BINARY PARSEVAL FRAMES FROM GROUP ORBITS

ROBERT P. MENDEZ, BERNHARD G. BODMANN, ZACHERY J. BAKER, MICAH G. BULLOCK, AND JACOB E. MCLANEY

Abstract. Binary Parseval frames share many structural properties with real and complex ones. On the other hand, there are subtle differences, for example that the Gramian of a binary Parseval frame is characterized as a symmetric idempotent whose range contains at least one odd vector. Here, we study binary Parseval frames obtained from the orbit of a vector under a group representation, in short, binary Parseval group frames. In this case, the Gramian of the frame is in the algebra generated by the right regular representation. We identify equivalence classes of such Parseval frames with binary functions on the group that satisfy a convolution identity. This allows us to find structural constraints for such frames. We use these constraints to catalogue equivalence classes of binary Parseval frames obtained from group representations. As an application, we study the performance of binary Parseval frames generated with abelian groups for purposes of error correction. We show that if p is an odd prime, then the group $\mathbb{Z}_p^q$ is always preferable to $\mathbb{Z}_{p^q}$ when searching for best performing codes associated with binary Parseval group frames.

1. Introduction

A binary frame is, in short, a finite, spanning family in a vector space over the Galois field with two elements. Binary frames share many properties with finite real or complex frames, which have been studied extensively in mathematics and engineering [16, 17, 6]. Because of the spanning property, frames can serve to expand any given vector in a linear combination of the frame vectors. In contrast to bases of a vector space, the frame vectors can include linear dependencies. If this is the case, then the expansion of a vector is no longer uniquely determined. However, for Parseval frames, there is a standard choice of coefficients appearing in the expansion of a vector that can be calculated efficiently. When the appropriate definition of a Parseval frame is made, then this holds in the binary as well as the real and complex setting [5]. In the case of real or complex frames, the expansion coefficients are computed by taking inner products with the frame vectors. The same property for binary frames requires replacing the inner product with the less restrictive concept of a bilinear form [14], which can be taken to be the standard dot product.

Equivalence classes are useful to classify frames and to study essential properties. In the real or complex case, a number of equivalence relations have been used, ranging from similarity for frames to unitary equivalence [11], projective unitary equivalence [8], and switching equivalence [10, 4] for Parseval frames. As for real and complex frames, each set of unitarily equivalent binary Parseval frames can be identified with a corresponding Gramian [5, Proposition 4.8]. Even with this reduction up to unitary equivalence, the number of (inequivalent) binary Parseval frames appears to grow quickly as the dimension of the vector space and the number of frame vectors increase, see exhaustive lists for lowest dimensions in [5] and [1].

Next to similarities, binary frames exhibit differences with the theory of real and complex frames. One of the more striking ways in which they differ is when considering the Gram matrices. The Gram matrices of real or complex Parseval frames are characterized as symmetric or Hermitian idempotent matrices. In the binary case, these properties have to be augmented with the condition

Key words and phrases. Binary Parseval frames, group representation, group algebra, binary codes; MSC (2010): 42C15, 15A33, 94B05.

The research in this paper was partially supported by NSF grants DMS-1412524 and DMS-1715735.

of at least one non-zero diagonal entry of the Gram matrix [1]. Equivalently, one of its column vectors must be odd, meaning it contains an odd number of 1's. The underlying reason is the range of the Gram matrix of a Parseval frame consists precisely of its eigenspace corresponding to eigenvalue one, which necessarily contains only odd vectors. If none of the column vectors were odd, then the span could not satisfy this requirement.

In this paper, we continue comparing the structure of binary Parseval frames with their real or complex counterparts. We specialize to frames obtained from the orbit of a vector under a group representation. There is already a substantial amount of literature on real and complex group frames [11, 27, 12, 28, 7, 29]. Here, we study binary Parseval group frames, with special emphasis on the structure of the Gramians associated with them. Our first main result is that a binary Parseval frame is obtained from the action of a group if and only if its Gramian is in the group algebra.

For such group frames, the Gram matrix is shown to be a binary linear combination of elements of the right regular representation, thus associated with a binary function on the group. This function provides a concise characterization of binary Parseval group frames, allowing us to find structural constraints for such frames. We use these constraints to catalogue coarser equivalence classes of binary Parseval frames obtained from group representations. We specialize further to abelian groups and deduce more specific design constraints.

The results on the structure of binary Parseval frames have significance for the design of error-correcting codes [19]. There has already been a number of works on real or complex frames as codes [20, 21, 10, 24, 25, 13, 4, 15]. We continue efforts of an earlier paper [2] to develop results on binary codes from a frame-theoretic perspective. In that paper, methods from graph theory produced results for the design of such codes. Here, we show that when a frame is obtained from the orbit of a vector under a group action, then the choice of the group can have a significant impact on the coding performance of the resulting frame: Each binary Parseval $\mathbb{Z}_{p^q}$-frame is switching equivalent to a $\mathbb{Z}_p^q$-frame. Thus, when searching for best performers, the group $\mathbb{Z}_p^q$ is a better choice. We investigate group representations of $\mathbb{Z}_p^q$ and $\mathbb{Z}_{p^q}$ for small values of p and q and explicitly determine the best performance for $p = q = 3$ and $p = 5$, $q = 3$.

We leave the study and applications of non-abelian groups and their associated binary group frames for future work. In addition, one may use finite fields other than the Galois field with two elements. Here, the motivation for code design was a natural reason to restrict the discussion to binary numbers.

This paper is organized as follows:

Throughout Section 2, we introduce the relevant definitions of binary group frames, accompanied by illustrating examples. Fundamental to the theory of real and complex frames is the fact that every group representation that generates a Parseval group frame is unitary. Section 2 concludes with the corresponding binary result, along with an explicit formulation of such representations in terms of the frame vectors and the group algebra.

Section 3 is dedicated to the properties of the Gramians of binary Parseval group frames. Corollary 3.3 summarizes our first main result, that a binary Parseval frame is a group frame if and only if the Gramian is in the group algebra. We follow this with Theorem 3.4, a characterization of the Gramians of binary Parseval group frames in terms of properties of the Gram matrices. This provides the foundation for a characterization of such Gramians in terms of binary functions on the group, Theorem 3.9. We devote the remainder of Section 3 to developing design constraints specific to binary Parseval group frames induced by abelian groups, leading to a refined characterization of the associated class of functions on the group. This characterization is used in an algorithm that performs an exhaustive search of all binary Parseval group frames for abelian groups of odd order. We walk through an application of this theory in Example 3.24 in order to motivate the ensuing practical guide to classifying binary Parseval frames for such groups.

