The Number of Harmonic Frames of Prime Order[☆]

Matthew J. Hirn

Yale University
Department of Mathematics
P.O. Box 208283
New Haven, Connecticut 06520-8283
USA

Abstract

Harmonic frames of prime order are investigated. The primary focus is the enumeration of inequivalent harmonic frames, with the exact number given by a recursive formula. The key to this result is a one-to-one correspondence developed between inequivalent harmonic frames and the orbits of a particular set. Secondarily, the symmetry group of prime order harmonic frames is shown to contain a subgroup consisting of a diagonal matrix as well as a permutation matrix, each of which is dependent on the particular harmonic frame in question.

Key words: finite unit norm tight frame, harmonic frame, symmetry group of frame
AMS classification codes: primary 42C15; secondary 05A05, 20E07

1. Introduction

1.1. DFT-FUNTFs

Let $N, d \in \mathbb{N} = \{1, 2, 3, \ldots\}$, $d \leq N$, and consider the space $\mathbb{C}^d$. An ordered set $X = (x_1, \ldots, x_N) \subset \mathbb{C}^d$ is a *finite frame* for $\mathbb{C}^d$ if there exist constants $A, B > 0$ such that

$$A\|f\|^2 \leq \sum_{j=1}^{N} |\langle f, x_j \rangle|^2 \leq B\|f\|^2, \quad \forall\ f \in \mathbb{C}^d. \tag{1.1}$$

The numbers A, B are called the *frame bounds*. It is well known that any spanning set is a frame for $\mathbb{C}^d$, while every frame is itself a spanning set. A

[☆]Submitted to *Linear Algebra and its Applications* 15 April 2009. Accepted 22 September 2009. Published in Volume 432, Issue 5, 15 February 2010, Pages 1105-1125. LaTeX file last compiled 2 September 2012.
Email address: matthew.hirn@yale.edu (Matthew J. Hirn)
URL: www.math.yale.edu/∼mh644 (Matthew J. Hirn)

frame is *tight* if one can choose $A = B$ in the definition, i.e., if

$$\sum_{j=1}^{N} |\langle f, x_j \rangle|^2 = A\|f\|^2, \quad \forall \ f \in \mathbb{C}^d. \tag{1.2}$$

Finally, a frame is *unit norm* if

$$\|x_j\| = 1, \quad \forall \ j = 1, \ldots, s. \tag{1.3}$$

If X satisfies (1.2) and (1.3), then we say X is a *finite unit norm tight frame* (FUNTF) for $\mathbb{C}^d$. In this case, the frame bounds satisfy $A = B = N/d$. In particular, if X is a FUNTF with frame bounds $A = B = 1$, then X is an orthonormal basis.

There has been much literature on the subject of finite tight frames, see for example [1, 2, 5, 8, 11] and references therein. One special class of FUNTFs is obtained by considering the un-normalized Discrete Fourier Transform (DFT) matrix,

$$D_N := (e^{2\pi imn/N})_{m,n=0}^{N-1}. \tag{1.4}$$

Choose any distinct d columns, $n_1, \ldots, n_d$, of D_N, with $n_j \in \{0, \ldots, N-1\}$ for each $j = 1, \ldots, d$, and form the following N vectors in $\mathbb{C}^d$,

$$\phi_m = \frac{1}{\sqrt{d}}(e^{2\pi imn_1/N}, e^{2\pi imn_2/N}, \ldots, e^{2\pi imn_d/N}) \in \mathbb{C}^d, \quad m = 0, 1, \ldots, N-1. \tag{1.5}$$

It is well known that $\Phi = (\phi_0, \ldots, \phi_{N-1})$ is a FUNTF for $\mathbb{C}^d$. Any frame of this type is called a DFT-FUNTF, and collectively, they form a subset of a special class of frames known as harmonic frames (see [9, 10] as well as section 2.1). We call the column choices $n_1, \ldots, n_d$ the *generators* of the frame.

A basic way of counting the number of DFT-FUNTFs is inspired by the following observation. For any vector $f \in \mathbb{C}^d$, the frame Φ gives the following representation of f:

$$f \mapsto (\langle f, \phi_m \rangle)_{m=0}^{N-1} \in \mathbb{C}^N.$$

Therefore, even a re-indexing of the frame would change the representation it gives for a fixed f. Thus, we could count the number of ordered DFT-FUNTFs. To accomplish this task, we observe that there are N columns in D_N and we select d of them. Since each ordered combination of column choices $n_1, \ldots, n_d$ gives a distinct frame, there are $N(N-1)\cdots(N-d+1)$ ordered DFT-FUNTFs.

There are of course other ways by which we may distinguish frames, and we shall consider two others here. The first is a natural counterpart to the ordered counting scheme, namely, counting the number of DFT-FUNTFs considered as unordered sets of vectors. The techniques developed for this method will then be expanded to our main goal, which is to count all inequivalent harmonic frames

of prime order, where two harmonic frames shall be considered equivalent if one is the unitary transformation of the other. As we shall see, this amounts to counting the number of inequivalent DFT-FUNTFs.

There has been some interest in harmonic frames in the literature, see [4, 9]. In particular, [10] presents a computer program for generating all equivalence classes of harmonic frames for a given N and d, where there is a limit on the size of either due to computational considerations. From this program, the authors conjecture that there are $\mathcal{O}(N^{d-1})$ inequivalent harmonic frames. The content of this paper is to not only validate this conjecture for the case when N is a prime number, but in fact give an exact formula for the number of harmonic frames in this case. Furthermore, we examine the structure of prime order harmonic frames via their symmetry group.

An outline of this paper is as follows: the remainder of section 1 reviews some algebraic theory and examines the problem of counting unordered DFT-FUNTFs. Section 2 defines harmonic frames and presents the main result of this paper. In section 3 we define an equivalence relation that is equivalent to (2.1) and then use this to develop a correspondence between inequivalent harmonic frames and the orbits of a particular set. Section 4 counts the number of orbits of this particular set, thus giving a formula for the number of inequivalent harmonic frames. The structure of the symmetry group is handled in section 5, and section 6 contains a few concluding remarks.

1.2. Algebra Review

Denote the additive group of integers mod N by $\mathbb{Z}_N$, and set

$$\mathbb{Z}_N^d := \underbrace{\mathbb{Z}_N \times \cdots \times \mathbb{Z}_N}_{d \text{ times}}.$$

Furthermore, let $\mathbb{Z}_N^\times$ denote the group of units of $\mathbb{Z}_N$, which, when N is prime, is simply the set $\{1, \ldots, N\}$ endowed with multiplication mod N. Finally, for $k \in \mathbb{N}$, let S_k denote the group of permutations of k elements. We will also need the following definitions and proposition:

Definition 1.1. A *group action* of a group G on a set S is a map π,

$$\begin{aligned} \pi : G \times S &\to S \\ (g, s) &\mapsto g \cdot s, \end{aligned}$$

satisfying the following properties:

1) $g_1 \cdot (g_2 \cdot s) = (g_1 g_2) \cdot s \ \ \forall \ \ g_1, g_2 \in G, \ \ s \in S,$
2) $1 \cdot s = s \ \ \forall \ \ s \in S.$

Definition 1.2. Let S be some set and let G be a group. Furthermore, let $\pi : G \times S \to S$ be a group action. For each $s \in S$ the *stabilizer* of s in G is the subgroup of G that fixes the element s:

$$G_s := \{g \in G : g \cdot s = s\}.$$

Proposition 1.3. *Let G be a group acting on the nonempty set S. The relation on S defined by:*

$$s_1 \sim s_2 \iff s_1 = g \cdot s_2 \text{ for some } g \in G$$

is an equivalence relation. For each $s \in S$, the number of elements in the equivalence class containing s is $|G : G_s|$, the index of the stabilizer of s.

Note, when G is a finite group,

$$|G : G_s| = \frac{|G|}{|G_s|}.$$

Definition 1.4. Let G be a group acting on the nonempty set S. The equivalence class $\mathcal{O}_s := \{g \cdot s : g \in G\}$ is called the *orbit* of G containing s.

As such, the orbits of a group action partition the set S. We are now ready to count the number of prime order DFT-FUNTFs, considered as unordered sets. The basic structure of the argument in subsection 1.3 will be used when we count all harmonic frames of prime order, albeit with added complexity.

1.3. The Number of Unordered DFT-FUNTFs

It is often the case that we would like to consider a frame as a set, where the order of elements does not matter. Given two ordered DFT-FUNTFs $\Phi = (\phi_0, \ldots, \phi_{N-1})$ and $\Psi = (\psi_0, \ldots, \psi_{N-1})$, we define the following equivalence relation:

$$\Phi \sim_1 \Psi \iff \exists\, \sigma \in S_N \ \ s.t.\ \ \phi_m = \psi_{\sigma(m)}, \quad \forall\ m = 0, \ldots, N-1. \tag{1.6}$$

(1.6) merely formalizes our consideration of frames as sets. An equivalence class of (1.6) will be denoted in the usual way, that is $\Phi = \{\phi_0, \ldots, \phi_{N-1}\}$. In this subsection, we count the number of DFT-FUNTFs of prime order under (1.6). First, however, we must change our perspective on the problem.

Remark 1.5. For the rest of the paper we will only consider unordered DFT-FUNTFs, and as such from now on Φ will denote $\{\phi_0, \ldots, \phi_{N-1}\}$.

