real frame**.

A tight frame $(gv)_{g\in G}$ which is the orbit of a vector v under the unitary action of a finite group G is called a **G-frame** (or **group frame**) [22]. For G abelian, there are finitely many G-frames for $\mathbb{C}^d$ up to unitary equivalence, which we call the **harmonic frames**. For G nonabelian, there are uncountably many G-frames for $\mathbb{C}^d$, $d \geq 2$. We now give the basic theory of harmonic frames required (see [7], [22], [8], [23] for details).

Let G be a finite abelian group (written additively). The (**irreducible**) **characters** of G are the group homomorphisms $\xi : G \to \mathbb{C}\setminus\{0\}$, where $\mathbb{C}\setminus\{0\}$ is a group under multiplication. Here we think of characters as vectors $\xi \in \mathbb{C}^G$ (with the Euclidean inner product), which satisfy

$$\xi(g+h) = \xi(g)\xi(h), \qquad \forall g, h \in G. \tag{2.4}$$

The set of irreducible characters of the abelian group G is denoted by $\hat{G}$.

The characters $\hat{G}$ form a group under the multiplication $(\xi\eta)(g) := \xi(g)\eta(g)$, which is called the **character group**. The character group $\hat{G}$ is isomorphic to G. For $\chi \in \hat{G}$, (2.4) implies that $\chi(g)$ is a $|G|$-th root of unity, and so the inverse of χ satisfies

$$\chi^{-1}(g) = \frac{1}{\chi(g)} = \overline{\chi(g)}. \tag{2.5}$$

The square matrix with the irreducible characters of G as rows is referred to as the **character table** of G. For example, if $G = \langle a\rangle$ is the cyclic group of order n, with its elements ordered $1, a, \ldots, a^{n-1}$, then its character table is given by (1.1).

The harmonic frames for $\mathbb{C}^d$ given by G can all be described (up to unitary equivalence) in two equivalent ways:

1. By a choice of d characters $\{\xi_1, \ldots, \xi_d\} \subset \hat{G}$ (d rows of the character table), i.e.,

$$\Psi_{\{\xi_1,\ldots,\xi_d\}} = (v_g)_{g\in G}, \qquad v_g := (\xi_j(g))_{j=1}^d \in \mathbb{C}^d. \tag{2.6}$$

2. By a choice of d group elements $J \subset G$ (d columns of the character table), i.e.,

$$\Phi_J = (\xi|_J)_{\xi\in\hat{G}}, \qquad \xi|_J \in \mathbb{C}^J \cong \mathbb{C}^d. \tag{2.7}$$

Many properties of harmonic frames are easy to describe in the second presentation. In particular:

- Φ_J has distinct vectors if and only if J generates G.
- Φ_J is a real frame if and only if J is closed under taking inverses.
- Φ_J is an ETF (equiangular tight frame) if and only if J is a difference set.
- If σ is an automorphism of G and $K = \sigma J$, then Φ_J and Φ_K are unitarily equivalent. In this case we say that Φ_J and Φ_K are **unitarily equivalent via an automorphism**.

Note that if J does not generate G, then Φ_J has $|\langle J\rangle|$ distinct vectors (where $\langle J\rangle$ is the group generated by J), each occurring $|G : \langle J\rangle|$ times. Moreover, the frame obtained by taking one of each of the distinct vectors is a harmonic frame associated to $\langle J\rangle$.

We now focus on the harmonic frames for $G = \mathbb{Z}_n$, which are said to be **cyclic** (harmonic) frames. In this case, the automorphism group of G (and hence $\hat{G}$) has a particularly simple form: each automorphism corresponds to a unit $a \in \mathbb{Z}_n^*$ via

$$\sigma g = ag, \quad \forall g \in G, \qquad \sigma \in \mathrm{Aut}(G),$$
$$\tau\chi = \chi^a, \quad \forall \chi \in \hat{G}, \qquad \tau \in \mathrm{Aut}(\hat{G}).$$

We say that d-element subsets $\{\xi_1, \ldots, \xi_d\}$ and $\{\eta_1, \ldots, \eta_d\}$ of $\hat{\mathbb{Z}}_n$, or d-elements subsets K and J of $\mathbb{Z}_n$, are **multiplicatively equivalent** if there is an automorphism mapping one to the other, i.e.,

$$\{\xi_1, \ldots, \xi_d\} = \{\eta_1, \ldots, \eta_d\}^a = \{\eta_1^a, \ldots, \eta_d^a\}, \qquad K = aJ.$$

This holds if and only if the cyclic harmonic frames they determine are unitarily equivalent via an automorphism. Because of this, we shall sometimes apply the term ‘multiplicatively equivalent’ to a pair of frames to mean they are unitarily equivalent via an automorphism. An **exceptional equivalence** is a unitary equivalence between cyclic harmonic frames given by sets of characters (or group elements) which are not multiplicatively equivalent. An **exceptional frame** is one having an exceptional equivalence with another frame.

3. The number of cyclic harmonic frames

Calculations of [7] indicate that *most cyclic harmonic frames are not exceptional*, i.e., unitarily equivalent cyclic harmonic frames usually come from multiplicatively equivalent subsets (this is proved in Proposition 4.6). This is the basic principle underlying our results.

Let $h_{n,d}$ be the number of unitarily inequivalent cyclic harmonic frames of n distinct vectors for $\mathbb{C}^d$. We recall that Euler’s totient function is given by

$$\varphi(n) = |\mathbb{Z}_n^*| = n \prod_{p|n} \big(1 - \frac{1}{p}\big).$$

The main result is the following, which gives the growth of $h_{n,d}$ (for d fixed).

Theorem 3.1. *If $d = 1$, then $h_{n,d} = 1$ for all n. If $d \geq 2$, then for all $\epsilon > 0$, we have*

$$h_{n,d} = \frac{n^d}{d!\varphi(n)} \prod_{p|n} (1 - p^{-d})\big(1 + O_\epsilon(n^{-1+\epsilon})\big), \qquad n \to \infty, \tag{3.8}$$

where φ is Euler’s totient function, and the product is over the prime factors p of n.

Throughout, we use asymptotic notation, e.g., $a_n = O_\epsilon(b_n)$ means $|a_n| \le Cb_n$ as $n \to \infty$, where $b_n \ge 0$ and C is a constant depending only on ϵ. For $a_n \ge 0$, $b_n \ge 0$, we write

$$\begin{aligned} a_n \ll b_n \quad &\iff \quad a_n = O(b_n), \\ a_n \approx b_n \quad &\iff \quad a_n = O(b_n),\ b_n = O(a_n). \end{aligned}$$

The *Euler product formula* for the Riemann zeta function gives

$$0 < \frac{1}{\zeta(d)} = \prod_{p \text{ prime}} (1 - p^{-d}) < \prod_{p|n} (1 - p^{-d}) \le 1, \qquad d = 2, 3, \ldots. \tag{3.9}$$

Thus (3.8) gives the asymptotic estimate

$$h_{n,d} \approx \frac{n^d}{\varphi(n)} \ge n^{d-1}, \qquad n \to \infty.$$

There are various upper bounds for the factor $n/\varphi(n)$ above, e.g., [18] (Theorem 15) gives

$$\frac{n}{\varphi(n)} < e^C \log\log n + \frac{2.51}{\log\log n}, \qquad n \ge 3,$$

where C is Euler's constant.

The proof of Theorem 3.1 (see the comments after Proposition 5.4) consists of two parts:

1. We think of cyclic harmonic frames as being given by subsets (or sequences) of d characters of $\mathbb{Z}_n$, and hence by n-th roots of unity. This allows us to show that a pair of unitarily equivalent frames gives a torsion point on the torus $\mathbb{T}^{2d}$ that satisfies certain algebraic equations. By using results about the solutions of algebraic equation in roots of unity, we show that the number exceptional cyclic harmonic frames grows slower than those which aren't (Proposition 4.6).
2. In view of Proposition 4.6, it suffices to count the cyclic harmonic frames up to unitary equivalence via an automorphism. This we do by (Burnside) counting the d-element subsets of $\mathbb{Z}_n$ up to multiplicative equivalence (Proposition 5.4).

We now give the arguments for each part (§4 and §5).