In Section 4, we apply the structural insights on binary Parseval group frames to the problem of code design. We draw from the results of the exhaustive search for abelian groups of odd order. We compare the performance of binary Parseval frames generated by the two groups $\mathbb{Z}_p^q$ and $\mathbb{Z}_{p^q}$. The remaining examples in the section demonstrate application of these methods, offering comparisons between $\mathbb{Z}_3^3$ and $\mathbb{Z}_{27}$ and between $\mathbb{Z}_5^3$ and $\mathbb{Z}_{125}$.

Acknowledgment. All authors would like to thank the anonymous referee for thoughtful comments and suggestions.

2. Preliminaries

Unless otherwise noted, the vectors and matrices in this paper are over the field $\mathbb{Z}_2$ containing the two elements 0 and 1. We write I_k to indicate the $k \times k$ identity matrix over $\mathbb{Z}_2$, occasionally suppressing the subscript when the dimension would not otherwise be noted. We shall refer to the number of nonzero entries of a vector $x \in \mathbb{Z}_2^n$ as the *weight* of x (sometimes written $\|x\|_0$), and we say that x is *odd* or *even* if it has an odd or even number of entries equal to 1, respectively. These labels extend naturally to the columns and rows of a matrix viewed as column and row vectors (for example, we may refer to an *odd* or *even column* of a matrix). In keeping with the notation of real or complex frames, we denote the transpose of a binary matrix T as T^*.

Additionally, we may suppress the range of indices on sums and sets for simplicity of notation, as in writing $\sum_j c_j f_j$ for $\sum_{j\in J} c_j f_j$ or $\{f_j\}$ for $\{f_j\}_{j\in J}$ when the index set J is clear from the context.

2.1. Binary Frames.

Although the dot product as defined below has the appearance of an inner product, it is not positive definite because taking the dot product of a non-zero even vector with itself gives zero.

2.1. **Definition** ($\langle\cdot,\cdot\rangle$, the dot product on $\mathbb{Z}_2^n$)**.** We define the bilinear map $\langle\cdot,\cdot\rangle : \mathbb{Z}_2^n \times \mathbb{Z}_2^n \to \mathbb{Z}_2$, called the *dot product* on $\mathbb{Z}_2^n$, by

$$\left\langle \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}, \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} \right\rangle := \sum_{i=1}^{n} a_i b_i,$$

compactly expressed as $\langle a, b\rangle = b^* a$ for vectors $a = [a_i]_{i=1}^n, b = [b_i]_{i=1}^n$. Consistent with the language of inner products, we say that two vectors in $\mathbb{Z}_2^n$ are *orthogonal* if their dot product is equal to zero.

The absence of an inner product motivated the definition of binary frames in terms of a characterizing feature of finite real and complex frames, that they are a spanning set for the vector space in which they reside [5].

2.2. **Definition** (Binary frame, binary Parseval frame)**.** Let $\mathcal{F} = \{f_j\}_{j\in J}$ be a family of vectors in $\mathbb{Z}_2^n$, indexed by a finite set J. If $\mathcal{F}$ spans $\mathbb{Z}_2^n$, we call $\mathcal{F}$ a (binary) frame; if $\mathcal{F}$ satisfies the *reconstruction identity*

$$x = \sum_{j\in J} \langle x, f_j\rangle\, f_j \quad \text{for all} \quad x \in \mathbb{Z}_2^n, \tag{1}$$

we say that $\mathcal{F}$ is a *binary Parseval frame*.

For other choices of indefinite bilinear form on vector spaces over $\mathbb{Z}_2$ and associated frames, see [14]. Here, we restrict ourselves to the canonical choice, the dot product.

Since any family of vectors satisfying (1) necessarily spans $\mathbb{Z}_2^n$, each Parseval frame $\{f_j\}_{j\in J}$ for $\mathbb{Z}_2^n$ is in fact a frame, and the index set necessarily has the size $|J| \geq n$. For classification purposes it is useful to introduce equivalence relations among Parseval frames as in [5].

2.3. **Definition** (Unitary binary matrices, unitary equivalence, switching equivalence)**.** We say that a binary $n \times n$ matrix U is *unitary* if $UU^* = U^*U = I_n$. Given vector families $\mathcal{F} := \{f_j\}_{j\in J}$ and $\mathcal{F}' := \{f'_j\}_{j\in J}$ in $\mathbb{Z}_2^n$, we say that $\mathcal{F}$ is *unitarily equivalent* to $\mathcal{F}'$ if there exists a unitary $U \in M_n(\mathbb{Z}_2)$ such that $f'_j = Uf_j$ for all $j \in J$; we say that $\mathcal{F}$ is *switching equivalent* to $\mathcal{F}'$ (written $\mathcal{F} \cong_{\text{sw}} \mathcal{F}'$) if there exists a unitary $U \in M_n(\mathbb{Z}_2)$ and a permutation σ on J such that $f'_j = Uf_{\sigma(j)}$ for all $j \in J$.

By definition, unitary equivalence is a refinement of switching equivalence. The nature of unitary and permutation matrices makes verifying that these are both equivalence relations a straightforward exercise. Hereafter, we focus on frames indexed by elements of a group. In this context, a restricted version of switching equivalence is useful, which limits the permutations to the subset preserving the group-structure, that is, group automorphisms.

2.4. **Definition** (Automorphic switching equivalence)**.** Let Γ be a group, we denote the automorphisms of Γ by $\text{Aut}(\Gamma)$. Given vector families $\mathcal{F} := \{f_g\}_{g\in\Gamma}$ and $\mathcal{F}' := \{f'_g\}_{g\in\Gamma}$ indexed by Γ, we say that $\mathcal{F}$ and $\mathcal{F}'$ are *automorphically switching equivalent* (written $\mathcal{F} \cong_{\text{aut}} \mathcal{F}'$) if there exist a unitary $U \in M_n(\mathbb{Z}_2)$ and an automorphism $\sigma \in \text{Aut}(\Gamma)$ such that $f_g = Uf'_{\sigma(g)}$ for all $g \in \Gamma$.