1.3.1. DFT-FUNTFs and Orbits

First notice that every DFT-FUNTF contains the vector $\phi_0 = \frac{1}{\sqrt{d}}(1, \ldots, 1) \in \mathbb{C}^d$, and so when comparing two such frames we need not consider this vector. Thus we will only compare sets of the form

$$\Phi' = \Phi - \{\phi_0\}.$$

Define the set $\tilde{\mathbb{Z}}_N^d$ as

$$\tilde{\mathbb{Z}}_N^d := \{n = (n_1, \ldots, n_d) \in \mathbb{Z}_N^d : n_i \neq n_j, \ \forall \ i \neq j\}.$$

There is a one-to-one correspondence between the vectors ϕ_m, $m \neq 0$, and the elements of $\tilde{\mathbb{Z}}_N^d$. Considering $\mathbb{Z}_N^\times$ as a group and $\tilde{\mathbb{Z}}_N^d$ as a set, we define the group action π_1 as:

$$\begin{aligned} \pi_1 : \mathbb{Z}_N^\times \times \tilde{\mathbb{Z}}_N^d &\to \tilde{\mathbb{Z}}_N^d \\ (m, n) &\mapsto m \cdot n := (mn_1, \ldots, mn_d). \end{aligned}$$

The orbits of π_1 are then the sets

$$\mathcal{O}_n = \{m \cdot n = (mn_1, \ldots, mn_d) : m \in \mathbb{Z}_N^\times\}, \quad n \in \tilde{\mathbb{Z}}_N^d.$$

Remark 1.6. For clarity of exposition we shall sometimes use Φ_n to denote the DFT-FUNTF Φ and $\phi_{m,n}$ its corresponding elements, where the subscript n emphasizes the generators $n = (n_1, \ldots, n_d)$.

The following proposition relates the equivalence classes of (1.6) and the orbits of π_1.

Proposition 1.7. *There is a one-to-one correspondence between the equivalence classes of (1.6) and the orbits of π_1, i.e. the sets Φ_n and $\mathcal{O}_n$ can be identified. We denote this identification as:*

$$\Phi_n = \{\phi_0, \ldots, \phi_{N-1}\} \longleftrightarrow \mathcal{O}_n.$$

Proof. As noted above, we have:

$$\Phi \longleftrightarrow \Phi' = \Phi - \{\phi_0\}.$$

Define a function F that maps orbits of $\tilde{\mathbb{Z}}_N^d$ to sets of the form Φ' as follows:

$$F(\mathcal{O}_n) = \{\phi_{m,n}\}_{m=1}^N.$$

We must show that F is both one-to-one and onto, however it is clear that F is surjective. Considering then the former, suppose $F(\mathcal{O}_n) = F(\mathcal{O}_{n'})$. This would imply that $\{\phi_{m,n}\}_{m=1}^N = \{\phi_{m',n'}\}_{m'=1}^N$. But then for some m and some m', we would have $(mn_1, \ldots, mn_d) = (m'n_1', \ldots, m'n_d')$, i.e. $\mathcal{O}_n \cap \mathcal{O}_{n'} \neq \emptyset$, and so in fact $\mathcal{O}_n = \mathcal{O}_{n'}$. □

Remark 1.8. Given the content of proposition 1.7, we now replace the problem of counting the equivalence classes of (1.6) with the problem of counting the orbits of π_1.

1.3.2. The Number of Orbits of π_1

By proposition 1.3 we see that the orbits of a group action partition the set into disjoint equivalence classes. In particular, the orbits $\mathcal{O}_n$ partition the set $\tilde{\mathbb{Z}}_N^d$. Furthermore, the size of each $\mathcal{O}_n$ is given by $|\mathcal{O}_n| = |\mathbb{Z}_N^\times : (\mathbb{Z}_N^\times)_n|$. Using these facts, we prove the following proposition.

Proposition 1.9. *Let N be a prime number and $d \leq N$. Then the number of orbits of π_1 is:*

1) 2, *if* $d = 1$ *or* $d = N = 2$.
2) $N(N-2)\cdots(N-d+1)$, *if* $d \geq 2$, $N > 2$.

Proof. We first consider the case $d = 1$. For $n = 0$ we have $(\mathbb{Z}_N^\times)_0 = \mathbb{Z}_N^\times$, and so $|\mathcal{O}_0| = (N-1)/(N-1) = 1$. For $n \neq 0$ we see $(\mathbb{Z}_N^\times)_n = \{1\}$, and thus $|\mathcal{O}_n| = N - 1$. Since $|\tilde{\mathbb{Z}}_N^1| = N$, there are only two orbits.

Now take $2 \leq d \leq N$. For each $n \in \tilde{\mathbb{Z}}_N^d$ we have $(\mathbb{Z}_N^\times)_n = \{1\}$, and thus $|\mathcal{O}_n| = N - 1$. Therefore the number of orbits is given by x, where

$$\begin{aligned} |\tilde{\mathbb{Z}}_N^d| &= x|\mathcal{O}_n|, \\ N(N-1)\cdots(N-d+1) &= x(N-1). \end{aligned}$$

For $N = 2$ and $d = 2$, we see $x = 2$. For $N > 2$ we have $x = N(N-2)\cdots(N-d+1)$. □

As an addendum to theorem 1.9, we note that one of the orbits in the $d = 1$ case corresponds to a degenerate DFT-FUNTF. Namely, the orbit $\mathcal{O}_0$ corresponds to the DFT-FUNTF consisting of the single element $\{1\}$.

2. The Number of Harmonic Frames of Prime Order

Using a similar correspondence between harmonic frames and orbits, we count all harmonic frames of prime order up to unitary transformations. We first give some background information.

2.1. Harmonic Frames

Let $\mathbb{C}^\times$ denote the group of units of $\mathbb{C}$, that is the set $\mathbb{C}\backslash\{0\}$ endowed with multiplication.

Definition 2.1. A *character* of a group G is a group homomorphism $\xi : G \to \mathbb{C}^\times$ that satisfies

$$\xi(g_1 g_2) = \xi(g_1)\xi(g_2), \quad \forall\ g_1, g_2 \in G.$$

If G is a finite group, then $\xi(g)$ is a $|G|$-th root of unity. A finite abelian group has exactly $|G|$ characters, and considered as vectors in $\mathbb{C}^{|G|}$, it can be shown that they form an orthogonal basis for $\mathbb{C}^{|G|}$. The square matrix with these vectors as rows is referred to as the *character table* of G. In particular, when $|G| = N$ is prime, then $G \cong \mathbb{Z}_N$, and the character table of G is the un-normalized DFT matrix, D_N.

Definition 2.2. Let G be a finite abelian group of order N with characters $(\xi_j)_{j=1}^N$, $J \subseteq \{1, \ldots, N\}$, and $U : \mathbb{C}^{|J|} \to \mathbb{C}^{|J|}$ unitary. Then the frame for $\mathbb{C}^{|J|}$ given by

$$\Phi = U\{(\xi_j(g))_{j\in J} : g \in G\}$$

is called a *harmonic frame*.

Remark 2.3. When N is prime and $U = I$, the identity matrix, Φ is a DFT-FUNTF.

We will also need the following definition and theorem later on.

Definition 2.4. Let $\mathcal{U}(\mathbb{C}^d)$ denote the group of unitary transformations on $\mathbb{C}^d$. The *symmetry group* of a FUNTF Φ for $\mathbb{C}^d$ is the group:

$$\mathrm{Sym}(\Phi) := \{U \in \mathcal{U}(\mathbb{C}^d) : U\Phi = \Phi\}.$$

For clarity, we emphasize that $U\Phi = \Phi$ is a set equality.

Theorem 2.5 (Vale and Waldron [10])**.** *A FUNTF Φ of N vectors for $\mathbb{C}^d$ is harmonic if and only if it is generated by an abelian group $G \subset \mathrm{Sym}(\Phi)$ of order N, i.e., $\Phi = G\phi, \ \forall \ \phi \in \Phi$.*

2.2. The Number of Inequivalent Harmonic Frames

Two harmonic frames $\Phi = \{\phi_0, \ldots, \phi_{N-1}\} \subset \mathbb{C}^d$ and $\Psi = \{\psi_0, \ldots, \psi_{N-1}\} \subset \mathbb{C}^d$ are said to be *equivalent* if the following equivalence relation holds:

$$\Phi \sim_2 \Psi \iff \exists \ U \in \mathcal{U}(\mathbb{C}^d) \text{ s.t. } \Phi = U\Psi. \tag{2.1}$$

Once again, we emphasize that the right hand side of (2.1) is set equality. (2.1) is a standard form of equivalence in much of the literature when dealing with frames. Recently, [10] conjectured that the number of *inequivalent* harmonic frames is $O(N^{d-1})$. We prove this conjecture for N a prime number as a corollary to theorem 2.6, which gives an exact formula for the number of harmonic frames. The proof of theorem 2.6 is handled in section 4, with much preliminary work accomplished in section 3.

For a fixed N and d, we backwards recursively define the set

$$\{\alpha_c \in \mathbb{N} \cup \{0\} : c \in \mathbb{N}, c \mid N-1, \text{ and } c \mid d \text{ or } c \mid d-1\}.$$

If $c \mid N-1$, $c \mid d$, and $c > 1$, then

$$\alpha_c := \frac{(N-1-c)(N-1-2c)\cdots(N-1-(\frac{d}{c}-1)c)}{c^{\frac{d}{c}-1}(d/c)!} - \frac{c}{N-1} \sum_{\substack{c<b<N \\ c|b,\, b|d}} \binom{N-1}{b} \alpha_b, \tag{2.2 d}$$

where we have used the notation (2.2 d) to emphasize its dependence on the condition $c \mid d$. If $c \mid N-1$, $c \mid d-1$, and $c > 1$, then

$$\alpha_c := \frac{(N-1-c)(N-1-2c)\cdots(N-1-(\frac{d-1}{c}-1)c)}{c^{\frac{d-1}{c}-1}((d-1)/c)!} - \frac{c}{N-1} \sum_{\substack{c<b<N \\ c|b,\, b|d-1}} \binom{N-1}{b} \alpha_b. \tag{2.2 $d-1$}$$

Finally, α_1 is defined as:

$$\alpha_1 := \frac{1}{N-1}\binom{N}{d} - \sum_{\substack{c|d \\ c>1}} \frac{\alpha_c}{c} - \sum_{\substack{c|d-1 \\ c>1}} \frac{\alpha_c}{c}. \tag{2.3}$$

Theorem 2.6. *Let N be a prime number and let $1 < d < N$. Define the set*

$$\{\alpha_c \in \mathbb{N} \cup \{0\} : c \in \mathbb{N}, c \mid N-1, \text{ and } c \mid d \text{ or } c \mid d-1\},$$

as in equations (2.2 d), (2.2 $d-1$), and (2.3). The total number of harmonic frames for $\mathbb{C}^d$ with N elements is then given by:

$$\alpha_1 + \sum_{\substack{c|d \\ c>1}} \alpha_c + \sum_{\substack{c|d-1 \\ c>1}} \alpha_c. \tag{2.4}$$

More concisely, we have the following corollary:

Corollary 2.7. *Let N be any prime number and fix d such that $1 < d < N$. Then the number of inequivalent harmonic frames for $\mathbb{C}^d$ with N elements is $O(N^{d-1})$.*

Proof. Using equations (2.2 d) and (2.2 $d-1$), we see that $\alpha_c = O(N^s)$, where $c > 1$ and $s \leq \frac{d}{c} - 1 < d - 1$. Therefore, by (2.3), we see that $\alpha_1 = O(N^{d-1})$, and the corollary follows. □

In the above theorems, the case $d = 1$ is omitted, however, it is not hard to see that there are two inequivalent harmonic frames in this case; in fact, there is only one inequivalent harmonic frame for $d = 1$ with N distinct vectors.