4. Torsion points and exceptional cyclic frames

Since any character ξ of $\mathbb{Z}_n$ satisfies

$$\xi(k) = \xi(1)^k, \qquad \forall k,$$

choosing ξ is equivalent to choosing the n-th root of unity $\xi(1)$. Thus a choice of characters (giving a cyclic frame) corresponds to a choice of n-th roots via

$$\{\xi_1, \ldots, \xi_d\} \quad \iff \quad \{\xi_1(1), \ldots, \xi_d(1)\}.$$

In this section, we shall often think of a choice of d characters (or n-th roots) as being an *ordered subset* $(\xi_1, \ldots, \xi_d)$. There are $d!$ such orderings of a given subset $\{\xi_1, \ldots, \xi_d\}$.

Two sets of n-th roots determining unitarily equivalent harmonic frames satisfy the following.

Lemma 4.1. *Let G be a finite abelian group. If $(v_g)_{g\in G}$ is a harmonic frame, then*

$$\langle v_{a+c}, v_{b+c}\rangle = \langle v_a, v_b\rangle, \qquad \forall a,b,c \in G.$$

In particular, if $\{\xi_1,\ldots,\xi_d\},\{\eta_1,\ldots,\eta_d\}\subset\hat{\mathbb{Z}}_n$ give unitarily equivalent cyclic harmonic frames, then for some $a\in\mathbb{Z}_n$, we have

$$\sum_{j=1}^{d}\xi_j(1)=\sum_{j=1}^{d}\eta_j(a). \tag{4.10}$$

Proof. Let $(v_g)_{g\in G}$ and $(w_g)_{g\in G}$ be the harmonic frames given by $\{\xi_j\}$ and $\{\eta_j\}$ via (2.6). Then we calculate

$$\langle v_{a+c}, v_{b+c}\rangle = \sum_j \xi_j(a+c)\overline{\xi_j(b+c)} = \sum_j \xi_j(a)\xi_j(c)\overline{\xi_j(b)\xi_j(c)} = \sum_j \xi_j(a)\overline{\xi_j(b)} = \langle v_a, v_b\rangle.$$

If $(v_g)_{g\in G}$ and $(w_g)_{g\in G}$ are unitarily equivalent via (2.3), then

$$\langle v_k, v_\ell\rangle = \langle Uw_{\sigma k}, Uw_{\sigma\ell}\rangle = \langle w_{\sigma k}, w_{\sigma\ell}\rangle = \langle w_{\sigma k-\sigma\ell}, w_0\rangle.$$

For $G=\mathbb{Z}_n$, taking $k=1$, $\ell=0$ above, gives $\langle v_1,v_0\rangle=\langle w_a,w_0\rangle$, $a:=\sigma1-\sigma0$, which is (4.10). $\square$

Let $V\subset\mathbb{C}^{2d}$ be the set of solutions to

$$\sum_{j=1}^{d} z_j - \sum_{j=1+d}^{2d} z_j = 0. \tag{4.11}$$

By Lemma 4.1, every unitary equivalence between cyclic harmonic frames of n vectors for $\mathbb{C}^d$ gives a solution

$$z=(\xi_1(1),\ldots,\xi_d(1),\eta_1(a),\ldots,\eta_d(a))\in V \tag{4.12}$$

in n-th roots of unity. Moreover, one may easily produce such solutions by letting $z_{d+1},\ldots,z_{2d}$ be a permutation of $z_1,\ldots,z_d$. We call a solution to (4.11) in roots of unity **exceptional** if $z_{d+1},\ldots,z_{2d}$ is not a permutation of $z_1,\ldots,z_d$.

We shall prove (Lemma 4.2) that any exceptional equivalence between cyclic harmonic frames gives rise to an exceptional solution to (4.11). This allows us to prove that the number of exceptional cyclic harmonic frames is small (Proposition 4.6), i.e.,

Of the $\approx n^d$ choices of d characters of $\mathbb{Z}_n$, $\ll n^{d-1}$ give exceptional cyclic harmonic frames.

This reduces the proof of Theorem 3.1 to that of counting the number of nonexceptional cyclic harmonic frames, which is done by counting $\mathbb{Z}_n^*$-orbits (see §5).

We will prove Proposition 4.6 by reducing it to a count of solutions to a linear equation in roots of unity. This is a well studied problem in the theory of Diophantine equations, and the set of solutions has a simple structure described by a theorem of Laurent [15], which is a special case of the Mordell–Lang conjecture. We now give the details.

Let $\mathbb{T}^k$ be the k**-torus**

$$\mathbb{T}^k := \{z\in\mathbb{C}^k : |z_1|=\cdots=|z_k|=1\},$$

which is a *compact abelian Lie group* under the group operation

$$z \cdot w := (z_1 w_1, \dots, z_k w_k).$$

If $z \in \mathbb{T}_k$ and $T \subset \mathbb{T}_k$ is a subgroup, we use $z \cdot T$ to denote the translate of T by z. A point on the torus of finite order is called a **torsion point**. We denote the set of torsion points by $\mathbb{T}^k_{\text{tors}}$. We let $\mathbb{T}^k[n]$ denote the set of n-torsion points (torsion points of order n), which is the same as k-tuples of n-th roots of unity. There is a bijection between d-tuples of characters of $\mathbb{Z}_n$ and $\mathbb{T}^d[n]$ sending $(\xi_1, \dots, \xi_d)$ to $(\xi_1(1), \dots, \xi_d(1))$.

If the ordered subsets $(\xi_1, \dots, \xi_d)$ and $(\eta_1, \dots, \eta_d)$ give equivalent harmonic frames, then (4.12) gives a point $z \in V \cap \mathbb{T}^{2d}[n]$. Note that z depends on the choice of unitary equivalence between the two frames made in the proof of Lemma 4.1.

The basic result that allows us to reduce from counting frames to counting solutions to equations in roots of unity is the following.

Lemma 4.2. *If the cyclic harmonic frame given by $(\xi_1(1), \dots \xi_d(1)) \in \mathbb{T}^d[n]$ has distinct vectors and is exceptional, then there is an exceptional point*

$$z = (\xi_1(1), \dots, \xi_d(1), z_{d+1}, \dots, z_{2d}) \in V \cap \mathbb{T}^{2d}[n].$$

Proof. By hypothesis, there is an ordered set $(\eta_1, \dots, \eta_d)$ of characters of $\mathbb{Z}_n$ such that $\{\xi_1, \dots, \xi_d\}$ and $\{\eta_1, \dots, \eta_d\}$ are multiplicatively inequivalent, but the frames they give are unitarily equivalent (and hence both have distinct vectors). Then by Lemma 4.1, there is an $a \in \mathbb{Z}_n$ satisfying (4.10), and so

$$z := (\xi_1(1), \dots, \xi_d(1), \eta_1(a), \dots, \eta_d(a)) \in V \cap \mathbb{T}^{2d}[n].$$

Suppose (by way of contradiction) that z is not exceptional, i.e., $z_{d+1}, \dots, z_{2d}$ is a permutation of $z_1, \dots, z_d$. Then after a reordering $\xi_j(1) = \eta_j(a) = \eta_j(1)^a$, $\forall j$, so that $\{\xi_j\} = \{\eta_j\}^a$. The frame given by $\{\xi_j\}$ has distinct vectors, and so $\{\xi_j\}$ generates $\hat{\mathbb{Z}}_n$. Thus $\{\xi_j(1)\} = \{\eta_j(1)\}^a$ generates the n-th roots of unity, and a must be a unit. This implies that $\{\xi_j\}$ and $\{\eta_j\}$ are multiplicatively equivalent, a contradiction. Thus z is an exceptional point. $\square$

The set of solutions to (4.11) in torsion points is described by the Mordell–Lang conjecture for tori, proved by Laurent [15, Theorem 2] (see also the Conjecture on page 299). This states the following:

Theorem 4.3. *Let $\Gamma \subset (\mathbb{C}^*)^k$ be a subgroup of finite rank, i.e. so that the quotient of Γ by its torsion subgroup is finitely generated, and let $X \subset (\mathbb{C}^*)^k$ be an algebraic subvariety. Then there is a finite collection of elements $\gamma_i \in \Gamma$ and algebraic subgroups $H_i \subset (\mathbb{C}^*)^k$ such that $\gamma_i \cdot H_i \subset X$ for all i, and*

$$X \cap \Gamma = \bigcup_i \gamma_i \cdot (H_i \cap \Gamma).$$

The following consequence of Theorem 4.3 will be useful for us.