2.2. **Operators associated with a frame.** The following four operators are defined in the same manner as for finite frames over the fields $\mathbb{R}$ and $\mathbb{C}$. In each definition, $\mathcal{F} = \{f_j\}_{j\in J}$ is assumed only to be a frame for $\mathbb{Z}_2^n$.

2.5. **Definition** ($\Theta_{\mathcal{F}}$, the analysis operator,$\Theta^*_{\mathcal{F}}$, the synthesis operator)**.** We denote the space of $\mathbb{Z}_2$-valued functions on a set J by $\mathbb{Z}_2^J$. The *analysis operator* for $\mathcal{F}$ is the map $\Theta_{\mathcal{F}} : \mathbb{Z}_2^n \to \mathbb{Z}_2^J$ given by $(\Theta_{\mathcal{F}}x)(j) = \langle x, f_j\rangle$. The adjoint of $\Theta_{\mathcal{F}}$, also called *synthesis operator*, maps $h \in \mathbb{Z}_2^J$ to $\Theta^*_{\mathcal{F}}h = \sum_{j\in J} h(j)f_j$.

2.6. **Definition** ($S_{\mathcal{F}}$, the frame operator)**.** The *frame operator* for $\mathcal{F}$ is the $n \times n$ matrix

$$S_{\mathcal{F}} := \Theta^*_{\mathcal{F}}\Theta_{\mathcal{F}}.$$

2.7. *Remark.* We note that the reconstruction identity (equation (1)) may be written as $x = \Theta^*_{\mathcal{F}}\Theta_{\mathcal{F}}x$. The reconstruction property of a Parseval frame $\mathcal{F}$ for $\mathbb{Z}_2^n$ is equivalent to $S_{\mathcal{F}} = I_n$.

2.8. **Definition** ($G_{\mathcal{F}}$, the Gramian)**.** The *Gramian* for $\mathcal{F}$, usually called the *Gram matrix* if $J = \{1, 2, \ldots, k\}$, is the linear map $G_{\mathcal{F}} : \mathbb{Z}_2^J \to \mathbb{Z}_2^J$

$$G_{\mathcal{F}} := \Theta_{\mathcal{F}}\Theta^*_{\mathcal{F}}.$$

Taking $\delta_j(k) = 1$ if $k = j$ and $\delta_j(k) = 0$ otherwise, $\{\delta_j\}_{j\in J}$ is the standard basis for $\mathbb{Z}_2^J$, and we use matrix notation to write $(G_{\mathcal{F}})_{i,j} = \langle \Theta_{\mathcal{F}}\Theta^*_{\mathcal{F}}\delta_j, \delta_i\rangle = \langle f_j, f_i\rangle$. It follows from the symmetry of $\langle\cdot,\cdot\rangle$ that $(G_{\mathcal{F}})_{i,j} = (G_{\mathcal{F}})_{j,i}$, and thus $G_{\mathcal{F}}$ is symmetric ($G_{\mathcal{F}} = G^*_{\mathcal{F}}$). Further, if $\mathcal{F}$ is a binary Parseval frame, then the Gramian is idempotent:

$$G^2_{\mathcal{F}} = (\Theta_{\mathcal{F}}\Theta^*_{\mathcal{F}})(\Theta_{\mathcal{F}}\Theta^*_{\mathcal{F}}) = \Theta_{\mathcal{F}} \underbrace{(\Theta^*_{\mathcal{F}}\Theta_{\mathcal{F}})}_{=S_{\mathcal{F}}=I_n} \Theta^*_{\mathcal{F}} = \Theta_{\mathcal{F}}\Theta^*_{\mathcal{F}} = G_{\mathcal{F}}\,. \tag{2}$$

For each of these matrices, we may suppress the subscript if doing so does not cause ambiguity, simply writing Θ ,Θ^*, S, and G.

2.3. **Group frames for $\mathbb{Z}_2^n$.** Recall that, given a finite group Γ and a vector space V, a *representation* of Γ on V is a group homomorphism

$$\rho : \Gamma \to \text{GL}(V).$$

In such a case, we say that Γ *acts on* V by ρ, and for any group element g we may interchangeably write $\rho(g)$ as ρ_g. We shall refer to the elements of $\{\rho_g\}_{g\in\Gamma}$ as the *matrices of the representation* ρ, or simply as representation matrices. Further, if each of the matrices ρ_g is unitary, then we call the representation itself unitary.

In the context of complex Hilbert spaces, given a finite group Γ, a *group frame* generated by Γ is any frame $\{f_g\}_{g\in\Gamma}$ that satisfies $\rho_g f_h = f_{gh}$ for all $g, h \in \Gamma$, for some representation ρ of Γ. If that representation is unitary, the frame is the orbit of a single vector [29]; it is this idea of a group generating a frame from a single vector that provides the basis of our definition.

2.9. **Definition** (Binary Parseval group frame, Γ-frame)**.** Given a natural number n and a group Γ acting on the vector space $\mathbb{Z}_2^n$ by a representation ρ, let $\mathcal{F} := \{\rho_g f\}_{g\in\Gamma}$ denote the orbit of a vector $f \in \mathbb{Z}_2^n$ under ρ. If $\mathcal{F}$ spans $\mathbb{Z}_2^n$, then it is a frame which we call a *binary group frame*. If $\mathcal{F}$ is a Parseval frame, we say that it is a *binary Parseval group frame*. For a given group Γ, we abbreviate the description "group frame generated by Γ" as Γ-frame [28]. We shall index frame vectors by their inducing group elements, so that $f_e := f$ and $f_g := \rho(g)f = \rho_g f$ for $g \in \Gamma$.

We begin with examples of frames generated with groups of size 27 acting on $\mathbb{Z}_2^9$. These examples show that depending on the choice of f_e, a unitary group representation may lead to an orbit that is a Parseval frame or just a frame.

2.10. *Examples* (Two binary cyclic frames). Let $\Gamma = \mathbb{Z}_{27}$ be the group of integers $\{0, 1, \ldots, 26\}$ with addition modulo 27. Let S_9 be the cyclic shift on $\mathbb{Z}_2^9$, so for each canonical basis vector e_i with $i \leq 8$, $S_9 e_i = e_{i+1}$ and $S_9 e_9 = e_1$. Since S_9 is a permutation matrix, the map $\rho : i \mapsto S_9^i$ is a homomorphism from Γ to $GL(\mathbb{Z}_2^9)$. Choosing $f_e^* = [1\,0\,1\,1\,1\,1\,1\,1\,0]$ gives that $\{f_j\}_{j\in\Gamma}$ spans $\mathbb{Z}_2^9$, but $\Theta_{\mathcal{F}}^*\Theta_{\mathcal{F}} \neq I_9$, so $\mathcal{F}$ is a frame but not Parseval.