3. Harmonic Frames and Orbits

In this section we develop a one-to-one correspondence between inequivalent harmonic frames and the orbits of a particular set, not unlike the ideas presented in subsection 1.3. First, however, we come up with an equivalent condition to (2.1).

We will assume N is prime for the remainder of this paper.

3.1. A New Equivalence Relation

When N is prime, every harmonic frame is of the form $U\Phi$, where $U \in \mathcal{U}(\mathbb{C}^d)$ and Φ is a DFT-FUNTF (see remark 2.3). Therefore, finding the number of inequivalent harmonic frames amounts to finding the number of inequivalent DFT-FUNTFs. Toward that end, we simplify (2.1) to the following:

Theorem 3.1. *If N is prime and $\Phi = \{\phi_0, \dots, \phi_{N-1}\}$ and $\Psi = \{\psi_0, \dots, \psi_{N-1}\}$ are DFT-FUNTFs, then*

$$\exists\ U \in \mathcal{U}(\mathbb{C}^d)\ s.t.\ \Phi = U\Psi \iff \begin{array}{c} \exists\ \sigma_1 \in S_N,\ \ \sigma_2 \in S_d\ such\ that \\ \phi_m(k) = \psi_{\sigma_1(m)}(\sigma_2(k)) \\ \forall\ m = 0, \dots, N-1,\ \ k = 1, \dots, d, \end{array} \tag{3.1}$$

where $\phi_m(k)$ denotes the k^{th} element of the vector ϕ_m.

Proof. It is clear that if the right hand side of (3.1) holds, then the left hand side must hold as well. Assume then that $\Phi = U\Psi$, and note that

$$\Phi = U\Psi \iff \phi_m = U\psi_{\sigma(m)}, \quad \forall\ m = 0, \dots, N-1, \tag{3.2}$$

for some permutation $\sigma \in S_N$. Without loss of generality, we may assume that $\sigma(0) = 0$. Indeed, let Φ_M and Ψ_M be $d \times N$ matrices whose N columns are the vectors $\phi_0, \dots, \phi_{N-1}$ and $\psi_0, \dots, \psi_{N-1}$, respectively. Combining (2.1) and (3.2), we then have:

$$\Phi \sim_2 \Psi \iff \Phi_M = U\Psi_M P_\sigma, \tag{3.3}$$

where P_σ is the $N \times N$ permutation matrix of σ. By theorem 2.5 there exists a $W \in \mathrm{Sym}(\Psi)$ such that $W\psi_0 = \psi_{\sigma(0)}$. By definition, W is a $d \times d$ matrix that permutes the columns of Ψ_M by acting on the left. Therefore, there exists an $N \times N$ permutation matrix P_W that permutes the columns of Ψ_M in the exact same manner, yet acts on the right. In particular, $W\Psi_M = \Psi_M P_W$, and thus

$$\Phi_M = UW\Psi_M P_W^{-1} P_\sigma.$$

Set $V := UW$ and $P := P_W^{-1} P_\sigma$. It is clear that V is a unitary transformation and that P is its associated permutation matrix. Furthermore, $\phi_0 = V\psi_0$, and so we can assume from the start that $\phi_0 = U\psi_0$, i.e., that $\sigma(0) = 0$.

Now let $n_1, \dots, n_d$ denote the column choices of Φ, and consider the following:

$$\langle \phi_m, \phi_0 \rangle = \sum_{k=1}^{d} e^{2\pi i m n_k / N}. \tag{3.4}$$

Letting $l_1, \dots, l_d$ denote the column choices of Ψ, we also have:

$$\langle \phi_m, \phi_0 \rangle = \langle U\psi_{\sigma(m)}, U\psi_0 \rangle = \langle \psi_{\sigma(m)}, \psi_0 \rangle = \sum_{k=1}^{d} e^{2\pi i \sigma(m) l_k / N}. \tag{3.5}$$

Define $p_\phi, p_\psi \in \mathbb{Z}[z]/\langle z^N \rangle$ as follows:

$$p_\phi(z) := \sum_{k=1}^{d} z^{mn_k} \quad \text{and} \quad p_\psi(z) := \sum_{k=1}^{d} z^{\sigma(m) l_k}. \tag{3.6}$$

By equations (3.4) and (3.5), we see that $p_\phi(z) = p_\psi(z)$ when $z = e^{2\pi i/N}$. In other words, $z = e^{2\pi i/N}$ is a root of the polynomial $p(z) := p_\phi(z) - p_\psi(z)$. However, since $p \in \mathbb{Z}[z]/\langle z^N \rangle$, and the minimum polynomial of $z = e^{2\pi i/N}$ is $q(z) := \sum_{k=0}^{N-1} z^k$, p must either be an integer multiple of q or the zero polynomial. It is clear, though, that only the latter option is feasible, thus giving

$$p_\phi(z) = p_\psi(z). \tag{3.7}$$

Combining equations (3.6) and (3.7), we see there exists a $\sigma_2 \in S_d$ such that

$$mn_k = \sigma(m) l_{\sigma_2(k)}, \quad \forall \ k = 1, \ldots, d. \tag{3.8}$$

Note that σ_2 is dependent on the choice of m. Taking $m = 1$ in (3.8), one has $n_k = \sigma(1) l_{\sigma_2(k)}$. Letting $\sigma_1(m) := \sigma(1)m$, we have:

$$\phi_m = (e^{2\pi i m n_k/N})_{k=1}^d = (e^{2\pi i \sigma_1(m) l_{\sigma_2(k)}})_{k=1}^d = \psi_{\sigma_1(m)}(\sigma_2(k)). \tag{3.9}$$

□

3.2. Inequivalent DFT-FUNTFs and Orbits

Similar to subsection 1.3.1, we now develop a one-to-one correspondence between inequivalent DFT-FUNTFs and the orbits of a particular set. As a matter of notation, we shall denote equivalence classes of (2.1) by $[\Phi]$, where $\Phi = \{\phi_0, \ldots, \phi_{N-1}\}$ is a DFT-FUNTF representative. By theorem 3.1, the equivalence classes of (2.1) are identical to the equivalence classes of the right hand side of (3.1). We now turn our attention to the set with which we will identify the equivalence classes $[\Phi]$.

Consider the following equivalence relation on the set $\tilde{\mathbb{Z}}_N^d$,

$$(n_1, \ldots, n_d) \sim (n_1', \ldots, n_d') \iff \exists \ \sigma \in S_d \ \ s.t. \ \ (n_1, \ldots, n_d) = (n'_{\sigma(1)}, \ldots, n'_{\sigma(d)}). \tag{3.10}$$

Denote an equivalence class of (3.10) by the representative $[n] = [n_1, \ldots, n_d]$, and define $\mathbb{A}_N^d$ as the set of all equivalence classes, i.e.

$$\mathbb{A}_N^d := \tilde{\mathbb{Z}}_N^d / \sim .$$

It is easy to see $|\mathbb{A}_N^d| = \binom{N}{d}$. Considering $\mathbb{Z}_N^\times$ as a group and $\mathbb{A}_N^d$ as a set, we define the group action π_2,

$$\begin{array}{rccc} \pi_2 : \mathbb{Z}_N^\times \times \mathbb{A}_N^d & \to & \mathbb{A}_N^d \\ (m, [n]) & \mapsto & m \cdot [n] := [mn_1, \ldots, mn_d]. \end{array} \tag{3.11}$$

The orbits of π_2 are the sets $\mathcal{O}_{[n]} = \{m \cdot [n] = [mn_1, \ldots, mn_d] : m \in \mathbb{Z}_N^\times\}$. The following proposition relates the equivalence classes of (2.1) and the orbits of π_2.

Proposition 3.2. *There is a one-to-one correspondence between the equivalences classes of* (2.1) *and the orbits of* π_2*, i.e.*

$$[\Phi_n] \longleftrightarrow \mathcal{O}_{[n]}.$$

Proof. Define the function F as follows:

$$F([\Phi_n]) = \mathcal{O}_{[n]} = \{[mn_1, \dots, mn_d] : m \in \mathbb{Z}_N^\times\}.$$

We must show that F is well defined, one-to-one, and onto. Surjectivity is clear, so we focus on the first two. To show F is well defined, suppose that $[\Phi_n] = [\Psi_{n'}]$. We want to show $F([\Phi_n]) = F([\Psi_{n'}])$, i.e. $\mathcal{O}_{[n]} = \mathcal{O}_{[n']}$. We have:

$$\begin{aligned}
[\Phi_n] = [\Psi_{n'}] &\iff \phi_m(k) = \psi_{\sigma_1(m)}(\sigma_2(k)) \ \ \forall \ \ k = 1, \dots, d, \ \ \forall \ \ m = 0, \dots, N-1 \\
&\iff \{\phi_0(k)_{k=1}^d, \dots, \phi_{N-1}(k)_{k=1}^d\} = \{\psi_0(\sigma_2(k))_{k=1}^d, \dots, \psi_{N-1}(\sigma_2(k))_{k=1}^d\} \\
&\iff \{\phi_1(k)_{k=1}^d, \dots, \phi_{N-1}(k)_{k=1}^d\} = \{\psi_1(\sigma_2(k))_{k=1}^d, \dots, \psi_{N-1}(\sigma_2(k))_{k=1}^d\} \\
&\iff \{(mn_1, \dots, mn_d) : m \in \mathbb{Z}_N^\times\} = \{(mn'_{\sigma_2(1)}, \dots, mn'_{\sigma_2(d)}) : m \in \mathbb{Z}_N^\times\} \\
&\iff \{[mn_1, \dots, mn_d] : m \in \mathbb{Z}_N^\times\} = \{[mn'_1, \dots, mn'_d] : m \in \mathbb{Z}_N^\times\} \\
&\iff \mathcal{O}_{[n]} = \mathcal{O}_{[n']},
\end{aligned}$$

where the first equivalence is due to theorem 3.1, and the third equivalence is because $\phi_0 = \psi_0 = \frac{1}{\sqrt{d}}(1, \dots, 1)$.