Corollary 4.4. *Let f be a (holomorphic) polynomial on $\mathbb{C}^k$ with zero set*

$$Z(f) := \{z \in \mathbb{C}^k : f(z) = 0\}.$$

Then there is a finite number of (topologically) closed, connected subgroups $T_1, \ldots, T_m$ of $\mathbb{T}^k$, and points $p_1, \ldots, p_m$ in $\mathbb{T}^k_{\mathrm{tors}}$, such that

$$\mathbb{T}^k_{\mathrm{tors}} \cap Z(f) = \mathbb{T}^k_{\mathrm{tors}} \cap \bigcup_{j=1}^{m} (p_j \cdot T_j), \qquad p_j \cdot T_j \subset Z(f),\ \forall j. \tag{4.13}$$

Proof. We apply Theorem 4.3 with $\Gamma = \mathbb{T}^k_{\mathrm{tors}}$ and $X = Z(f) \cap (\mathbb{C}^*)^k$ to produce $p_i \in \mathbb{T}^k_{\mathrm{tors}}$ and algebraic subgroups $H_i \subset (\mathbb{C}^*)^k$ such that $p_i \cdot H_i \subset Z(f)$ for all i, and

$$\mathbb{T}^k_{\mathrm{tors}} \cap Z(f) = \bigcup_i p_i \cdot (H_i \cap \mathbb{T}^k_{\mathrm{tors}}). \tag{4.14}$$

We have $H_i \cap \mathbb{T}^k_{\mathrm{tors}} = (H_i \cap \mathbb{T}^k) \cap \mathbb{T}^k_{\mathrm{tors}}$, and $H_i \cap \mathbb{T}^k = \cup_j q_{ij} \cdot T_i$ where $q_{ij} \in \mathbb{T}^k_{\mathrm{tors}}$ and T_i is the identity component of $H_i \cap \mathbb{T}^k$, which is a (topologically) closed connected subgroup of $\mathbb{T}^k$. Combining this with (4.14) gives

$$\mathbb{T}^k_{\mathrm{tors}} \cap Z(f) = \bigcup_i \bigcup_j p_i \cdot q_{ij} \cdot (T_i \cap \mathbb{T}^k_{\mathrm{tors}}) = \mathbb{T}^k_{\mathrm{tors}} \cap \bigcup_i \bigcup_j p_i \cdot q_{ij} \cdot T_i.$$

We have $q_{ij} \cdot T_i \subset H_i$ for all i and j, and so $p_i \cdot q_{ij} \cdot T_i \subset p_i \cdot H_i \subset Z(f)$. This completes the proof. □

We now apply Corollary 4.4 to $V \cap \mathbb{T}^{2d}_{\mathrm{tors}}$. Let π be the projection of $\mathbb{T}^{2d}$ onto the first d components, i.e.,

$$\pi : \mathbb{T}^{2d} = \mathbb{T}^d \times \mathbb{T}^d \to \mathbb{T}^d : (z, w) \mapsto z.$$

For any $\sigma \in S_d$, let $T_\sigma = \{(z_1, \ldots, z_d, z_{\sigma 1}, \ldots, z_{\sigma d}) : |z_j| = 1\} \subset \mathbb{T}^{2d}$, so that

$$\mathbb{T}^{2d}_{\mathrm{tors}} \cap \bigcup_{\sigma \in S_d} T_\sigma$$

is the set of solutions to (4.11) in roots of unity that are not exceptional.

Lemma 4.5. *There are a finite number of (topologically) closed, connected subgroups $T_1, \ldots, T_m$ of $\mathbb{T}^{2d}$ satisfying* $\dim \pi(T_j) < d$ *for all j, and points $p_1, \ldots, p_m$ in $\mathbb{T}^{2d}_{\mathrm{tors}}$, such that*

$$\mathbb{T}^{2d}_{\mathrm{tors}} \cap V = \bigcup_{\sigma \in S_d} (\mathbb{T}^{2d}_{\mathrm{tors}} \cap T_\sigma) \cup \bigcup_{j=1}^{m} (\mathbb{T}^{2d}_{\mathrm{tors}} \cap p_j \cdot T_j). \tag{4.15}$$

Proof. We apply Corollary 4.4 with $Z(f) = V$. We now determine the possible tori T_j in (4.13) that can satisfy $p_j \cdot T_j \subset V$. For $\alpha \in \mathbb{Z}^k$ and $z \in \mathbb{T}^k$, we define $z^\alpha := z_1^{\alpha_1} \ldots z_k^{\alpha_k}$.

A connected subgroup $T \subset \mathbb{T}^{2d}$ of dimension k is the image of a map

$$\mathbb{T}^k \to \mathbb{T}^{2d} : z = (z_1, \ldots, z_k) \mapsto (z^{\alpha_1}, \ldots, z^{\alpha_{2d}}), \qquad \alpha_j \in \mathbb{Z}^k,$$

where the α_j must span $\mathbb{R}^k$, since the map has a discrete kernel. If $p = (\omega_1, \ldots, \omega_{2d}) \in \mathbb{T}^{2d}$, then $p \cdot T$ is the image of the map $z \mapsto (\omega_1 z^{\alpha_1}, \ldots, \omega_{2d} z^{\alpha_{2d}})$. Thus for the linear polynomial (4.11) to vanish on $p \cdot T$, we must have

$$\sum_{j=1}^{d} \omega_j z^{\alpha_j} - \sum_{j=d+1}^{2d} \omega_j z^{\alpha_j} = 0, \qquad \forall z \in \mathbb{T}^k.$$

For any exponent β, the sum of the coefficients of z^β above must be 0. It follows that any β occurring as an α_j must occur at least twice, and so there can be at most d distinct exponents. Thus the α_j can span $\mathbb{R}^k$ only if $k \le d$. If $k < d$, then clearly $\dim \pi(T) < d$.

If $k = d$, then every exponent occurs exactly twice. If some exponent occurs twice in the first sum, i.e., $\alpha_j = \alpha_k$ for some $1 \le j \ne k \le d$, then the function z_j/z_k is constant on T, which implies that $\dim \pi(T) < d$. If no exponent occurs twice in the first sum, then each exponent occurs once in each sum, i.e., $\alpha_{d+j} = \alpha_{\sigma j}$, $1 \le j \le d$, for some $\sigma \in S_d$. This implies that $T \subset T_\sigma$, and as both are d-dimensional and connected, we have that $T = T_\sigma$. We must also have $\omega_{d+j} = \omega_{\sigma j}$, $1 \le j \le d$, so that $p \in T$ and $p \cdot T = T_\sigma$.

We have shown that

$$\mathbb{T}^{2d}_{\text{tors}} \cap V = \bigcup_{\sigma \in X} (\mathbb{T}^{2d}_{\text{tors}} \cap T_\sigma) \cup \bigcup_{j=1}^{m} (\mathbb{T}^{2d}_{\text{tors}} \cap p_j \cdot T_j),$$

where $X \subset S_d$ and $\dim \pi(T_j) < d$ for all j. The inclusion

$$\bigcup_{\sigma \in S_d} (\mathbb{T}^{2d}_{\text{tors}} \cap T_\sigma) \subset \mathbb{T}^{2d}_{\text{tors}} \cap V$$

means that we can take $X = S_d$, which completes the proof. □

Proposition 4.6. *For d fixed, the number of choices of d characters of $\mathbb{Z}_n$ which lead to exceptional cyclic harmonic frames with distinct vectors is $\ll n^{d-1}$ as $n \to \infty$.*

Proof. Let $\mathcal{E} \subset \mathbb{T}^d[n]$ be the set of d-tuples of characters of $\mathbb{Z}_n$ (viewed as n-th roots) that give exceptional cyclic harmonic frames with distinct vectors, and let $\widetilde{\mathcal{E}} \subset V \cap \mathbb{T}^{2d}[n]$ be the set of exceptional points. By Lemma 4.2 and Lemma 4.5, we have

$$\mathcal{E} \subset \pi(\widetilde{\mathcal{E}}) \subset \mathbb{T}^d[n] \cap \bigcup_{j=1}^{m} \pi(p_j \cdot T_j),$$

with $\dim \pi(T_j) < d$ for all j, which implies that $|\mathbb{T}^d[n] \cap \pi(p_j \cdot T_j)| \ll n^{d-1}$. Since the collection of translates $p_j \cdot T_j$ only depends on d, we obtain $|\mathcal{E}| \ll n^{d-1}$ as required. □

5. Counting the nonexceptional cyclic harmonic frames

Let $m_{n,d}$ be the number of cyclic harmonic frames of n distinct vectors for $\mathbb{C}^d$, up to unitary equivalence via an automorphism, i.e., the number of d-element subsets which generate $\mathbb{Z}_n$, up to multiplicative equivalence. (In this section, it will be convenient to work with group elements rather than characters.) We will prove Theorem 3.1 by calculating $m_{n,d}$, then using Proposition 4.6 to conclude

$$h_{n,d} \approx m_{n,d}, \qquad n \to \infty.$$

Since all elements which generate $\mathbb{Z}_n$ are multiplicatively equivalent, we have $h_{n,1} = m_{n,1} = 1$. We may therefore assume that $d \ge 2$ for the rest of this section.