Moreover, choosing $f_e = e_1$ shows that $\{f_i\}_{i\in\Gamma}$ with $f_i = S_9^i e_1 = e_{1+i(\mathrm{mod}\,9)}$ and $e_0 \equiv e_9$ repeats the sequence of canonical basis vectors three times. Consequently, the synthesis operator is $\Theta_{\mathcal{F}}^* = [I_9\, I_9\, I_9]$ and $\Theta_{\mathcal{F}}^*\Theta_{\mathcal{F}} = I_9$, so $\mathcal{F}$ is Parseval.

An exhaustive search of all Parseval frames obtained from group orbits under the action of $\mathbb{Z}_{27}$ on $\mathbb{Z}_2^9$ reveals that up to unitary equivalence, the second example is the only case of a Parseval $\mathbb{Z}_{27}$-frame for $\mathbb{Z}_2^9$. Such an exhaustive search is made feasible by methods developed in Section 3.4. In a preceding paper, the linear dependence among repeated frame vectors, as exhibited in the frame having synthesis operator $[I_9\, I_9\, I_9]$, has been called *trivial redundancy* [5]; In the next example, we show that another group of the same size generates frames as well as Parseval frames without the occurrence of repeated vectors in either case.

2.11. *Example* (Two binary Gabor frames). Let $a, b \in \mathrm{GL}(\mathbb{Z}_3^3)$ and the suggestively named $\rho_a, \rho_b \in \mathrm{GL}(\mathbb{Z}_2^9)$ be defined by

$$a := \begin{bmatrix} 1&0&0\\0&1&1\\0&0&1 \end{bmatrix}, \quad b := \begin{bmatrix} 1&1&0\\0&1&0\\0&0&1 \end{bmatrix}, \quad \rho_a := \begin{bmatrix} I_3&\mathbb{O}&\mathbb{O}\\\mathbb{O}&X&\mathbb{O}\\\mathbb{O}&\mathbb{O}&Y \end{bmatrix}, \quad \rho_b := \begin{bmatrix} \mathbb{O}&I_3&\mathbb{O}\\\mathbb{O}&\mathbb{O}&I_3\\I_3&\mathbb{O}&\mathbb{O} \end{bmatrix},$$

where $\mathbb{O}$ is the 3×3 matrix of zeros, $X = \begin{bmatrix} 0&0&1\\1&0&0\\0&1&0 \end{bmatrix}$, and $Y = X^2$.

The group generated by a and b under matrix multiplication is the nonabelian finite *Heisenberg-Weyl* group modulo 3, denoted HW_3. From the fact that products of powers of a and b give all upper triangular ternary matrices whose diagonal entries are fixed at 1, one can deduce that this group has order 27, see also [26]. The matrices ρ_a and ρ_b generate a group isomorphic to HW_3 and have been chosen such that setting $\rho(a) := \rho_a$ and $\rho(b) := \rho_b$ extends to an isomorphism $\rho : HW_3 \to \mathrm{GL}(\mathbb{Z}_2^9)$. For compactness of notation, we designate a third group element[1] c and corresponding $\rho_c \in \mathrm{GL}(\mathbb{Z}_2^9)$

$$c := \begin{bmatrix} 1&0&1\\0&1&0\\0&0&1 \end{bmatrix} \quad \text{and} \quad \rho_c := \rho(c) = \begin{bmatrix} X&\mathbb{O}&\mathbb{O}\\\mathbb{O}&X&\mathbb{O}\\\mathbb{O}&\mathbb{O}&X \end{bmatrix},$$

[1]Note that $\{e, c, c^2\}$ is the center of HW_3.

and order the elements of HW_3 in the sequence

$$e,\ a,\ a^2,\ b,\ ab,\ a^2b,\ b^2,\ ab^2,\ a^2b^2,$$
$$c,\ ac,\ a^2c,\ bc,\ abc,\ a^2bc,\ b^2c,\ ab^2c,\ a^2b^2c,$$
$$c^2,\ ac^2,\ a^2c^2,\ bc^2,\ abc^2,\ a^2bc^2,\ b^2c^2,\ ab^2c^2,\ a^2b^2c^2.$$

Choosing $f_e = [1\,1\,0\,1\,0\,0\,0\,0\,0]^*$ and $f'_e = [1\,1\,0\,1\,1\,0\,1\,0\,0]^*$ induces HW_3-frames $\{f_e\}$ and $\{f'_e\}$ whose synthesis operators $\Theta_1^* := [f_e|f_a|f_{a^2}|\cdots|f_{a^2b^2c^2}]$ and $\Theta_2^* := [f'_e|f'_a|f'_{a^2}|\cdots|f'_{a^2b^2c^2}]$ are given in Figure 1. One may verify that $\{f'_g\}_{g\in HW_3}$ is the only Parseval frame of the pair by calculating the corresponding frame operators.

$$\left[\begin{array}{ccccccccccccccccccccccccccc}
1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0\\
1&1&1&0&0&0&0&0&0&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&1&1&1&1&1&1&0&0&0\\
1&0&0&0&0&0&1&0&1&0&0&1&0&0&0&0&1&1&0&1&0&0&0&0&1&1&0\\
0&1&0&0&0&0&1&1&0&1&0&0&0&0&0&1&0&1&0&0&1&0&0&0&0&1&1\\
0&0&1&0&0&0&0&1&1&0&1&0&0&0&0&1&1&0&1&0&0&0&0&0&1&0&1\\
0&0&0&1&1&0&1&0&0&0&0&0&0&1&1&0&1&0&0&0&0&1&0&1&0&0&1\\
0&0&0&1&0&1&0&0&1&0&0&0&1&1&0&1&0&0&0&0&0&0&1&1&0&1&0\\
0&0&0&0&1&1&0&1&0&0&0&0&1&0&1&0&0&1&0&0&0&1&1&0&1&0&0
\end{array}\right]
\qquad
\left[\begin{array}{ccccccccccccccccccccccccccc}
1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&0&0&0\\
1&1&1&1&1&1&0&0&0&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&0&0&0&1&1&1&1&1&1&1&1&1\\
1&0&1&1&0&0&1&0&1&0&1&1&0&0&1&0&1&1&1&1&0&0&1&0&1&1&0\\
1&1&0&0&1&0&1&1&0&1&0&1&1&0&0&1&0&1&0&1&1&0&0&1&0&1&1\\
0&1&1&0&0&1&0&1&1&1&1&0&0&1&0&1&1&0&1&0&1&1&0&0&1&0&1\\
1&0&0&1&1&0&1&1&0&0&1&0&0&1&1&0&1&1&0&0&1&1&0&1&1&0&1\\
0&0&1&1&0&1&1&0&1&1&0&0&1&1&0&1&1&0&1&1&0&0&1&1&0&1&1\\
0&1&0&0&1&1&0&1&1&0&0&1&1&0&1&1&0&1&1&0&0&1&1&0&1&1&0
\end{array}\right]$$
$$\Theta_1^* \qquad\qquad\qquad\qquad \Theta_2^*$$