To prove injectivity, we assume $\mathcal{O}_{[n]} = \mathcal{O}_{[n']}$. According to this assumption, there must exist an $m'_0 \in \mathbb{Z}_N^\times$ such that $[n_1, \dots, n_d] = [m'_0 n'_1, \dots, m'_0 n'_d]$. Therefore we have:

$$\begin{aligned}
\mathcal{O}_{[n]} = \mathcal{O}_{[n']} &\iff [n_1, \dots, n_d] = [m'_0 n'_1, \dots, m'_0 n'_d] \\
&\iff (n_1, \dots, n_d) = (m'_0 n'_{\sigma_2(1)}, \dots, m'_0 n'_{\sigma_2(d)}) \\
&\iff (mn_1, \dots, mn_d) = (mm'_0 n'_{\sigma_2(1)}, \dots, mm'_0 n'_{\sigma_2(d)}), \ \ \forall \ \ m \in \mathbb{Z}_N^\times \\
&\iff \{(mn_1, \dots, mn_d) : m \in \mathbb{Z}_N^\times\} = \{(mn'_{\sigma_2(1)}, \dots, mn'_{\sigma_2(d)}) : m \in \mathbb{Z}_N^\times\} \\
&\iff \{\phi_1(k)_{k=1}^d, \dots, \phi_{N-1}(k)_{k=1}^d\} = \{\psi_1(\sigma_2(k))_{k=1}^d, \dots, \psi_{N-1}(\sigma_2(k))_{k=1}^d\} \\
&\iff \{\phi_0(k)_{k=1}^d, \dots, \phi_{N-1}(k)_{k=1}^d\} = \{\psi_0(\sigma_2(k))_{k=1}^d, \dots, \psi_{N-1}(\sigma_2(k))_{k=1}^d\} \\
&\iff \phi_m(k) = \psi_{\sigma_1(m)}(\sigma_2(k)), \ \ \forall \ \ k = 1, \dots, d, \ \ m = 0, \dots, N-1 \\
&\iff [\Phi_n] = [\Psi_{n'}],
\end{aligned}$$

where the fourth equivalence uses the fact that $\{mm'_0 : m \in \mathbb{Z}_N^\times\} = \{m : m \in \mathbb{Z}_N^\times\}$. ∎

To conclude this section, we note that when $d = N$, we see $|\mathbb{A}_N^d| = 1$, and so there can be only one orbit. Thus there is only one harmonic frame in this case.

4. The Number of Orbits of $\mathbb{A}_N^d$

We begin by counting the number of orbits of $\mathbb{A}_N^d$ under the group action π_2 for the cases $d = 2$ and $d = 3$. We then generalize these results for all $1 < d < N$.

4.1. Some Examples: $d = 2$ and $d = 3$

Proposition 4.1. *Let N be an odd prime number and let $d = 2$. Then there are $(N+1)/2$ orbits of $\mathbb{A}_N^2$. Therefore, there are $(N+1)/2$ inequivalent harmonic frames for $\mathbb{C}^2$.*

Proof. Let $[n] \in \mathbb{A}_N^2$. If $(\mathbb{Z}_N^\times)_{[n]} = \{1\}$, then $|\mathcal{O}_{[n]}| = N - 1$. Therefore, if we can find all $[n] \in \mathbb{A}_N^2$ with non-trivial stabilizer and their corresponding orbits, we will be able to solve for the total number of orbits. Assume that $m \cdot [n_1, n_2] = [mn_1, mn_2] = [n_1, n_2]$ for some $m \neq 1$. This implies that

$$\begin{aligned} mn_1 &\equiv n_2 \bmod N, \\ mn_2 &\equiv n_1 \bmod N. \end{aligned}$$

Combining the above equations yields

$$\begin{aligned} m^2 n_1 &\equiv n_1 \bmod N \\ \Rightarrow \quad m &\equiv \pm 1 \bmod N. \end{aligned}$$

The only valid solution is $m \equiv -1 \bmod N$, which implies $n_2 \equiv -n_1 \bmod N$. Therefore all $[n] \in \mathbb{A}_N^2$ of the form $[n] = [n_1, -n_1]$, $n_1 \neq 0$, have stabilizer $\{1, -1\}$. Furthermore, since

$$\mathcal{O}_{[1,-1]} = \{m \cdot [1, -1] = [m, -m] : m \in \mathbb{Z}_N^\times\},$$

we see that all such $[n]$ lie in the orbit $\mathcal{O}_{[1,-1]}$. Finally, these are the only elements of $\mathbb{A}_N^2$ with nontrivial stabilizer, and thus the number of orbits of $\mathbb{A}_N^2$ is $x + 1$, where x is the number of orbits of size $N - 1$. Therefore,

$$\begin{aligned} |\mathbb{A}_N^2| &= x(N-1) + |\mathcal{O}_{(1,-1)}|, \\ \binom{N}{2} &= x(N-1) + (N-1)/2, \\ N(N-1)/2 &= x(N-1) + (N-1)/2. \end{aligned}$$

Solving for x we get $x = (N-1)/2$ and so $\mathbb{A}_N^2$ has $x + 1 = (N-1)/2 + 1 = (N+1)/2$ orbits. □

Proposition 4.2. *Let N be a prime number, $N > 3$, and let $d = 3$:*

1. *If $N \equiv 1 \mod 3$, then there are $(N^2 - 2N + 7)/6$ orbits of $\mathbb{A}_N^3$.*
2. *If $N \equiv 2 \mod 3$, then there are $(N^2 - 2N + 3)/6$ orbits of $\mathbb{A}_N^3$.*

Therefore, if $N \equiv 1 \mod 3$, there are $(N^2 - 2N + 7)/6$ inequivalent harmonic frames for $\mathbb{C}^3$, and if $N \equiv 2 \mod 3$, there are $(N^2 - 2N + 3)/6$ inequivalent harmonic frames for $\mathbb{C}^3$.

Proof. As in the proof of proposition 4.1, we are looking for all $[n] \in \mathbb{A}_N^3$ with non-trivial stabilizer and their corresponding orbits. So again we suppose

$$m \cdot [n_1, n_2, n_3] = [mn_1, mn_2, mn_3] = [n_1, n_2, n_3], \tag{4.1}$$

for some $m \neq 1$. We now consider two cases:

I: Suppose $n_1 = 0$. Then we want $m \cdot [0, n_2, n_3] = [0, mn_2, mn_3] = [0, n_2, n_3]$. But this is just the same situation as the $d = 2$ case, and so the elements of $\mathbb{A}_N^3$ of this form with non-trivial stabilizer all lie in the following orbit:

$$\begin{aligned} \mathcal{O}_{[0,1,-1]} &= \{m \cdot [0, 1, -1] = [0, m, -m] : m \in \mathbb{Z}_N^\times\}, \\ |\mathcal{O}_{[0,1,-1]}| &= (N-1)/2. \end{aligned}$$

II: Suppose $n_k \neq 0$ for all $k = 1, 2, 3$. According to (4.1), we have three options for the value of mn_1:

$$mn_1 \equiv \begin{cases} n_1 \bmod N, \\ n_2 \bmod N, \\ n_3 \bmod N. \end{cases}$$

If $mn_1 \equiv n_1 \bmod N$, then $m = 1$, which is trivial and so we disregard this case. Since the order of elements does not matter in $\mathbb{A}_N^3$, there is no difference between $mn_1 \equiv n_2 \bmod N$ and $mn_1 \equiv n_3 \bmod N$, and so we choose the former. Moving on to the value of mn_2, we once again have the same three options. However, $mn_2 \equiv n_1 \bmod N$, combined with $mn_1 \equiv n_2 \bmod N$ would imply that $mn_3 \equiv n_3 \bmod N$, thus resulting in $m = 1$. $mn_2 \equiv n_2 \bmod N$ not only would imply $m = 1$, but since $mn_1 \equiv n_2 \bmod N$, would also lead to a contradiction. Therefore $mn_2 \equiv n_3 \bmod N$ must hold, which in turn forces $mn_3 \equiv n_1 \bmod N$. Summarizing, we have

$$\begin{aligned} mn_1 &\equiv n_2 \bmod N, \\ mn_2 &\equiv n_3 \bmod N, \\ mn_3 &\equiv n_1 \bmod N. \end{aligned} \tag{4.2}$$

Proceeding in a similar fashion to the proof of proposition 4.1, we see that (4.2) implies

$$m^3 n_1 \equiv n_1 \bmod N. \tag{4.3}$$

We now find all $m \in \mathbb{Z}_N^\times$ that satisfy (4.3). Let g be any primitive root mod N, i.e. $\langle g \rangle = \mathbb{Z}_N^\times$. Then all nontrivial solutions to (4.3) are of the form

$$m \equiv g^{(N-1)/3} \bmod N \quad \text{or} \quad m \equiv g^{2(N-1)/3} \bmod N. \tag{4.4}$$

We have two cases:

II.a: If 3 does not divide $N - 1$, i.e. $N \equiv 2 \bmod 3$, then the only solution to (4.3) is $m = 1$.