Let $\mathcal{Y}_{\text{gen}}$ be the set of all d-element subsets which generate $\mathbb{Z}_n$ (i.e. give cyclic harmonic frames with distinct vectors), and $\mathcal{Y}_{\text{ex}} \subset \mathcal{Y}_{\text{gen}}$ be the subset which gives exceptional frames. Then $m_{n,d}$ is the number of $\mathbb{Z}_n^*$-orbits of $\mathcal{Y}_{\text{gen}}$ under the multiplicative action of $\mathbb{Z}_n^*$.

If S is a collection of d-element subsets of $\mathbb{Z}_n$, and S is stable under the action of $\mathbb{Z}_n^*$, we denote the set of its orbits by $S/\mathbb{Z}_n^*$, and the set of its elements fixed by $a \in \mathbb{Z}_n^*$ by $\text{Fix}(a) = \text{Fix}(a, S)$.

Lemma 5.1. *We have the bounds*

$$|(\mathcal{Y}_{\mathrm{gen}} \setminus \mathcal{Y}_{\mathrm{ex}})/\mathbb{Z}_n^*| \leq h_{n,d} \leq m_{n,d} = |\mathcal{Y}_{\mathrm{gen}}/\mathbb{Z}_n^*|.$$

Proof. We observe $h_{n,d}$ is the number of equivalence classes in $\mathcal{Y}_{\mathrm{gen}}$ under the equivalence relation given by unitary equivalence of the corresponding frames. Since each equivalence class is stable under the action of $\mathbb{Z}_n^*$, the number of such classes is at most the number of $\mathbb{Z}_n^*$-orbits, which gives the upper bound. By definition of $\mathcal{Y}_{\mathrm{ex}}$, the unitary equivalence classes in $\mathcal{Y}_{\mathrm{gen}} \setminus \mathcal{Y}_{\mathrm{ex}}$ are exactly the $\mathbb{Z}_n^*$-orbits, which gives the lower bound. □

We now estimate the sizes of $\mathcal{Y}_{\mathrm{gen}}$ and $\mathcal{Y}_{\mathrm{gen}} \setminus \mathcal{Y}_{\mathrm{ex}}$.

Lemma 5.2. *We have*

$$|\mathcal{Y}_{\mathrm{gen}}|, |\mathcal{Y}_{\mathrm{gen}} \setminus \mathcal{Y}_{\mathrm{ex}}| = \frac{n^d}{d!} \prod_{p|n} (1 - p^{-d}) + O(n^{d-1}), \quad n \to \infty, \tag{5.16}$$

where the product is over the prime factors p of n.

Proof. It is convenient to work with the ordered subsets of $\mathbb{Z}_n$. Let $\mathcal{X} = \mathbb{Z}_n^d$ be the set of d-tuples of elements of $\mathbb{Z}_n$, $\mathcal{X}_{\mathrm{gen}}$ be the subset of those whose elements generate $\mathbb{Z}_n$, and $\mathcal{X}_{\mathrm{dist}}$ be the subset of those whose elements are all distinct. Clearly,

$$|\mathcal{Y}_{\mathrm{gen}}| = |\mathcal{X}_{\mathrm{dist}} \cap \mathcal{X}_{\mathrm{gen}}|/d!.$$

The size of $\mathcal{X}_{\mathrm{gen}}$ is *Hall's d-th Eulerian function* ($d = 1$ gives Euler's totient function $\varphi(n)$). We now calculate $|\mathcal{X}_{\mathrm{gen}}|$ by using inclusion–exclusion counting. Let $\mathcal{X}(m) \subset \mathcal{X}$ be the collection of d-tuples all of whose elements lie in $m\mathbb{Z}_n$. If some d-tuple does not generate $\mathbb{Z}_n$, then its elements must be contained in some maximal proper subgroup $p\mathbb{Z}_n$, $p|n$, and so we have

$$\mathcal{X}_{\mathrm{gen}} = \mathcal{X} \setminus \bigcup_{p|n} \mathcal{X}(p).$$

It is easy to see that if $p_1, \ldots, p_k$ are distinct primes dividing n, then

$$\Big|\bigcap_{j=1}^{k} \mathcal{X}(p_j)\Big| = |\mathcal{X}(p_1 p_2 \cdots p_k)| = \big(n/(p_1 p_2 \cdots p_k)\big)^d.$$

Thus, inclusion–exclusion counting gives

$$\begin{aligned} |\mathcal{X}_{\mathrm{gen}}| &= |\mathcal{X}| - \sum_{p|n} |\mathcal{X}(p)| + \sum_{\substack{p_1,p_2|n \\ p_1 \neq p_2}} |\mathcal{X}(p_1) \cap \mathcal{X}(p_2)| - \cdots \\ &= n^d \prod_{p|n} (1 - p^{-d}). \end{aligned}$$

Since $|\mathcal{X} \setminus \mathcal{X}_{\mathrm{dist}}| = n^d - n(n-1)\cdots(n-d+1) \ll n^{d-1}$, we have

$$d!|\mathcal{Y}_{\mathrm{gen}}| = |\mathcal{X}_{\mathrm{gen}} \cap \mathcal{X}_{\mathrm{dist}}| = n^d \prod_{p|n} (1 - p^{-d}) + O(n^{d-1})$$

which gives the estimate for $|\mathcal{Y}_{\text{gen}}|$. Because $|\mathcal{Y}_{\text{ex}}| \ll n^{d-1}$ by Proposition 4.6, we also have the estimate for $|\mathcal{Y}_{\text{gen}} \setminus \mathcal{Y}_{\text{ex}}|$. $\square$

We now count the number of orbits for the action of $\mathbb{Z}_n^*$ on $\mathcal{Y}_{\text{gen}}$ and $\mathcal{Y}_{\text{gen}} \setminus \mathcal{Y}_{\text{ex}}$. Recall Burnside's Theorem (see [17]), which states that if G is a finite group acting on a finite set S then the number of orbits is

$$|S/G| = \frac{1}{|G|} \sum_{a \in G} |\operatorname{Fix}(a, S)|. \tag{5.17}$$

We shall combine Burnside's Theorem with the following bound for $|\operatorname{Fix}(a, \mathcal{Y}_{\text{gen}})|$.

Lemma 5.3. *Let $a \in \mathbb{Z}_n^*$. Then*

1. $|\operatorname{Fix}(a, \mathcal{Y}_{\text{gen}})| \le n^{d-1}$ *for* $a \ne 1$.
2. $|\operatorname{Fix}(a, \mathcal{Y}_{\text{gen}})| \le n^{d-2}$ *for* $a^2 \ne 1$.

Proof. Let $A \in \operatorname{Fix}(a, \mathcal{Y}_{\text{gen}})$. We note that the elements of $A \in \mathcal{Y}_{\text{gen}}$ generate $\mathbb{Z}_n$.