FIGURE 1. Synthesis operators of two binary Gabor frames (see Ex. 2.11)

2.4. **Regular representations and group frames.** Constructing a faithful unitary representation of a finite group Γ is always possible; if Γ has order k and given a k-dimensional vector space V, one can find a collection of $k \times k$ permutation matrices $\{P_g\}_{g\in\Gamma} \subset \mathrm{GL}(V)$ that form a group isomorphic to Γ. This is just a result of Cayley's theorem for groups based on the left or right regular representation, as given below. The challenge is to find vector spaces of smaller dimension carrying a unitary representation and vectors whose orbits under the group action form a Parseval frame.

With this in mind, we recall that the *regular representations* of a finite group Γ over a field $\mathbb{K}$ act on $\mathbb{K}^\Gamma$, the vector space of $\mathbb{K}$-valued functions on Γ; the *left* regular representation $\Lambda = \{\Lambda_g\}_{g\in\Gamma}$ and *right* regular representation $R = \{R_g\}_{g\in\Gamma}$ act on $\varphi : \Gamma \to \mathbb{K}$ according to

$$\Lambda_g\varphi : h \mapsto \varphi(g^{-1}h) \quad \text{and} \quad R_g\varphi : h \mapsto \varphi(hg)$$

and hence define group isomorphisms. By associativity, $\Lambda_g R_h\varphi$ and $R_h\Lambda_g\varphi$ are well defined, and commutativity among operators of the regular representations follows from the chain of equalities

$$\big(\Lambda_g R_h\varphi\big)(x) = \big(R_h\varphi\big)(g^{-1}x) = \varphi(g^{-1}xh) = \big(\Lambda_g\varphi\big)(xh) = \big(R_h\Lambda_g\varphi\big)(x)$$

which holds for all $g, h, x \in \Gamma$ and $\varphi \in \mathbb{K}^\Gamma$.

2.12. *Remark.* For future use, we note that for each $g \in \Gamma$, the nonzero entries of the permutation matrix associated with Λ_g and the canonical basis are indexed by the set $\{(gh, h)\colon h \in \Gamma\}$, and R_g is nonzero exactly on index set $\{(hg^{-1}, h)\colon h \in \Gamma\}$. Written in terms of the Kronecker delta,

$$(\Lambda_g)_{\alpha,\beta} = \delta^g_{\alpha\beta^{-1}} \quad \text{and} \quad (R_g)_{\alpha,\beta} = \delta^g_{\alpha^{-1}\beta}, \qquad \text{where} \qquad \delta^j_i := \begin{cases} 1 \text{ if } i = j \\ 0 \text{ if } i \neq j \end{cases}.$$

We close the section by showing that, as in the real or complex case [29], the group representations which generate binary Parseval group frames are unitary.

2.13. **Proposition** (Binary Parseval group frames are generated by unitary representations)**.** *Given a finite group Γ, let $\mathcal{F}$ be a binary Γ-frame generated by a group representation ρ. If $\mathcal{F}$ is Parseval with analysis operator Θ, then ρ is a unitary representation with matrices explicitly given by $\rho_g = \Theta^*\Lambda_g\Theta$ for each $g \in \Gamma$.*

Proof. Let Γ, $\mathcal{F}$ and Θ be as in the hypothesis. For $g, h \in \Gamma$ and $x \in \mathbb{Z}_2^n$,

$$(\Lambda_g \Theta x)(h) = \Theta x(g^{-1}h) = \langle x, \rho_{g^{-1}} f_h \rangle = \langle \rho_{g^{-1}}^* x, f_h \rangle = (\Theta \rho_{g^{-1}}^* x)(h),$$

so the following diagram commutes:

$$\begin{array}{ccc} \mathbb{Z}_2[\Gamma] & \xrightarrow{\Lambda_g} & \mathbb{Z}_2[\Gamma] \\ {\scriptstyle\Theta}\uparrow & & \uparrow{\scriptstyle\Theta} \\ \mathbb{Z}_2^n & \xrightarrow{(\rho_{g^{-1}})^*} & \mathbb{Z}_2^n \end{array}$$

By the Parseval property and the intertwining relationship, $\rho_{g^{-1}}^* = \Theta^*\Theta\rho_{g^{-1}}^* = \Theta^*\Lambda_g\Theta$. Replacing g with g^{-1} and taking the transpose, we then get $\rho_g = \Theta^*\Lambda_{g^{-1}}^*\Theta$. Next, the unitarity of Λ_g gives the claimed expression $\rho_g = \Theta^*\Lambda_g\Theta$. It follows that

$$\begin{aligned} \rho_{g^{-1}}^* &= \Theta^*\Lambda_g\Theta \\ &= (\Theta^*\Lambda_{g^{-1}}\Theta)^* \\ &= (\rho_g^*)^* \equiv \rho_g. \end{aligned}$$