II.b: If 3 does divide $N-1$, i.e. $N \equiv 1 \bmod 3$, then the solution set to (4.3) is:

$$\{1, g^{(N-1)/3}, g^{2(N-1)/3} : g \text{ is a primitive root mod } N\}. \tag{4.5}$$

Therefore all elements in $\mathbb{A}_N^3$ of the form $[n_1, g^{(N-1)/3}n_1, g^{2(N-1)/3}n_1]$, $n_1 \neq 0$, have stabilizer $\{1, g^{(N-1)/3}, g^{2(N-1)/3}\}$. Furthermore, all elements of this form lie in the following orbit:

$$\mathcal{O}_{[1,g^{(N-1)/3},g^{2(N-1)/3}]} = \{[m, mg^{(N-1)/3}, mg^{2(N-1)/3}] : m \in \mathbb{Z}_N^\times\},$$

where

$$|\mathcal{O}_{[1,g^{(N-1)/3},g^{2(N-1)/3}]}| = (N-1)/3.$$

Indeed, since we have assumed that $n_1 \neq 0$, there are $N-1$ choices for n_1. However, since the order of elements in the 3-tuple does not matter, choosing n_1 is the same as choosing $g^{(N-1)/3}n_1$ or $g^{2(N-1)/3}n_1$. Therefore there are $(N-1)/3$ elements of this form, and they must all lie in the orbit $\mathcal{O}_{[1,g^{(N-1)/3},g^{2(N-1)/3}]}$. Using the same techniques as in proposition 4.1, we may now count the number of orbits (recall that x is the number of orbits of size $N-1$):

1. If $N \equiv 1 \bmod 3$, then there are $x+2$ orbits:

   $$|\mathbb{A}_N^3| = x(N-1) + (N-1)/2 + (N-1)/3.$$

   Solving for x we get $x+2 = (N^2-2N+7)/6$.
2. If $N \equiv 2 \bmod 3$, then there are $x+1$ orbits:

   $$|\mathbb{A}_N^3| = x(N-1) + (N-1)/2.$$

   Solving for x we get $x+1 = (N^2-2N+3)/6$.

□

4.2. The Structure of the Orbits of $\mathbb{A}_N^d$

We now turn our attention to the more general setting, beginning with the following theorem which addresses the order of the orbits of $\mathbb{A}_N^d$ and the form of the elements in the orbits.

Theorem 4.3. *Let N be a prime number and let $1 < d < N$. If $\mathcal{O}$ is an orbit of $\mathbb{A}_N^d$ under the group action π_2, then there exists $c \in \mathbb{N}$ such that $c \mid d$ or $c \mid d-1$, and*

$$|\mathcal{O}| = (N-1)/c. \tag{4.6}$$

Furthermore, let g be a primitive root mod N and set

$$n_k^c := [n_k, g^{(N-1)/c}n_k, \ldots, g^{(c-1)(N-1)/c}n_k], \quad n_k \neq 0. \tag{4.7}$$

If $[n] \in \mathcal{O}$, then $[n]$ can be written in the form

$$[n] = \begin{cases} [n_1^c, n_2^c, \ldots, n_{d/c}^c] & \text{if } c \mid d, \\ [0, n_1^c, n_2^c, \ldots, n_{(d-1)/c}^c] & \text{if } c \mid d-1. \end{cases} \tag{4.8 c}$$

Proof. Let $m \in \mathbb{Z}_N^\times$; we determine which elements of $\mathbb{A}_N^d$ are stabilized by m based on the order of m. In particular, we will break the argument into two cases: $|m| = c > d$ and $|m| = c \leq d$. We begin with the former.

I. Assume $|m| = c > d$.

We show that no element in $\mathbb{A}_N^d$ can be stabilized by m. Let $[n] = [n_1, \ldots, n_d] \in \mathbb{A}_N^d$, $n_j \neq 0$ for all $j = 1, \ldots, d$, and suppose

$$\begin{aligned} m \cdot [n] &= [n], \\ \implies m \cdot [n_1, \ldots, n_d] &= [n_1, \ldots, n_d], \\ \implies [mn_1, \ldots, mn_d] &= [n_1, \ldots, n_d]. \end{aligned}$$

Therefore, $mn_1 \equiv n_j \bmod N$ for some $j \in \{1, \ldots, d\}$, and because the order of $n_1, \ldots, n_d$ does not matter, without loss of generality we have two choices:

$$mn_1 \equiv \begin{cases} n_1 \bmod N, \\ n_2 \bmod N. \end{cases}$$

If $mn_1 \equiv n_1 \bmod N$, then $m = 1$ and we have a contradiction to the assumption $|m| = c > d$. Therefore, $mn_1 \equiv n_2 \bmod N$ must hold. Continuing, we see that $mn_2 \equiv n_j \bmod N$ for some $j \in \{1, \ldots, d\}$. Without loss of generality, we now have three choices:

$$mn_2 \equiv \begin{cases} n_1 \bmod N, \\ n_2 \bmod N, \\ n_3 \bmod N. \end{cases}$$

If $mn_2 \equiv n_1 \bmod N$, then, combining this with the fact that $mn_1 \equiv n_2 \bmod N$, we see that $m^2 = 1$. However, this contradicts our initial assumption, and so is eliminated from consideration. Similarly, $mn_2 \equiv n_2 \bmod N$ implies $m = 1$ and again leads to a contradiction. Therefore, $mn_2 \equiv n_3 \bmod N$ must hold. Continuing in the same manner, we see:

$$\begin{aligned} mn_1 &\equiv mn_1 &&\equiv n_2 \bmod N, \\ mn_2 &\equiv m^2 n_1 &&\equiv n_3 \bmod N, \\ mn_3 &\equiv m^3 n_1 &&\equiv n_4 \bmod N, \\ &\vdots \\ mn_{d-1} &\equiv m^{d-1} n_1 &&\equiv n_d \bmod N. \end{aligned}$$

Therefore, we must have $mn_d \equiv m^d n_1 \equiv n_1 \bmod N$, which implies $m^d = 1$. Since this contradicts our initial assumption, we see that no element $m \in \mathbb{Z}_N^\times$ with $|m| = c > d$ can stabilize an element of $\mathbb{A}_N^d$ of the form $[n_1, \ldots, n_d]$, $n_j \neq 0$ for all $j = 1, \ldots, d$. The argument for elements of the form $[0, n_1, \ldots, n_{d-1}]$, $n_j \neq 0$ for all $j = 1, \ldots, d-1$, follows similarly.

II. Assume $|m| = c \leq d$.

We show an element of $\mathbb{A}_N^d$ is stabilized by m if and only if $c \mid d$ or $c \mid d-1$. First, suppose $c \nmid d$ and $c \nmid d-1$. Therefore, there exists $q, r \in \mathbb{Z}$ such that

$$d = qc + r, \quad q \geq 0, \;\; 1 < r < c.$$

Let $[n] = [n_1, \ldots, n_d] \in \mathbb{A}_N^d$, $n_j \neq 0$ for all $j = 1, \ldots, d$, and suppose $m \cdot [n] = [n]$. Following the same argument as in part I of this proof, we see:

$$\begin{array}{rcccl} mn_1 & \equiv & mn_1 & \equiv & n_2 \bmod N, \\ mn_2 & \equiv & m^2 n_1 & \equiv & n_3 \bmod N, \\ & & \vdots & & \\ mn_{c-1} & \equiv & m^{c-1} n_1 & \equiv & n_c \bmod N, \\ mn_c & \equiv & m^c n_1 & \equiv & n_1 \bmod N, \end{array}$$

where the last line results from the fact that $|m| = c \leq d$. Continuing, we see there are two possibilities for mn_{c+1}:

$$mn_{c+1} \equiv \begin{cases} n_j \bmod N \text{ for some } j \in \{1, \ldots, c\}, \\ n_{c+2} \bmod N. \end{cases}$$

If $mn_{c+1} \equiv n_j \bmod N$ for some $j \in \{1, \ldots, c\}$, then $mn_{c+1} \equiv mn_{j-1} \bmod N$, where $n_0 := n_c \bmod N$. However, this would imply that $n_{c+1} \equiv n_{j-1} \bmod N$, a contradiction. Therefore, $mn_{c+1} \equiv mn_{c+2} \bmod N$ must hold, and we can continue with the previous line of reasoning to obtain:

$$\begin{array}{rcccl} mn_{c+1} & \equiv & mn_{c+1} & \equiv & n_{c+2} \bmod N, \\ mn_{c+2} & \equiv & m^2 n_{c+1} & \equiv & n_{c+3} \bmod N, \\ & & \vdots & & \\ mn_{2c-1} & \equiv & m^{c-1} n_{c+1} & \equiv & n_{2c} \bmod N, \\ mn_{2c} & \equiv & m^c n_{c+1} & \equiv & n_{c+1} \bmod N. \end{array}$$

Continuing with the pattern that has now been established, we arrive at:

$$\begin{array}{rcccl} mn_{qc+1} & \equiv & mn_{qc+1} & \equiv & n_{qc+2} \bmod N, \\ mn_{qc+2} & \equiv & m^2 n_{qc+1} & \equiv & n_{qc+3} \bmod N, \\ & & \vdots & & \\ mn_{qc+r-1} & \equiv & m^{r-1} n_{qc+1} & \equiv & n_{qc+r} \bmod N. \end{array}$$

We must then have:

$$mn_{qc+r} \equiv m^r n_{qc+1} \equiv n_{qc+1} \bmod N,$$

which in turn implies $m^r = 1$, a contradiction. Therefore, no element of $\mathbb{A}_N^d$ of the form $[n_1, \ldots, n_d]$, $n_j \neq 0$ for all $j = 1, \ldots, d$, can be stabilized by an $m \in \mathbb{Z}_N^\times$ with $|m| = c \leq d$ such that $c \nmid d$ and $c \nmid d-1$. The argument for elements of $\mathbb{A}_N^d$ of the form $[0, n_1, \ldots, n_{d-1}]$, $n_j \neq 0$ for all $j = 1, \ldots, d-1$, follows similarly.