If $a \ne 1$, then $H = \{b \in \mathbb{Z}_n : ab = b\}$ is a proper subgroup of $\mathbb{Z}_n$, and so there is some $b \in A$, $b \notin H$. As the choice of b determines a second element $ab \in A$, the number of choices for A is less than $n \cdot n^{d-2} = n^{d-1}$. Similarly, if $a^2 \ne 1$ (so $a \ne 1$), then $H = \{b \in \mathbb{Z}_n : a^2 b = b\}$ is a proper subgroup of $\mathbb{Z}_n$, so that $\{b, ab, a^2 b\}$ are distinct elements of A for $b \in A$, $b \notin H$. It follows that if $d = 2$ then $\operatorname{Fix}(a, \mathcal{Y}_{\text{gen}}) = \emptyset$, and if $d \ge 3$ the number of choices for A is less than $n \cdot n^{d-3} = n^{d-2}$. $\square$

Proposition 5.4. *For each $\epsilon > 0$, we have*

$$|\mathcal{Y}_{\text{gen}}/\mathbb{Z}_n^*|, |(\mathcal{Y}_{\text{gen}} \setminus \mathcal{Y}_{\text{ex}})/\mathbb{Z}_n^*| = \frac{1}{d!\varphi(n)} \Big(n^d \prod_{p|n} (1 - p^{-d}) + O_\epsilon(n^{d-1+\epsilon}) \Big), \quad n \to \infty. \tag{5.18}$$

Proof. Since $|\mathbb{Z}_n^*| = \varphi(n)$, counting the $\mathbb{Z}_n^*$-orbits of $\mathcal{Y}_{\text{gen}}$ by Burnside's Theorem (5.17) gives

$$|\mathcal{Y}_{\text{gen}}/\mathbb{Z}_n^*| = \frac{1}{\varphi(n)} \sum_{a \in \mathbb{Z}_n^*} |\operatorname{Fix}(a, \mathcal{Y}_{\text{gen}})|.$$

Partition $\mathbb{Z}_n^*$ into $\{1\}$, $B = \{a : a^2 = 1, a \ne 1\}$ and $\{a : a^2 \ne 1\}$, and apply Lemma 5.3 to the last two sets to obtain

$$|\mathcal{Y}_{\text{gen}}/\mathbb{Z}_n^*| \le \frac{1}{\varphi(n)} \big(|\mathcal{Y}_{\text{gen}}| + |B| n^{d-1} + \varphi(n) n^{d-2} \big).$$

We recall that $\mathbb{Z}_{p^m}^*$ is cyclic for p an odd prime, and $\mathbb{Z}_{2^m}^*$ is a product of at most two cyclic groups. By the Chinese Remainder Theorem and the structure of $\mathbb{Z}_{p^m}^*$ for p prime, we have

$$|B| < |\{a \in \mathbb{Z}_n^* : a^2 = 1\}| \le 2^{\omega(n)+1}$$

where $\omega(n)$ is the number of prime factors of n. We see that $2^{\omega(n)}$ is at most the number of divisors $d(n)$ of n, and it is known that $d(n) \ll_\epsilon n^\epsilon$, see for instance [1, Thm 13.12]. Applying this and $\varphi(n) \le n$ gives

$$|\mathcal{Y}_{\text{gen}}/\mathbb{Z}_n^*| \le \frac{1}{\varphi(n)} \big(|\mathcal{Y}_{\text{gen}}| + O_\epsilon(n^{d-1+\epsilon}) \big).$$

Combining this with the estimate (5.16) for $|\mathcal{Y}_{\rm gen}|$ gives the upper bound

$$|\mathcal{Y}_{\rm gen}/\mathbb{Z}_n^*| \le \frac{1}{d!\varphi(n)}\big(n^d\prod_{p|n}(1-p^{-d})+O_\epsilon(n^{d-1+\epsilon})\big). \tag{5.19}$$

We estimate $|(\mathcal{Y}_{\rm gen}\setminus\mathcal{Y}_{\rm ex})/\mathbb{Z}_n^*|$ in the same way. Let $S=\mathcal{Y}_{\rm gen}\setminus\mathcal{Y}_{\rm ex}$ in (5.17) and take only the $a=1$ term to obtain

$$|(\mathcal{Y}_{\rm gen}\setminus\mathcal{Y}_{\rm ex})/\mathbb{Z}_n^*| \ge \frac{1}{\varphi(n)}|\mathcal{Y}_{\rm gen}\setminus\mathcal{Y}_{\rm ex}|.$$

Combining this with the estimate (5.16) for $|\mathcal{Y}_{\rm gen}\setminus\mathcal{Y}_{\rm ex}|$ gives the lower bound

$$|(\mathcal{Y}_{\rm gen}\setminus\mathcal{Y}_{\rm ex})/\mathbb{Z}_n^*| \ge \frac{1}{d!\varphi(n)}\big(n^d\prod_{p|n}(1-p^{-d})+O_\epsilon(n^{d-1+\epsilon})\big). \tag{5.20}$$

Since $|(\mathcal{Y}_{\rm gen}\setminus\mathcal{Y}_{\rm ex})/\mathbb{Z}_n^*| \le |\mathcal{Y}_{\rm gen}/\mathbb{Z}_n^*|$, the bounds (5.19) and (5.20) give (5.18). $\square$

By Lemma 5.1, Proposition 5.4 and (3.9), we have

$$\begin{aligned} h_{n,d}, m_{n,d} &= \frac{1}{d!\varphi(n)}\big(n^d\prod_{p|n}(1-p^{-d})+O_\epsilon(n^{d-1+\epsilon})\big) \\ &= \frac{n^d}{d!\varphi(n)}\prod_{p|n}(1-p^{-d})\big(1+O_\epsilon(n^{-1+\epsilon})\big), \qquad n\to\infty, \end{aligned}$$

which completes the proof of Theorem 3.1 (we already observed that $h_{n,1}=m_{n,1}=1$).

6. Some examples

The number of cyclic harmonic frames up to multiplicative equivalence can be calculated exactly by Burnside counting (this can be done by a computer algebra package):

$$m_{n,d}=|\mathcal{Y}_{\rm gen}/\mathbb{Z}_n^*| = \frac{1}{\varphi(n)}\Big(|\mathcal{Y}_{\rm gen}| + \sum_{\substack{a\in\mathbb{Z}_n^* \\ a\ne 1}} |\operatorname{Fix}(a,\mathcal{Y}_{\rm gen})|\Big). \tag{6.21}$$

This slightly over counts $h_{n,d}$ when there are exceptional frames. Theorem 3.1 gives the approximation

$$h_{n,d}\approx a_{n,d} := \frac{n^d}{d!\varphi(n)}\prod_{p|n}(1-p^{-d}), \qquad n\to\infty. \tag{6.22}$$

This appears to give a good fit to $h_{n,d}$ and $m_{n,d}$ (even for small values of n), see Fig. 1.

Since $\varphi(n)$ is multiplicative, with

$$\varphi(p^m)=p^m\Big(1-\frac{1}{p}\Big),$$

it follows that

$$a_{n,1}=1, \qquad a_{n,2}=\frac{n}{2}\prod_{p|n}\Big(1+\frac{1}{p}\Big)\in\mathbb{Z}, \quad n>2.$$

For $d>2$, $a_{n,d}$ may not be an integer.

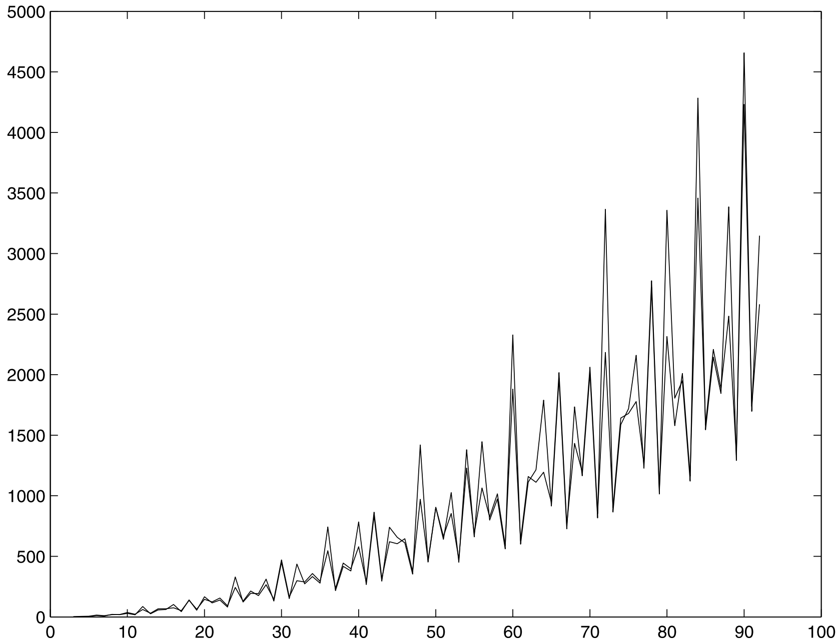

Fig. 1. The number of harmonic frames of n distinct vectors for $\mathbb{C}^3$ (including noncyclic frames) as calculated by [24] together with $a_{n,3}$.