We conclude that each ρ_g is unitary. □

2.14. *Example* (A binary Parseval $\mathbb{Z}_3^2$-frame). The family of vectors and matrix

$$\mathcal{F} = \left\{ \underset{f_{\binom{0}{0}}}{\begin{bmatrix}0\\1\\0\\0\\0\end{bmatrix}}, \underset{f_{\binom{0}{1}}}{\begin{bmatrix}0\\0\\1\\0\\0\end{bmatrix}}, \underset{f_{\binom{0}{2}}}{\begin{bmatrix}0\\0\\0\\1\\0\end{bmatrix}}, \underset{f_{\binom{1}{0}}}{\begin{bmatrix}0\\1\\0\\1\\0\end{bmatrix}}, \underset{f_{\binom{1}{1}}}{\begin{bmatrix}0\\0\\1\\1\\0\end{bmatrix}}, \underset{f_{\binom{1}{2}}}{\begin{bmatrix}0\\1\\0\\1\\1\end{bmatrix}}, \underset{f_{\binom{2}{0}}}{\begin{bmatrix}1\\1\\0\\1\\0\end{bmatrix}}, \underset{f_{\binom{2}{1}}}{\begin{bmatrix}1\\1\\1\\0\\0\end{bmatrix}}, \underset{f_{\binom{2}{2}}}{\begin{bmatrix}1\\0\\1\\1\\0\end{bmatrix}} \right\} \quad \text{and} \quad G = \begin{bmatrix} 1&0&0&1&0&1&1&1&0 \\ 0&1&0&1&1&0&0&1&1 \\ 0&0&1&0&1&1&1&0&1 \\ 1&1&0&1&0&0&1&0&1 \\ 0&1&1&0&1&0&1&1&0 \\ 1&0&1&0&0&1&0&1&1 \\ 1&0&1&1&1&0&1&0&0 \\ 1&1&0&0&1&1&0&1&0 \\ 0&1&1&1&0&1&0&0&1 \end{bmatrix}$$

are a binary Parseval $\mathbb{Z}_3^2$ frame and its Gramian. Denoting the left regular representation of $\mathbb{Z}_3$ as ρ' with $\rho_1' := \left[\begin{smallmatrix}0&0&1\\1&0&0\\0&1&0\end{smallmatrix}\right]$, the left regular representation matrices of $\mathbb{Z}_3^2$ are defined by the Kronecker products $\Lambda_{\binom{i}{j}} = \rho_i' \otimes \rho_j'$, with $\rho_i' = (\rho_1')^i$ for $i \in \mathbb{Z}_2$. The corresponding matrices $\rho\binom{i}{j} := \Theta^*\Lambda_{\binom{i}{j}}\Theta$ provide a representation of the group $\mathbb{Z}_3^2$ on the vector space $\mathbb{Z}_2^5$.

$$\rho\tbinom{0}{0} = \begin{bmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}, \quad \rho\tbinom{0}{1} = \begin{bmatrix}1&0&0&0&0\\0&0&0&1&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&0&1\end{bmatrix}, \quad \rho\tbinom{0}{2} = \begin{bmatrix}1&0&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&1&0&0&0\\0&0&0&0&1\end{bmatrix},$$

$$\rho\tbinom{1}{0} = \begin{bmatrix}0&0&0&0&1\\1&1&0&1&0\\1&1&1&0&0\\1&0&1&1&0\\0&1&1&1&0\end{bmatrix}, \quad \rho\tbinom{1}{1} = \begin{bmatrix}0&0&0&0&1\\1&0&1&1&0\\1&1&0&1&0\\1&1&1&0&0\\0&1&1&1&0\end{bmatrix}, \quad \rho\tbinom{1}{2} = \begin{bmatrix}0&0&0&0&1\\1&1&1&0&0\\1&0&1&1&0\\1&1&0&1&0\\0&1&1&1&0\end{bmatrix},$$

$$\rho\tbinom{2}{0} = \begin{bmatrix}0&1&1&1&0\\0&1&1&0&1\\0&0&1&1&1\\0&1&0&1&1\\1&0&0&0&0\end{bmatrix}, \quad \rho\tbinom{2}{1} = \begin{bmatrix}0&1&1&1&0\\0&1&0&1&1\\0&1&1&0&1\\0&0&1&1&1\\1&0&0&0&0\end{bmatrix}, \quad \rho\tbinom{2}{2} = \begin{bmatrix}0&1&1&1&0\\0&0&1&1&1\\0&1&0&1&1\\0&1&1&0&1\\1&0&0&0&0\end{bmatrix}.$$

One may verify that the induced map $\rho : \mathbb{Z}_3^2 \to \mathrm{GL}(\mathbb{Z}_2^5)$ is a unitary representation and that $\mathcal{F}$ is in fact the orbit of $f_{\binom{0}{0}}$ under ρ.

3. The structure of the Gramian of a binary Parseval group frame

The Gramian captures geometric information about the structure of the associated frame, since it records every pairwise dot product among frame vectors. If the frame is a group frame, then it also reflects the group structure. As shown below, the Gramian of a binary Parseval group frame is an element of the algebra generated by the right regular representation.

3.1. **Theorem** (Gramians of binary Parseval group frames as elements of the group algebra)**.** *Let Γ be a finite group with right regular representation $\{R_g\}_{g\in\Gamma}$ and associated group algebra $\mathbb{Z}_2[\{R_g\}]$, and suppose G is the Gramian of a binary Parseval Γ-frame $\mathcal{F} := \{f_g\}_{g\in\Gamma}$, then the Gram matrix is in the group algebra. More explicitly, G is given by*

$$G = \sum_{g\in\Gamma} \eta(g) R_g \tag{3}$$

where the function $\eta : \Gamma \to \mathbb{Z}_2$ is defined by $\eta(g) := \langle f_g, f_e\rangle$.

Proof. Let ρ be the frame-generating group representation, which by Proposition 2.13 is a unitary representation of Γ. Consider $H = \sum_{g\in\Gamma} \eta(g) R_g$ with η as in the statement of the theorem. We compute for $a, b \in \Gamma$ the value

$$\begin{aligned} H_{a,b} &= \sum_{g\in\Gamma} \eta(g)(R_g)_{a,b} \\ &= \sum_{g\in\Gamma} \eta(g)\delta^g_{a^{-1}b} = \eta(a^{-1}b) \\ &= \langle f_{a^{-1}b}, f_e\rangle \\ &= \langle \rho_b f_e, \rho^*_{a^{-1}} f_e\rangle \\ &= \langle f_b, f_a\rangle = G_{a,b}\,. \end{aligned}$$