We now shift our attention to $m \in \mathbb{Z}_N^\times$ such that $c \mid d$ or $c \mid d-1$. In either case there exists a $q \in \mathbb{Z}$ such that,

$$d = qc, \;\; q \geq 0, \quad \text{or} \quad d-1 = qc, \;\; q \geq 0.$$

Using the same argument that we just completed, we see that if $c \mid d$ then m stabilizes certain elements of the form $[n_1, \ldots, n_d]$, $n_j \neq 0$ for all $j = 1, \ldots, d$, whereas if $c \mid d-1$ then m stabilizes certain elements of the form $[0, n_1, \ldots, n_{d-1}]$, $n_j \neq 0$ for all $j = 1, \ldots, d-1$. The only difference in reasoning comes at the end, where in this case we do not run into a contradiction. Furthermore, looking back at the above reasoning, we see all elements $[n_1, \ldots, n_d] \in \mathbb{A}_N^d$ stabilized by m must satisfy:

$$mn_{jc+k} \equiv m^k n_{jc+1} \equiv n_{jc+k+1}, \quad \forall \;\; j = 0, \ldots, q-1, \;\; k = 1, \ldots, c-1, \quad (4.9)$$

where $d = qc$ or $d-1 = qc$, depending on the type of element of $\mathbb{A}_N^d$. By equation (4.9), any element in $\mathbb{A}_N^d$ stabilized by m can be written in one of two general forms:

$$[n] = \begin{cases} [n_1, mn_1, \ldots, m^{c-1}n_1, \ldots, n_{\frac{d}{c}}, mn_{\frac{d}{c}}, \ldots, m^{c-1}n_{\frac{d}{c}}] \\ [0, n_1, mn_1, \ldots, m^{c-1}n_1, \ldots, n_{\frac{d-1}{c}}, mn_{\frac{d-1}{c}}, \ldots, m^{c-1}n_{\frac{d-1}{c}}], \end{cases} \quad (4.10)$$

where $n_j \neq 0$ and $n_j \neq n_k$ for all $j, k = 1, \ldots, d/c$ or $j, k = 1, \ldots, (d-1)/c$, depending on the form of $[n]$. Also, since $|m| = c$, there must exist a primitive root mod N, g, such that

$$m = g^{(N-1)/c}, \quad (4.11)$$

noting that $c \mid N-1$ since the order of any group element must divide the order of the group. Combining equations (4.10) and (4.11) gives (4.8 c).

In order to prove (4.6), we exploit the fact that

$$|\mathcal{O}_{[n]}| = \frac{N-1}{|(\mathbb{Z}_N^\times)_{[n]}|}. \quad (4.12)$$

By (4.12), we need only compute the stabilizer of $[n]$ in $\mathbb{Z}_N^\times$, that is $(\mathbb{Z}_N^\times)_{[n]}$. But (4.10) and (4.11) easily give

$$(\mathbb{Z}_N^\times)_{[n]} = \{g^{l(N-1)/c} : l = 0, \ldots, c-1\}.$$

Clearly $|(\mathbb{Z}_N^\times)_{[n]}| = c$, thus proving (4.6). □

Before counting the number of orbits $\mathbb{A}_N^d$, we prove two lemmas that simplify this task. The first shows that the choice of g in (4.7) does not matter.

Lemma 4.4. *If g_1 and g_2 are two primitive roots mod N, and $n_1 \in \mathbb{Z}_N$, $n_1 \neq 0$, then*

$$[n_1, g_1^{(N-1)/c} n_1, \ldots, g_1^{(c-1)(N-1)/c} n_1] = [n_1, g_2^{(N-1)/c} n_1, \ldots, g_2^{(c-1)(N-1)/c} n_1].$$

Proof. Since g_1 and g_2 are both primitive roots mod N, the sets $\{1, g_1^{(N-1)/c}, \ldots, g_1^{(c-1)(N-1)/c}\}$ and $\{1, g_2^{(N-1)/c}, \ldots, g_2^{(c-1)(N-1)/c}\}$ are both complete solution sets to $x^c \equiv 1 \bmod N$. Therefore $(n_1, g_2^{(N-1)/c} n_1, \ldots, g_2^{(c-1)(N-1)/c} n_1)$ is a rearrangement of $(n_1, g_1^{(N-1)/c} n_1, \ldots, g_1^{(c-1)(N-1)/c} n_1)$, and the lemma follows. □

The second lemma shows that the representation given by (4.8 *c*) is not unique and gives the instances where confusion can occur.

Lemma 4.5. *Let $[n] \in \mathbb{A}_N^d$ such that $[n]$ can be written in the form (4.8 b). If $c \mid b$, then $[n]$ can be written in the form (4.8 c) as well.*

Proof. We assume $[n] = [\tilde{n}_1^b, \tilde{n}_2^b, \ldots, \tilde{n}_{d/b}^b]$ and show that we can rewrite this as $[n] = [n_1^c, n_2^c, \ldots, n_{d/c}^c]$. If $[n] = [0, \tilde{n}_1^b, \tilde{n}_2^b, \ldots, \tilde{n}_{(d-1)/b}^b]$ then a similar proof shows how to rewrite this as $[n] = [0, n_1^c, n_2^c, \ldots, n_{(d-1)/c}^c]$. Recall

$$\tilde{n}_k^b = [\tilde{n}_k, g^{(N-1)/b}\tilde{n}_k, \ldots, g^{(b-1)(N-1)/b}\tilde{n}_k].$$

Let $a = b/c$ and set $n_1 = \tilde{n}_1$; we want to construct n_1^c out of elements of $\tilde{n}_1^b$, where:

$$\tilde{n}_1^b = [\tilde{n}_1, g^{(N-1)/b}\tilde{n}_1, \ldots, g^{(b-1)(N-1)/b}\tilde{n}_1^b].$$

Since the order of elements does not matter, we may pick them however we like and rearrange them as we wish. We have that n_1^c is formed out of the following elements of $\tilde{n}_1^b$:

$$\begin{aligned} n_1^c &= [\tilde{n}_1, g^{a(N-1)/b}\tilde{n}_1, \ldots, g^{(c-1)a(N-1)/b}\tilde{n}_1] \\ &= [n_1, g^{a(N-1)/b} n_1, \ldots, g^{(c-1)a(N-1)/b} n_1] \\ &= [n_1, g^{a(N-1)/ca} n_1, \ldots, g^{(c-1)a(N-1)/ca} n_1] \\ &= [n_1, g^{(N-1)/c} n_1, \ldots, g^{(c-1)(N-1)/c} n_1]. \end{aligned}$$

Likewise, set $n_k = \tilde{n}_k$ for $k = 2, \ldots, d/b$, and construct n_k^c in a similar manner. For the next c-tuple, set $n_{\frac{d}{b}+1} = g^{(N-1)/b}\tilde{n}_1$. We then have:

$$\begin{aligned} n_{\frac{d}{b}+1}^c &= [g^{(N-1)/b}\tilde{n}_1, g^{(a+1)(N-1)/b}\tilde{n}_1, \ldots, g^{((c-1)a+1)(N-1)/b}\tilde{n}_1] \\ &= [n_{\frac{d}{b}+1}, g^{a(N-1)/b} n_{\frac{d}{b}+1}, \ldots, g^{(c-1)a(N-1)/b} n_{\frac{d}{b}+1}] \\ &= [n_{\frac{d}{b}+1}, g^{(N-1)/c} n_{\frac{d}{b}+1}, \ldots, g^{(c-1)(N-1)/c} n_{\frac{d}{b}+1}]. \end{aligned}$$

In general,

$$n_{\frac{jd}{b}+k} = g^{j(N-1)/b}\tilde{n}_k, \quad \forall\ j = 0, \ldots, a-1,\ \ k = 1, \ldots, d/b,$$

and the resulting $n_{\frac{jd}{b}+k}^c$ follows similarly. □

4.3. Proof of Theorem 2.6

Using theorem 4.3 as well as lemmas 4.4 and 4.5, we now count the number of orbits of $\mathbb{A}_N^d$. By proposition 3.2 this is the same as counting the number of inequivalent harmonic frames, and so will complete the proof of theorem 2.6. Let γ_c denote the total number of orbits of $\mathbb{A}_N^d$ with $(N-1)/c$ elements. Then, by theorem 4.3, the total number of orbits of $\mathbb{A}_N^d$ is given by

$$\gamma_1 + \sum_{\substack{c|d \\ c>1}} \gamma_c + \sum_{\substack{c|d-1 \\ c>1}} \gamma_c. \tag{4.13}$$

Notice the similarity between equations (4.13) and (2.4). In fact, we shall prove that

$$\gamma_c = \alpha_c, \quad \forall\ c \in \mathbb{N} \text{ such that } c \mid N-1 \text{ and } c \mid d \text{ or } c \mid d-1.$$

Theorem 4.6. *Let N be a prime number, $1 < d < N$, $c \mid N-1$, $c > 1$, and let β_c denote the cumulative order of all orbits of size $(N-1)/c$. Furthermore, let γ_c denote the number of orbits of $\mathbb{A}_N^d$ of size $(N-1)/c$, so that*

$$\gamma_c = \frac{c\beta_c}{N-1}.$$

If $c \mid d$, then β_c is given by the following backwards recursive formula:

$$\beta_c = \frac{(N-1)(N-1-c)\cdots(N-1-(\frac{d}{c}-1)c)}{c^{\frac{d}{c}}(d/c)!} - \sum_{\substack{c<b<N \\ c|b,\, b|d}} \beta_b.$$

If $c \mid d-1$, then β_c is given by the following backwards recursive formula:

$$\beta_c = \frac{(N-1)(N-1-c)\cdots(N-1-(\frac{d-1}{c}-1)c)}{c^{\frac{d-1}{c}}((d-1)/c)!} - \sum_{\substack{c<b<N \\ c|b,\, b|d-1}} \beta_b.$$