Example 6.1. For $d = 2$, unitary equivalence and multiplicative equivalence are the same [7], i.e., $h_{n,2} = m_{n,2}$. Despite $a_{n,2}$ being an integer, it does not always equal $m_{n,2}$. They first differ for $n = 8$, when the units group has three elements of order 2, i.e., $3, 5, 7 \in \mathbb{Z}_8^*$ with

$$\mathrm{Fix}(3) = \big\{\{1,3\},\{5,7\}\big\}, \quad \mathrm{Fix}(5) = \big\{\{1,5\},\{3,7\}\big\} \qquad \mathrm{Fix}(7) = \big\{\{3,5\},\{1,7\}\big\}.$$

Since $\mathcal{Y}_{\mathrm{gen}}$ has 22 elements, (6.21) gives $a_{8,2} = 6 < 7 = \frac{1}{4}(22 + 2 + 2 + 2) = m_{8,2}$.

Example 6.2. For $d > 2$ there exist exceptional cyclic frames, e.g., for $n = 8$ vectors in $\mathbb{C}^3$, there are 17 multiplicative equivalence classes of 3-element subsets that generate $\mathbb{Z}_8$. The classes

$$\big\{\{1,2,5\},\{3,6,7\}\big\}, \qquad \big\{\{1,5,6\},\{2,3,7\}\big\}$$

give exceptional frames (a frame from each class gives an exceptional pair), and it is easy to show that $h_{8,3} = 16 < 17 = m_{8,3}$.

7. Harmonic frames with a prime number of vectors

When n is prime, then the $n-1$ primitive n-th roots of unity are a $\mathbb{Q}$-basis for the cyclotomic field $\mathbb{Q}[\omega]$ that they generate. As a consequence, many of the inner products between vectors of the (cyclic) harmonic frames are distinct, and so there are no exceptional frames:

Proposition 7.1. *If $n = p$ is prime, then all harmonic frames of n distinct vectors for $\mathbb{C}^d$ are cyclic, and multiplicative and unitary equivalence are the same for these frames, i.e., $h_{p,d} = m_{p,d}$.*

Proof. Let $\{\xi_1, \ldots, \xi_d\}$ and $\{\eta_1, \ldots, \eta_d\}$ be characters of $\mathbb{Z}_p$ giving unitarily equivalent harmonic frames with distinct vectors. By Lemma 4.1 there is some $a \in \mathbb{Z}_p$ with

$$\sum_{j=1}^{d} \xi_j(1) = \sum_{j=1}^{d} \eta_j(a). \tag{7.23}$$

We will show that after a reordering $\xi_j(1) = \eta_j(a)$, $\forall j$. The argument of Lemma 4.2 then implies that the frames are multiplicatively equivalent.

Let ω be a primitive p-th root of unity, and a_j and b_j be the number of times that ω^j occurs as a summand on the left hand and right hand sides of (7.23). Then

$$a_0 + \cdots + a_{p-1} = b_0 + \cdots + b_{p-1} = d. \tag{7.24}$$

Since $1+\omega+\cdots+\omega^{p-1} = 0$, we may replace each appearance of 1 in (7.23) by $-\omega - \cdots - \omega^{p-1}$, and equate coefficients of the resulting $\mathbb{Q}$-linear combinations of primitive roots to obtain

$$a_j - a_0 = b_j - b_0, \qquad j = 1, 2, \ldots, p-1. \tag{7.25}$$

Solving the system (7.24) and (7.25) of p linear equations in $a_0, \ldots, a_{p-1}$ gives $a_j = b_j$, $\forall j$. $\square$

The above argument shows that harmonic frames that are unitarily inequivalent have no inner product between distinct vectors in common.

For $n = p$ prime we are able to give an explicit formula for the count (6.21) of $m_{p,d} = h_{p,d}$. It is convenient to split this into the *lifted* and *unlifted* harmonic frames. We say that a harmonic frame given by $J \subset \mathbb{Z}_n$ is **lifted** if $0 \in J$, equivalently, the subset of characters defining it contains the trivial character $1 \in \hat{\mathbb{Z}}_n$, or its vectors have a nonzero sum.

Theorem 7.2. *Let p be a prime, and $h^{\mathrm{u}}_{p,d}$ and $h^{\mathrm{l}}_{p,d}$ be the number of unlifted and lifted harmonic frames of p distinct vectors for $\mathbb{C}^d$ up to unitary equivalence. For $d > 1$, we have*

$$h^{\mathrm{u}}_{p,d} = \frac{1}{p-1} \sum_{j|\gcd(p-1,d)} \binom{\frac{p-1}{j}}{\frac{d}{j}} \varphi(j), \tag{7.26}$$

$$h^{\mathrm{l}}_{p,d} = \frac{1}{p-1} \sum_{j|\gcd(p-1,d-1)} \binom{\frac{p-1}{j}}{\frac{d-1}{j}} \varphi(j). \tag{7.27}$$

Proof. For $d = 1$, the unique harmonic frame (with distinct vectors) is unlifted, so that $h^{\mathrm{u}}_{p,1} = 1$, $h^{\mathrm{l}}_{p,1} = 0$. We observe that the formula (7.26) also holds for $d = 1$. For $d > 1$, all d-element subsets of $\mathbb{Z}_p$ generate $\mathbb{Z}_p$, and so all harmonic frames have distinct vectors.

We first count the unitarily inequivalent unlifted harmonic frames, i.e., the number of d-element subsets of $\mathbb{Z}_p \setminus \{0\}$ up to multiplicative equivalence. If $a \in \mathbb{Z}_p^*$ has order j, then its action on $\mathbb{Z}_p \setminus \{0\}$ gives $\frac{p-1}{j}$ orbits of size j. In order for there to be a d-element subset J of $\mathbb{Z}_p \setminus \{0\}$ fixed by a, we must have $j|d$, and the number of such subsets is $|\operatorname{Fix}(a)| = \binom{\frac{p-1}{j}}{\frac{d}{j}}$. There are $\varphi(j)$ elements in $\mathbb{Z}_p^*$ of order j, and so Burnside's theorem (5.17) applied to S the collection of d-element subsets of $\mathbb{Z}_p \setminus \{0\}$ gives the first formula:

$$h^{\mathrm{u}}_{p,d} = \frac{1}{|\mathbb{Z}_p^*|} \sum_{j|\gcd(p-1,d)} \sum_{\substack{a\in\mathbb{Z}_p^* \\ \operatorname{ord}(a)=j}} |\operatorname{Fix}(a,S)| = \frac{1}{p-1} \sum_{j|\gcd(p-1,d)} \binom{\frac{p-1}{j}}{\frac{d}{j}} \varphi(j).$$

We now count the lifted frames. These are given by the d-element subsets $J \subset \mathbb{Z}_p$ with $0 \in J$, which are multiplicatively equivalent if and only if the $(d-1)$-element subsets $J \setminus \{0\}$ are. Thus $h^{\mathrm{l}}_{p,d} = h^{\mathrm{u}}_{p,d-1}$, which gives (7.27) since the formula for $h^{\mathrm{u}}_{p,d}$ holds for $d \geq 1$. $\square$

A backwards recursive formula for $h_{p,d}$ based on orbit counting is given in [12].

Example 7.3. For $d = 2$ and $p > 2$, we have $h_{p,2} = \frac{1}{2}(p+1)$, since

$$h^{\mathrm{u}}_{p,1} = h^{\mathrm{l}}_{p,2} = 1, \qquad h^{\mathrm{u}}_{p,2} = h^{\mathrm{l}}_{p,3} = \frac{1}{p-1}\Big\{\binom{p-1}{2} + \binom{\frac{p-1}{2}}{1}\Big\} = \frac{1}{2}(p-1).$$

Example 7.4. For $d = 3$ and $p > 2$, we have

$$h^{\mathrm{u}}_{p,3} = h^{\mathrm{l}}_{p,4} = \frac{1}{p-1}\begin{cases}\binom{p-1}{3}, & p \not\equiv 1 \pmod 3;\\ \binom{p-1}{3} + 2\binom{\frac{p-1}{3}}{1}, & p \equiv 1 \pmod 3.\end{cases}$$

Hence

$$h_{p,3} = \begin{cases}\frac{1}{6}(p^2-2p+3), & p \not\equiv 1 \pmod 3;\\ \frac{1}{6}(p^2-2p+7), & p \equiv 1 \pmod 3.\end{cases}$$

The above formulas for $p \equiv 1 \pmod 3$ and $p \equiv 2 \pmod 3$ appear in [12] (Prop. 4.2).