In the last identity, we have used the unitarity, $\rho_{a^{-1}} = \rho^*_a$. □

3.2. **Theorem** (Gramians of binary Parseval frames in a group algebra imply group frame structure)**.** *Let Γ be a finite group with regular representations Λ and R, and suppose $\mathcal{F} = \{f_g\}_{g\in\Gamma}$ is a binary Parseval frame with Gramian G and analysis operator Θ. If G is in the group algebra $\mathbb{Z}_2[\{R_g\}]$, then $\rho_g := \Theta^*\Lambda_g\Theta$ defines a unitary representation of Γ and $\{f_g\}_{g\in\Gamma}$ is a Γ-frame obtained from the orbit of f_e under the representation $\{\rho_g\}_{g\in\Gamma}$.*

Proof. Assume that $G = \Theta\Theta^* \in \mathbb{Z}_2[\{R_g\}]$. Since Λ_g and $R_{g'}$ commute for each $g, g' \in \Gamma$, so do Λ_g and G. From $\Theta^*\Theta\Theta^* = \Theta^*$, then, we have $\Theta^*\Lambda_g\Theta\Theta^*\Lambda_h\Theta = \Theta^*\Lambda_{gh}\Theta$ for each $g, h \in \Gamma$, and since $(\Theta^*\Lambda_g\Theta)^* = \Theta^*\Lambda_{g^{-1}}\Theta$, it follows that $\rho_g = \Theta^*\Lambda_g\Theta$ defines a unitary representation of Γ. Using these properties for ρ_g then shows that

$$\rho_g f_e = \Theta^*\Lambda_g\Theta\Theta^*\delta_e = \Theta^*\Theta\Theta^*\Lambda_g\delta_e = \Theta^*\delta_g = f_g\,,$$

so the frame vectors are obtained from the orbit under the unitaries $\{\rho_g\}_{g\in\Gamma}$. □

We summarize the preceding two theorems in a characterization of binary Parseval group frames.

3.3. **Corollary** (Characterization of binary Parseval group frames in terms of Gramians)**.** *Let Γ be a finite group with right regular representation $\{R_g\}_{g\in\Gamma}$. A binary Parseval frame $\mathcal{F}$ indexed by Γ is a Γ-frame if and only if its Gramian is in the algebra $\mathbb{Z}_2[\{R_g\}_{g\in\Gamma}]$.*

3.1. **Characterizing the structure of the Gramian.** In order to facilitate a catalogue of binary Parseval group frames, we identify necessary and sufficient conditions for their Gramians.

In the real or complex case, each symmetric idempotent matrix is the Gram matrix of a Parseval frame. In the binary case, [1, Theorem 4.1] characterizes Parseval frames with the additional requirement that at least one row or column vector is odd. This condition is equivalent to the condition that the Gramian has at least one odd vector in its range, since the span of the column vectors of a matrix forms the range of the matrix; we use these statements interchangeably throughout this paper. This condition is *also* equivalent to that of having at least one nonzero entry on the diagonal, since the idempotence and symmetry of a Gramian G induce the identity between the dot product of a vector $G\delta_g$ with itself and the corresponding diagonal entry of the Gramian, $\langle G\delta_g, G\delta_g\rangle = G_{g,g}$ for all $g \in \Gamma$.

We next combine the results we obtained so far with the characterization of the Gramians of binary Parseval frames to characterize Gramians that belong to binary Parseval group frames.

3.4. **Theorem** (The structure of Gramians of binary Parseval group frames)**.** *Given a finite group Γ with right regular representation R, a map $G : \mathbb{Z}_2^\Gamma \to \mathbb{Z}_2^\Gamma$ is the Gramian of binary Parseval Γ-frame if and only if G is symmetric and idempotent, $G \in \mathbb{Z}_2[\{R_g\}]$ and the range of G contains an odd vector.*

Proof. As noted above, [1, Theorem 4.1] characterizes the Gram matrices of binary Parseval frames as symmetric, idempotent matrices having at least one odd column. Thus, given a finite group Γ, the characterization in the current theorem reduces to Corollary 3.3, and is thereby proven. □

In short, this last theorem states that we can move back and forth between elements in the unitary equivalence class of a frame and the Gramian. Since we focus on the construction of Gramians hereafter, we summarize how to obtain a group frame from the corresponding Gramian more explicitly. To this end, we recall that if G is the Gramian of a binary Parseval frame, then it factors into $G = \Theta\Theta^*$ where the columns of Θ are orthonormal with respect to the dot product and form a basis for the range of G. This means, the columns of Θ^* are in the space whose dimension is the rank of G, as expected. Moreover, for any such factorization of G, the columns of Θ^* form a binary Parseval frame in the unitary equivalence class associated with G. Factoring G can be achieved by performing a version of a Gram-Schmidt algorithm, as demonstrated in [1]. We summarize the most practically relevant consequences of these observations and the preceding theorems.

3.5. **Corollary.** *Let Γ be a finite group with left and right regular representations $\{\Lambda_g\}_{g\in\Gamma}$ and $\{R_g\}_{g\in\Gamma}$, respectively. If a map $G \in \mathbb{Z}_2[\{R_g\}_{g\in\Gamma}]$ is symmetric, idempotent and its range contains an odd vector, then it can be factored in the form $G = \Theta\Theta^*$ where $f_g = \Theta^*\delta_g$ defines a binary Parseval frame $\{f_g\}_{g\in\Gamma}$ for $\mathbb{Z}_2^k$, and k is the rank of G. Moreover, $\rho_g = \Theta^*\Lambda_g\Theta$ defines a unitary representation of Γ and the vectors $\{f_g\}_{g\in\Gamma}$ are a binary Parseval Γ-frame obtained from the orbit of f_e under the representation $\{\rho_g\}_{g\in\Gamma}$.*

3.2. **Additional properties of the Gramian.** Since regular representation matrices are permutation matrices, a consequence of Theorem 3.1 is that each of the rows of the Gramian of a binary Parseval group frame has the same weight. Thus, if a Gramian is assumed to be that of a binary Parseval group frame, the condition that one column is odd is equivalent to the condition that *every* column is odd, which equates to the condition that every diagonal entry is a 1, or even simply that $\eta(e) = 1$. Continuing under the assumption that the Gramian may be written as $G = \Sigma_g \eta(g) R_g$, the quantity of 1's in a column is the quantity of elements $g \in \Gamma$ such that $\eta(g) = 1$; it follows that G has an odd column if and only if the sum $\Sigma_g \eta(g) = 1$.