The number of orbits of $\mathbb{A}_N^d$ of size $N-1$, denoted γ_1, is given by:

$$\gamma_1 = \frac{1}{N-1}\binom{N}{d} - \sum_{\substack{c|d \\ c>1}} \frac{\gamma_c}{c} - \sum_{\substack{c|d-1 \\ c>1}} \frac{\gamma_c}{c}.$$

Proof. We prove the formula for β_c when $c \mid d$, noting that the proof is identical for the case when $c \mid d-1$. In order to accomplish this task, we will build up the formula using combinatorial arguments. By theorem 4.3, the elements we are counting are of the form $[n_1^c, n_2^c, \ldots, n_{d/c}^c]$, where

$$n_k^c = [n_k, g^{(N-1)/c} n_k, \ldots, g^{(c-1)(N-1)/c} n_k], \quad n_k \neq 0.$$

It is clear then, that we have $N-1$ choices for n_1, $N-1-c$ choices for n_2, $N-1-2c$ choices for n_3, and so on. Continuing to the end, we see there are

$N-1-(d/c-1)c$ choices for $n_{d/c}$. Furthermore, by lemma 4.4, the choice of g does not matter, and so does not add any new elements to count. Therefore, at the moment, we have

$$(N-1)(N-1-c)\cdots(N-1-(d/c-1)c)$$

elements. Fixing the choice of n_1 temporarily, it is clear that if we chose any of $g^{(N-1)/c}n_1, \ldots, g^{(c-1)(N-1)/c}n_1$ instead of n_1, then we would have a rearranged version of n_1^c. However, the order of elements does not matter in $\mathbb{A}_N^d$, and so these choices are in fact the same as choosing n_1. Since there are c such elements (including n_1), the number of distinct choices for n_1 is in fact $(N-1)/c$. Similarly, we must divide the number of choices for each n_k by a factor of c, thus giving

$$\frac{(N-1)(N-1-c)\cdots(N-1-(d/c-1)c)}{c^{d/c}}$$

elements. Furthermore, again recalling that the order of elements does not matter, we see that the order in which we choose $n_1, \ldots, n_{d/c}$ does not matter either. Consequently, we are now down to

$$\frac{(N-1)(N-1-c)\cdots(N-1-(d/c-1)c)}{c^{d/c}(d/c)!} \tag{4.14}$$

elements. We note that equation (4.14) gives the number of elements of the form (4.8 c). However, we are not counting all elements of the form (4.8 c), but only those that are in an orbit of size $(N-1)/c$. In fact, by lemma 4.5 any element in an orbit of size $(N-1)/b$, where $c \mid b$ and $b \mid d$, can be rewritten as $[n_1^c, n_2^c, \ldots, n_{d/c}^c]$. Therefore, we must subtract all elements in orbits of size $(N-1)/b$, where $c \mid b$ and $b \mid d$, thus giving:

$$\beta_c = \frac{(N-1)(N-1-c)\cdots(N-1-(\frac{d}{c}-1)c)}{c^{\frac{d}{c}}(d/c)!} - \sum_{\substack{c<b<N \\ c|b,\, b|d}} \beta_b.$$

The equation for γ_1 follows from

$$|\mathbb{A}_N^d| = \gamma_1(N-1) + \sum_{\substack{c|d \\ c>1}} \left(\frac{N-1}{c}\right)\gamma_c + \sum_{\substack{c|d-1 \\ c>1}} \left(\frac{N-1}{c}\right)\gamma_c,$$

and the fact that $|\mathbb{A}_N^d| = \binom{N}{d}$. □

Example 4.7. We apply theorem 4.6 for the case when $d = 3$ and $N \equiv 1 \bmod 3$. In this case, $c = 3$ divides d as well as $N-1$, while $c = 2$ divides $d-1$ as well as $N-1$. Therefore we compute:

$$\beta_3 = \frac{N-1}{3} \quad \text{and} \quad \beta_2 = \frac{N-1}{2},$$

which in turn gives:

$$\gamma_3 = 1 \quad \text{and} \quad \gamma_2 = 1.$$

Thus,

$$\begin{aligned} \gamma_1 &= \frac{1}{N-1}\binom{N}{3} - \frac{1}{3} - \frac{1}{2} \\ &= \frac{N^2-2N}{6} - \frac{2}{6} - \frac{3}{6} \\ &= \frac{N^2-2N-5}{6}, \end{aligned}$$

and so the total number of orbits is:

$$\begin{aligned} \gamma_1+\gamma_2+\gamma_3 &= \frac{N^2-2N-5}{6} + 1 + 1 \\ &= \frac{N^2-2N+7}{6}. \end{aligned}$$

Notice this is the same result as proposition 4.2.

5. The Symmetry Group

We now turn our attention to the symmetry group of prime order harmonic frames. The following theorem proves the existence of a particular subgroup of $\mathrm{Sym}(\Phi_n)$ that is dependent on the generators $n_1, \ldots, n_d$ as well as the order of $\mathcal{O}_{[n]}$.

Theorem 5.1. *Let $\mathcal{O}_{[n]}$ be an orbit of $\mathbb{A}_N^d$ such that $|\mathcal{O}_{[n]}| = (N-1)/c$, and let Φ_n be the harmonic frame that corresponds to $\mathcal{O}_{[n]}$ under the one-to-one correspondence described by proposition 3.2. Then*

$$\langle \mathrm{diag}(\omega^{n_1}, \ldots, \omega^{n_d}), Q \rangle \subseteq \mathrm{Sym}(\Phi_n),$$

where $\mathrm{diag}(\omega^{n_1}, \ldots, \omega^{n_d})$ *denotes a $d \times d$ matrix with $\omega^{n_1}, \ldots, \omega^{n_d}$ on the diagonal and zeros elsewhere, $\omega = e^{2\pi i/N}$, Q is a $d \times d$ permutation matrix dependent on Φ_n, and $|\langle Q \rangle| = c$.*

Proof. Similar to the proof of theorem 3.1, let Φ_M denote the $d \times N$ matrix whose columns are the elements of Φ_n. We note that $U \in \mathrm{Sym}(\Phi_n)$ if and only if there exists an $N \times N$ permutation matrix P such that

$$U\Phi_M = \Phi_M P. \tag{5.1}$$

First using the left hand side of (5.1), we have

$$(U\Phi_M)^\star (U\Phi_M) = \Phi_M^\star U^\star U \Phi_M = \Phi_M^\star \Phi_M, \tag{5.2}$$

and then equivalently for the right hand side of (5.1),

$$(\Phi_M P)^\star (\Phi_M P) = P^\star \Phi_M^\star \Phi_M P. \tag{5.3}$$

Combining (5.2) and (5.3) we obtain the following necessary condition for (5.1),

$$\Phi_M^\star \Phi_M = P^\star \Phi_M^\star \Phi_M P,$$

or equivalently,

$$P\Phi_M^\star \Phi_M P^\star = \Phi_M^\star \Phi_M. \tag{5.4}$$

The matrix $\Phi_M^\star \Phi_M$ is called the Gram matrix and has the following form:

$$(\Phi_M^\star \Phi_M)_{j,k} = \langle \phi_k, \phi_j \rangle = \sum_{l=1}^{d} e^{2\pi i n_l (k-j)/N}, \quad \forall\ j,k = 0,\dots,N-1. \tag{5.5}$$

Two elements $\langle \phi_k, \phi_j \rangle$ and $\langle \phi_{k'}, \phi_{j'} \rangle$ of $\Phi_M^\star \Phi_M$ are equal if and only if

$$\sum_{l=1}^{d} e^{2\pi i n_l (k-j)/N} = \sum_{l=1}^{d} e^{2\pi i n_l (k'-j')/N}. \tag{5.6}$$

Using the same minimum polynomial argument as the one found in the proof of theorem 3.1, we see that (5.6) holds for off diagonal elements of $\Phi_M^\star \Phi_M$ if and only if there exists a permutation $\mu \in S_d$ such that

$$n_l(k-j) \equiv n_{\mu(l)}(k'-j') \bmod N, \quad \forall\ l = 1,\dots,d,\ \ k \neq j,\ \ k' \neq j'. \tag{5.7}$$

(5.7) is in fact the same condition as (3.10), and so we may define the following equivalence relation between the off diagonal entries of $\Phi_M^\star \Phi_M$ and the elements of $\mathbb{A}_N^d$:

$$\langle \phi_k, \phi_j \rangle \sim (k-j \bmod N) \cdot [n], \quad k \neq j. \tag{5.8}$$

For the diagonal entries of $\Phi_M^\star \Phi_M$, we define the representative $[0]$ as

$$[0] := [\underbrace{0,\dots,0}_{d}],$$

and extend our equivalence relation to diagonal elements:

$$\langle \phi_j, \phi_j \rangle \sim [0]. \tag{5.9}$$

In order to ease notation, we set $0 \cdot [n] := [0]$, and thus can write $k \cdot [n]$ for all $k \in \mathbb{Z}_N$. Combining (5.8) and (5.9), we see $\sim$ induces an equivalence relation between the set of inner products, $\{\langle \phi_j, \phi_k \rangle : j,k = 0,\dots,N-1\}$, and the set $\mathbb{A}_N^d \cup \{[0]\}$. Defining the matrix G as

$$G_{j,k} := (k-j) \cdot [n], \quad \forall\ j,k \in \mathbb{Z}_N \tag{5.10}$$

we then have an equivalence relation between $\Phi_M^\star \Phi_M$ and G:

$$\Phi_M^\star \Phi_M \sim G. \tag{5.11}$$

Combining (5.4) with (5.11) gives the following necessary condition for (5.1) to hold:

$$PGP^\star = G. \tag{5.12}$$

Returning to (5.10), we see G has the form:

$$G = \begin{pmatrix} a_0 & a_{N-1} & a_{N-2} & \cdots & a_2 & a_1 \\ a_1 & a_0 & a_{N-1} & a_{N-2} & \cdots & a_2 \\ a_2 & a_1 & a_0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & a_{N-1} & a_{N-2} \\ a_{N-2} & \cdots & a_2 & a_1 & a_0 & a_{N-1} \\ a_{N-1} & a_{N-2} & \cdots & a_2 & a_1 & a_0 \end{pmatrix}, \tag{5.13}$$

where $a_k = k \cdot [n]$ for all $k \in \mathbb{Z}_N$. Therefore G is a circulant matrix, and is completely determined by its first column vector. The permutation matrix

$$C := \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{5.14}$$

is called the basic circulant permutation matrix. A matrix A can be written in the form

$$A = \sum_{k=0}^{N-1} a_k C^k, \tag{5.15}$$

if and only if A is circulant. Therefore, G can be written in the form (5.15), and as such, it is clear that

$$C^k G (C^k)^\star = G, \quad \forall \ k = 0, \ldots, N-1.$$

A simple computation shows that when $U = \mathrm{diag}(\omega^{n_1}, \ldots, \omega^{n_d})$, one has

$$U^k \Phi_M = \Phi_M C^k, \quad \forall \ k = 0, \ldots, N-1.$$

Thus, regardless of the size $\mathcal{O}_{[n]}$,

$$\mathrm{diag}(\omega^{kn_1}, \ldots, \omega^{kn_d}) \in \mathrm{Sym}(\Phi_n), \quad \forall \ k = 0, \ldots, N-1.$$

Note this proves the theorem for the case $|\mathcal{O}_{[n]}| = N - 1$.