Example 7.5. For $d = 4$ and $p > 2$, we have

$$h^{\mathrm{u}}_{p,4} = h^{\mathrm{l}}_{p,5} = \frac{1}{p-1}\begin{cases}\binom{p-1}{4} + \binom{\frac{p-1}{2}}{2}, & p \not\equiv 1 \pmod 4;\\ \binom{p-1}{4} + \binom{\frac{p-1}{2}}{2} + 2\binom{\frac{p-1}{4}}{1}, & p \equiv 1 \pmod 4.\end{cases}$$

As indicated, we can construct formulas for $h_{p,d}$ depending on p modulo d and $d-1$, e.g.,

$$h_{p,4} = h^{\mathrm{u}}_{p,4} + h^{\mathrm{l}}_{p,4} = \frac{1}{24}(p^3 - 5p^2 + 9p + 19), \qquad p \equiv 1 \pmod{12}.$$

It is also possible to count the number of *real* harmonic frames. We recall that $J \subset \mathbb{Z}_n$ gives a real harmonic frame if and only if it is closed under taking inverses, i.e., $J = -J$. For $n = p$ an odd prime, $-j = j$ if and only if $j = 0$, and so the J giving real frames have $0 \notin J$ when d is even, and $0 \in J$ when d is odd. Burnside counting gives the following.

Proposition 7.6. *Let p be an odd prime and $d > 1$. For d even, the number of real harmonic (unlifted) frames of p distinct vectors for $\mathbb{R}^d$ (up to unitary equivalence) is*

$$h^{\mathbb{R}}_{p,d} = \frac{1}{p-1}\Big\{\sum_{\substack{j \mid \gcd(p-1,d)\\ j \text{ even}}} \binom{\frac{p-1}{j}}{\frac{d}{j}}\varphi(j) + \sum_{\substack{j \mid \gcd(p-1,\frac{d}{2})\\ j \text{ odd}}} \binom{\frac{p-1}{2j}}{\frac{d}{2j}}\varphi(j)\Big\}.$$

For d odd, the number of real harmonic (lifted) frames of p distinct vectors for $\mathbb{R}^d$ is

$$h^{\mathbb{R}}_{p,d} = \frac{1}{p-1}\Big\{\sum_{\substack{j \mid \gcd(p-1,d-1)\\ j \text{ even}}} \binom{\frac{p-1}{j}}{\frac{d-1}{j}}\varphi(j) + \sum_{\substack{j \mid \gcd(p-1,\frac{d-1}{2})\\ j \text{ odd}}} \binom{\frac{p-1}{2j}}{\frac{d-1}{2j}}\varphi(j)\Big\}.$$

Proof. We first consider the case when d is even. The unit group $\mathbb{Z}_p^*$ is cyclic of even order $p-1$, and we let $a \in \mathbb{Z}_p^*$ have order j. We wish to count the number of d-element sets $J \subset \mathbb{Z}_p \setminus \{0\}$ that are invariant under multiplication by a and -1. If j is even, then $-1 = a^{\frac{j}{2}}$, and so this is equal to the number of subsets invariant under multiplication by a. This is $\binom{\frac{p-1}{j}}{\frac{d}{j}}$ as in the proof of Theorem 7.2. If j is odd, then the subgroup of $\mathbb{Z}_p^*$ generated by -1 and a is cyclic with generator $-a$. We therefore wish to find the number of subsets invariant under multiplication by $-a$, and as this element has order $2j$, this is $\binom{\frac{p-1}{2j}}{\frac{d}{2j}}$.

Thus Burnside orbit counting gives

$$h^{\mathbb{R}}_{p,d} = \frac{1}{p-1}\Big\{ \sum_{\substack{j \mid \gcd(p-1,d) \\ j \text{ even}}} \binom{\frac{p-1}{j}}{\frac{d}{j}} \varphi(j) + \sum_{\substack{j \mid \gcd(p-1,\frac{d}{2}) \\ j \text{ odd}}} \binom{\frac{p-1}{2j}}{\frac{d}{2j}} \varphi(j) \Big\}.$$

When d is odd, the subsets J giving real frames are multiplicatively equivalent if and only if the sets $J \setminus \{0\}$ are, and so we may apply the previous count (with d replaced by $d-1$). $\square$

Example 7.7. For $d = 2, 3$, there is a single real harmonic frame of p distinct vectors, i.e.,

$$h^{\mathbb{R}}_{p,2} = h^{\mathbb{R}}_{p,3} = 1.$$

For d even, $d \geq 4$, we have the estimate

$$h^{\mathbb{R}}_{p,d} = h^{\mathbb{R}}_{p,d+1} \approx p^{\frac{d}{2}-1}, \qquad p \to \infty.$$

8. Projective unitary equivalence of harmonic frames

Many applications of tight frames (v_j) are based on the expansion (2.2), i.e., depend only on the vectors up to unit scalar multiples. We say that tight frames (v_j) and (w_k) are **projectively unitarily equivalent** (up to a reindexing) if there is a unitary map U, unit modulus scalars c_j, and a bijection $\sigma : j \to k$ (a reindexing) between their index sets for which

$$v_j = c_j U w_{\sigma j}, \qquad \forall j.$$

In [8] it is shown that harmonic frames given by subsets $J, K \subset G$ are projectively unitarily equivalent (with σ the identity) if J and K are translates, i.e., $K = J - b$, $b \in G$. Therefore the *affine transformations* $L_{(\sigma,b)}$ given by

$$L_{(\sigma,b)} g := \sigma g + b, \qquad \sigma \in \mathrm{Aut}(G),\ b \in G$$

map subsets $J \subset G$ to subsets which give projectively unitarily equivalent harmonic frames (via an automorphism). Calculations of [8] suggest that the majority of projective unitary equivalences occur in this way, via a reindexing which is an automorphism (indeed there is no known case where it does not). We observe that every d-element subset of $\mathbb{Z}_n$ is a translate of one which generates $\mathbb{Z}_n$, and so every cyclic harmonic frame is projectively unitarily equivalent to one with distinct vectors.

We now count the number $p_{n,d}$ of cyclic harmonic frames Φ_J for $\mathbb{C}^d$ up to this projective unitary equivalence via an affine transformation of the index set J. Since the affine group (group of affine transformations) has order $n\varphi(n)$ and there are $\binom{n}{d}$ subsets of $\mathbb{Z}_n$ of size d, we have

$$p_{n,d} \geq \frac{\binom{n}{d}}{n\varphi(n)} \gg \frac{n^{d-1}}{\varphi(n)} \geq n^{d-2}, \qquad n \to \infty.$$

For $d \geq 4$, we can establish this rate of growth. Since $\mathbb{Z}_n^*$ gives the automorphisms of $\mathbb{Z}_n$, the group of affine transformations of $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_n^* \ltimes \mathbb{Z}_n$, with $(a,b) \in \mathbb{Z}_n^* \ltimes \mathbb{Z}_n$ acting on $\mathbb{Z}_n$ via $x \mapsto ax + b$.

Theorem 8.1. *Let $p_{n,d}$ be the number of orbits of the affine group acting on the d-element subsets of $\mathbb{Z}_n$. For $d \geq 4$, we have*

$$p_{n,d} \approx \frac{n^{d-1}}{\varphi(n)} \geq n^{d-2}, \qquad n \to \infty. \tag{8.28}$$

Proof. To obtain an upper bound for $p_{n,d}$, we estimate the terms in the Burnside orbit counting formula

$$p_{n,d} = \frac{1}{n\varphi(n)} \sum_{(a,b)\in\mathbb{Z}_n^*\ltimes\mathbb{Z}_n} |\operatorname{Fix}(a,b)|, \tag{8.29}$$

where $\operatorname{Fix}(a,b)$ is the collection of d-element subsets $A \subset \mathbb{Z}_n$ fixed by the action of (a,b). The orbit of x under the action of $(a,b) \in \mathbb{Z}_n^* \ltimes \mathbb{Z}_n$ is

$$x, \quad ax+b, \quad a^2x+ab+b, \quad \ldots.$$

Since $ax+b = x+((a-1)x+b)$, all orbits will have at least two elements provided that $b \notin (a-1)\mathbb{Z}_n$. Thus, our assumption $d \geq 4$ implies that any A fixed by (a,b) with $b \notin (a-1)\mathbb{Z}_n$ will have at least two of its elements determined by the fact it is a union of orbits. This implies the contribution to the sum in (8.29) by these elements is at most $n^{d-2}|\mathbb{Z}_n^* \ltimes \mathbb{Z}_n| \leq n^d$. It therefore remains to show the contribution to the sum in (8.29) from the elements (a,b) with $b \in (a-1)\mathbb{Z}_n$ is $\ll n^d$.

Suppose that $b \in (a-1)\mathbb{Z}_n$. Conjugating (a,b) by $(1,c)$ does not change the size of $\operatorname{Fix}(a,b)$. Since $(1,c)(a,b)(1,c)^{-1} = (a, b+c(1-a))$ and $b \in (a-1)\mathbb{Z}_n$, we may choose a c so that $(1,c)(a,b)(1,c)^{-1} = (a,0)$. Thus $|\operatorname{Fix}(a,b)| = |\operatorname{Fix}(a,0)|$. We observe the action of $(a,0)$ and a on $\mathbb{Z}_n$ is the same. Let $m := \gcd(a-1,n)$. Then

$$(a-1)\mathbb{Z}_n = m\mathbb{Z}_n,$$

and the subgroup of $\mathbb{Z}_n$ on which a acts trivially is

$$H = \{x \in \mathbb{Z}_n : ax = x\} = \frac{n}{m}\mathbb{Z}_n.$$

We partition $\operatorname{Fix}(a,0) = \cup_j F_j$, where each $A \in F_j$ has exactly j elements not in H, i.e.,

$$F_j := \{A \in \operatorname{Fix}(a,0) : |A \setminus H| = j\}, \qquad j = 0,1,\ldots,d.$$

If $x \notin H$, then $ax \neq x$ and $ax \notin H$ (otherwise $ax = a^{-1}a(ax) = a^{-1}ax = x$), so that

$$|F_0| \leq |H|^d = m^d, \qquad |F_1| = 0, \qquad |F_2| \leq |H|^{d-2}n = m^{d-2}n, \qquad \sum_{j\geq 3}|F_j| \leq n^{d-2}.$$

The last inequality holds because any A with at least 3 elements not in H has at least 2 elements determined by the fact it is a union of orbits. Using these, we have the estimate

$$\begin{aligned}
\sum_{\substack{(a,b)\in\mathbb{Z}_n^*\ltimes\mathbb{Z}_n \\ b\in(a-1)\mathbb{Z}_n}} |\operatorname{Fix}(a,b)| &\leq \sum_{m|n} \sum_{\substack{a\in\mathbb{Z}_n^* \\ m=\gcd(a-1,n)}} \sum_{b\in m\mathbb{Z}_n} |\operatorname{Fix}(a,0)| \leq \sum_{m|n} \frac{n}{m}\frac{n}{m}\Big(|F_0| + |F_2| + \sum_{j\geq 3}|F_j|\Big) \\
&\leq n^d \sum_{m|n}\left(\frac{n}{m}\right)^{2-d} + n^{d-1}\sum_{m|n}\left(\frac{n}{m}\right)^{4-d} + n^d \sum_{m|n}\frac{1}{m^2} \\
&\leq n^d \sum_k \frac{1}{k^2} + n^{d-1}\sum_{m|n} 1 + n^d \sum_m \frac{1}{m^2} \ll n^d,
\end{aligned}$$

which completes the proof. $\square$

Lemma 8.2. *For n prime, (8.28) also holds for $d = 3$.*

Proof. If n is prime, then for any 3-element subset $A \subset \mathbb{Z}_n$ there is an affine transformation (a, b) so that $(a, b)A$ contains 0 and 1. There are at most n choices for the third element, so that $n \geq p_{n,3}$. $\square$

Acknowledgments

The first author was supported by NSF grants DMS-1509331 and DMS-1501230, and would like to thank the University of Auckland for its hospitality while part of this work was carried out.

References

[1] Tom M. Apostol, Introduction to Analytic Number Theory, Undergrad. Texts Math., Springer, 1976.
[2] Bernhard G. Bodmann, Vern I. Paulsen, Frames, graphs and erasures, Linear Algebra Appl. 404 (2005) 118–146.
[3] Peter G. Casazza, Jelena Kovačević, Equal-norm tight frames with erasures, Adv. Comput. Math. 18 (2–4) (2003) 387–430, Frames.
[4] A. Chebira, J. Kovačević, Life beyond bases: the advent of frames (part i), IEEE Signal Process. Mag. 24 (2007) 86–104.
[5] Peter G. Casazza, Gitta Kutyniok (Eds.), Finite Frames, Appl. Numer. Harmon. Anal., Birkhäuser/Springer, New York, 2013, Theory and applications.
[6] Emmanuel J. Candès, Justin K. Romberg, Terence Tao, Stable signal recovery from incomplete and inaccurate measurements, Comm. Pure Appl. Math. 59 (8) (2006) 1207–1223.
[7] Tuan-Yow Chien, Shayne Waldron, A classification of the harmonic frames up to unitary equivalence, Appl. Comput. Harmon. Anal. 30 (3) (2011) 307–318.
[8] Tuan-Yow Chien, Shayne Waldron, A characterization of projective unitary equivalence of finite frames and applications, SIAM J. Discrete Math. 30 (2) (2016) 976–994.
[9] Yonina C. Eldar, Helmut Bölcskei, Geometrically uniform frames, IEEE Trans. Inform. Theory 49 (4) (2003) 993–1006.
[10] Vivek K. Goyal, Jelena Kovačević, Jonathan A. Kelner, Quantized frame expansions with erasures, Appl. Comput. Harmon. Anal. 10 (3) (2001) 203–233.
[11] Vivek K. Goyal, Martin Vetterli, Nguyen T. Thao, Quantized overcomplete expansions in $\mathbf{R}^N$: analysis, synthesis, and algorithms, IEEE Trans. Inform. Theory 44 (1) (1998) 16–31.
[12] Matthew Hirn, The number of harmonic frames of prime order, Linear Algebra Appl. 432 (5) (2010) 1105–1125.
[13] B.M. Hochwald, T.L. Marzetta, T.J. Richardson, W. Sweldens, R. Urbanke, Systematic design of unitary space-time constellations, IEEE Trans. Inform. Theory 46 (6) (Sep 2000) 1962–1973.
[14] Roderick B. Holmes, Vern I. Paulsen, Optimal frames for erasures, Linear Algebra Appl. 377 (2004) 31–51.
[15] Michel Laurent, Équations diophantiennes exponentielles, Invent. Math. 78 (2) (1984) 299–327.
[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] Joseph J. Rotman, An Introduction to the Theory of Groups, fourth ed., Grad. Texts in Math., vol. 148, Springer-Verlag, New York, 1995.
[18] J. Barkley Rosser, Lowell Schoenfeld, Approximate formulas for some functions of prime numbers, Illinois J. Math. 6 (1962) 64–94.
[19] Mark Rudelson, Roman Vershynin, On sparse reconstruction from Fourier and Gaussian measurements, Comm. Pure Appl. Math. 61 (8) (2008) 1025–1045.
[20] A.J. Scott, M. Grassl, SIC-POVMs: a new computer study, ArXiv e-prints, October 2009.
[21] Richard Vale, Shayne Waldron, Tight frames and their symmetries, Constr. Approx. 21 (1) (2005) 83–112.
[22] Shayne Waldron, Group frames, in: Finite Frames, in: Appl. Numer. Harmon. Anal., Birkhäuser/Springer, New York, 2013, pp. 171–191.
[23] Shayne Waldron, An Introduction to Finite Tight Frames, Birkhäuser/Springer, New York, 2017.
[24] Shayne Waldron, Nick Hay, On computing all harmonic frames of n vectors in $\mathbb{C}^d$, Appl. Comput. Harmon. Anal. 21 (2) (2006) 168–181.
[25] Gerhard Zauner, Quantum Designs: Foundations of a Non-Commutative Design Theory, PhD thesis, University of Vienna, 2010, English translation of 1999 Doctorial thesis including a new preface.