To prove the existence of the matrix $Q \in \mathrm{Sym}(\Phi_n)$ with $|\langle Q \rangle| = c$, suppose that Φ_n corresponds to $\mathcal{O}_{[n]}$ such that $|\mathcal{O}_{[n]}| = (N-1)/c$, where $c > 1$. Note that by theorem 4.3 we have

$$g^{k(N-1)/c} m \cdot [n] = m \cdot [n], \quad \forall \ m \in \mathbb{Z}_N^\times, \ \ k = 1, \ldots, c,$$

and in particular

$$g^{k(N-1)/c} \cdot [n] = [n], \quad \forall \ k = 1, \ldots, c.$$

Therefore, the action of $g^{(N-1)/c}$ on n defines a permutation $\rho \in S_d$ such that

$$(n_{\rho^k(1)}, \ldots, n_{\rho^k(d)}) = g^{k(N-1)/c} \cdot (n_1, \ldots, n_d), \quad \forall \ k = 1, \ldots, c. \tag{5.16}$$

Since a permutation of the generators $n_1, \ldots, n_d$ is equivalent to a permutation of the rows of Φ_M, (5.16) implies the existence of a $d \times d$ permutation matrix Q, where Q is the matrix equivalent of ρ, as well as an $N \times N$ permutation matrix P_0, such that

$$Q^k \Phi_M = \Phi_M P_0^k, \quad \forall \ k = 1, \ldots, c.$$

In other words, $Q \in \mathrm{Sym}(\Phi_n)$, and since $\mathrm{diag}(\omega^{n_1}, \ldots, \omega^{n_d}) \in \mathrm{Sym}(\Phi_n)$ as well, we must have

$$\langle \mathrm{diag}(\omega^{n_1}, \ldots, \omega^{n_d}), Q \rangle \subseteq \mathrm{Sym}(\Phi_n).$$

□

Corollary 5.2. *Let $\mathcal{O}_{[n]}$ be an orbit of $\mathbb{A}_N^d$ such that $|\mathcal{O}_{[n]}| = N - 1$, and let Φ_n be the harmonic frame that corresponds to $\mathcal{O}_{[n]}$ under the one-to-one correspondence described by proposition 3.2. Then*

$$\mathrm{Sym}(\Phi_n) = \langle \mathrm{diag}(\omega^{n_1}, \ldots, \omega^{n_d}) \rangle,$$

where $\mathrm{diag}(\omega^{n_1}, \ldots, \omega^{n_d})$ denotes a $d \times d$ matrix with $\omega^{n_1}, \ldots, \omega^{n_d}$ on the diagonal and zeros elsewhere, and $\omega = e^{2\pi i/N}$.

Proof. Recall the matrices G and C from the proof of theorem 5.1, as given by equations (5.10) and (5.14), respectively. We will show that $P = C^k$, $k = 0, \ldots, N-1$, are the only matrices satisfying the necessary condition given by equation (5.12). Combining the fact that $\mathcal{O}_{[n]} = \{m \cdot [n] : m \in \mathbb{Z}_N^\times\}$ with the assumption that $|\mathcal{O}_{[n]}| = N - 1$, we have

$$k \cdot [n] = k' \cdot [n] \iff k \equiv k' \bmod N. \tag{5.17}$$

Furthermore, let $\sigma \in S_N$ be the permutation corresponding to the permutation matrix P. Equation (5.12) can be rewritten as

$$(\sigma(j) - \sigma(k)) \cdot [n] = (j - k) \cdot [n], \quad \forall \ j, k \in \mathbb{Z}_N. \tag{5.18}$$

Combining equations (5.17) and (5.18), one obtains

$$\sigma(j) - \sigma(k) = j - k, \quad \forall \ j, k \in \mathbb{Z}_N. \tag{5.19}$$

One can think of (5.19) as a system of N^2 linear equations in the N variables $\sigma(0), \ldots, \sigma(N-1)$, with the two added constraints:

1. $\sigma(k) \in \mathbb{Z}_N$ for all $k \in \mathbb{Z}_N$,

2. $\sigma(j) = \sigma(k)$ if and only if $j = k$.

Clearly (5.19) is an overdetermined system. However, (5.19) has $N-1$ independent equations, given by:

$$\begin{aligned} \sigma(1) - \sigma(0) &\equiv 1 \bmod N \\ \sigma(2) - \sigma(0) &\equiv 2 \bmod N \\ &\vdots \\ \sigma(N-1) - \sigma(0) &\equiv N-1 \bmod N. \end{aligned}$$

Thus $\sigma(0)$ is a free variable, and can be assigned any value from $\mathbb{Z}_N$. The remaining values of σ are then given by:

$$\sigma(j) \equiv j + \sigma(0) \bmod N, \quad \forall\ j = 1, \ldots, N-1.$$

In conclusion, there are N possible permutations, each corresponding to a different value of $\sigma(0)$. In particular, we have the following correspondence:

$$\sigma(0) = k \iff P = C^k.$$

□

The following conjecture asserts that the subgroup described in theorem 5.1 in fact is the symmetry group for all prime order harmonic frames, not just those corresponding to orbits of size $N-1$.

Conjecture 5.3. *Let $\mathcal{O}_{[n]}$ be an orbit of $\mathbb{A}_N^d$ such that $|\mathcal{O}_{[n]}| = (N-1)/c$, and let Φ_n be the harmonic frame that corresponds to $\mathcal{O}_{[n]}$ under the one-to-one correspondence described by proposition 3.2. Then*

$$\mathrm{Sym}(\Phi_n) = \langle \mathrm{diag}(\omega^{n_1}, \ldots, \omega^{n_d}), Q \rangle,$$

where $\mathrm{diag}(\omega^{n_1}, \ldots, \omega^{n_d})$ *denotes a $d \times d$ matrix with $\omega^{n_1}, \ldots, \omega^{n_d}$ on the diagonal and zeros elsewhere, $\omega = e^{2\pi i/N}$, Q is a $d \times d$ permutation matrix dependent on Φ_n, and $|\langle Q \rangle| = c$.*

6. Closing remarks

We have enumerated all harmonic frames for $\mathbb{C}^d$ with N elements, where N is a prime number. A natural question is how to extend these results to all N. Certain problems arise, however, with the techniques used in this paper, since in several instances the fact that N is prime is a key element. In particular, for a general N, distinct harmonic frames will arise from groups other than $\mathbb{Z}_N$. Also, even for those harmonic frames that do come from $\mathbb{Z}_N$, new representations must be developed since in general $\mathbb{Z}_N^\times \subseteq \{1, \ldots, N\}$.

7. Acknowledgements

I would like to thank John Benedetto for introducing me to this problem, as well as Kasso Okoudjou for numerous helpful discussions on this topic.

References

[1] John J. Benedetto and Matt Fickus. Finite normalized tight frames. *Adv. Comput. Math.*, 18:357–385, 2003.

[2] Peter Casazza and Jelena Kovacevic. Equal-norm tight frames with erasures. *Adv. Comput. Math.*, 18(2–4):387–430, 2003.

[3] David Dummit and Richard Foote. *Abstract Algebra*. John Wiley and Sons, Inc., 3rd edition, 2004.

[4] Yonina C. Eldar and Helmut Bolcskei. Geometrically uniform frames. *IEEE Trans. Inform. Theory*, 49(4):993–1006, 2003.

[5] Vivek Goyal, Jelena Kovacevic, and Jonathan Kelner. Quantized frame expansions with erasures. *Journ. of Appl. and Comput. Harmonic Analysis*, 10(3):203–233, 2001.

[6] Jelena Kovacevic and Amina Chebira. Life beyond bases: The advent of frames (part I). *IEEE SP Mag.*, 24(4):86–104, July 2007. Feature article.

[7] Jelena Kovacevic and Amina Chebira. Life beyond bases: The advent of frames (part II). *IEEE SP Mag.*, 24(5):115–125, September 2007. Feature article.

[8] Robert Reams and Shayne Waldron. Isometric tight frames. *Electron. J. Linear Algebra*, 9:122–128, 2002.

[9] Richard Vale and Shayne Waldron. Tight frames and their symmetries. *Const. Approx.*, 21(1):83–112, 2005.

[10] Shayne Waldron and Nick Hay. On computing all harmonic frames of n vectors in $\mathbb{C}^d$. *Appl. Comput. Harmon. Anal.*, 21:168–181, 2006.

[11] Georg Zimmermann. Normalized tight frames in finite dimensions. In W. Haussmann, K. Jetter, and M. Reimer, editors, *Recent Progress in Multivariate Approximation*, pages 249–252. Internat. Ser. Numer. Math., 2001.