Now, suppose Γ is a finite group of order k and that we wish to exhaustively search for Γ-frames. The characterization in Theorem 3.4 tells us that the candidate set of Gramians is a subset of

$$\left\{ H = \sum_{g\in\Gamma} \eta(g) R_g \;\middle|\; \begin{array}{l} \eta(e) = 1 \\ \eta(g) = \eta(g^{-1}) \text{ for all } g \in \Gamma \\ \sum_g \eta(g) = 1 \end{array} \right\}. \tag{4}$$

From a computational standpoint, the three necessary criteria are easy to check as properties of the coefficient function η; in fact, no matrix multiplication is required until we wish to check idempotence. The following proposition reduces the idempotence condition to a property of η as well.

3.6. **Proposition** (Idempotence in group algebra characterized by convolution identity)**.** *Given a finite group Γ with right regular representation $\{R_g\}_{g\in\Gamma}$ and a binary function $\eta : \Gamma \to \mathbb{Z}_2$, the matrix $\sum_g \eta(g) R_g$ is idempotent if and only if η is invariant under convolution with itself; that is, if and only if $\eta(h) = \eta * \eta(h) := \sum_g \eta(g)\eta(g^{-1}h)$ for each $h \in \Gamma$.*

Proof. Let Γ and $\{R_g\}_{g\in\Gamma}$ be as given above and $\eta:\Gamma\to\mathbb{Z}_2$ be a binary function. We note that

$$\Big(\sum_{g\in\Gamma}\eta(g)R_g\Big)^2=\sum_{g_1,g_2\in\Gamma}\eta(g_1)\eta(g_2)R_{g_1g_2}=\sum_{g,h\in\Gamma}\eta(g)\eta(g^{-1}h)R_h; \tag{5}$$

it follows that $\sum\eta(g)R_g=\big(\sum\eta(g)R_g\big)^2$ implies $\eta(h)=\sum_g\eta(g)\eta(g^{-1}h)$ for each $h\in\Gamma$. On the other hand, suppose $\eta:\Gamma\to\mathbb{Z}_2$ is convolution invariant. Then

$$\sum_{h\in\Gamma}\eta(h)R_h=\sum_{h\in\Gamma}\Big[\sum_{g\in\Gamma}\eta(g)\eta(g^{-1}h)\Big]R_h=\sum_{g,h\in\Gamma}\eta(g)\eta(g^{-1}h)R_h,$$

which by equation (5) is equal to $\big(\sum\eta(g)R_g\big)^2$, and the proof is complete. □

3.7. *Example.* Consider D_3, the dihedral group of order 6, described $\langle a,b:a^3=1,b^2=1,b^{-1}ab=a^{-1}\rangle$; ordering the elements $1,a,a^2,b,ab,a^2b$, then the right regular representation matrices of D_3 are given by

$$\underset{R_1}{\begin{bmatrix}1&0&0&0&0&0\\0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\end{bmatrix}},\ \underset{R_a}{\begin{bmatrix}0&1&0&0&0&0\\0&0&1&0&0&0\\1&0&0&0&0&0\\0&0&0&0&0&1\\0&0&0&1&0&0\\0&0&0&0&1&0\end{bmatrix}},\ \underset{R_{a^2}}{\begin{bmatrix}0&0&1&0&0&0\\1&0&0&0&0&0\\0&1&0&0&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\\0&0&0&1&0&0\end{bmatrix}},\ \underset{R_b}{\begin{bmatrix}0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\\1&0&0&0&0&0\\0&1&0&0&0&0\\0&0&1&0&0&0\end{bmatrix}},\ \underset{R_{ab}}{\begin{bmatrix}0&0&0&0&1&0\\0&0&0&0&0&1\\0&0&0&1&0&0\\0&0&1&0&0&0\\1&0&0&0&0&0\\0&1&0&0&0&0\end{bmatrix}},\ \underset{R_{a^2b}}{\begin{bmatrix}0&0&0&0&0&1\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&1&0&0&0&0\\0&0&1&0&0&0\\1&0&0&0&0&0\end{bmatrix}}.$$

A quick check for convolution invariance among the twelve coefficient functions satisfying the conditions in (4) shows that only I_6 and $G_1:=R_1+R_a+R_{a^2}$ give suitable Gramians. Synthesis matrices for the two classes are given by $\Theta^*_{G_1}:=\left[\begin{smallmatrix}1&1&1&0&0&0\\0&0&0&1&1&1\end{smallmatrix}\right]$ and $\Theta^*_{I_6}=I_6$.

It follows from Proposition 3.6 that the coefficient function of the Gramian of a binary Parseval group frame is always convolution invariant, but convolution invariance of such a function does not ensure matrix symmetry:

3.8. *Example.* Let $\{R_j\}_{j=0}^6$ be the right regular representation matrices for the group $\mathbb{Z}_7$, noting that $R_j^*=R_j^{-1}=R_{-j}$. Consider the coefficient function given by

$$\eta(x)=\begin{cases}1 & \text{if } x\in\{0,1,2,4\}\\ 0 & \text{if } x\in\{3,5,6\}\end{cases},$$

which is easily verified to satisfy $\eta=\eta*\eta$. It is clear, however, that the matrix $G=\sum_{j=0}^6\eta(j)R_j$ is not symmetric (since $\eta(1)\neq\eta(6)$, for example), so G is not the Gramian of any frame.

Adding idempotence under convolution to the conditions in (4) removes the need to require that the coefficient function sums to 1, which is then implicit in $\eta(e)=1$. We conclude a characterization of the coefficient functions of binary Parseval group frames.

3.9. **Theorem** (Gramians of binary Parseval Γ-frames characterized by η)**.** *Given a finite group Γ with right regular representation matrices $\{R_g\}_{g\in\Gamma}$ and $G=\sum_g\eta(g)R_g$, then G is the Gramian of a binary Parseval Γ-frame if and only if $\eta(e)=1$, η is symmetric under inversion of its argument and idempotent under convolution.*

Proof. Since $G=\sum_g\eta(g)R_g$ and $R_g^*=R_{g^{-1}}$ for all $g\in\Gamma$, it follows that G is symmetric if and only if η is. Further, Proposition 3.6 equates the idempotence of G with that of η. Now, $\eta(e)=1$ if and only if $\eta(g)=1$ for all $g\in\Gamma$, if and only if G has at least one odd column.

Theorem 3.4 provides four conditions which characterize the Gramians of binary Parseval group frames, three of which we have just demonstrated are equivalent to conditions on η. Since G automatically satisfies the remaining condition as an element of the group algebra $\mathbb{Z}_2[\{R_g\}]$, it follows that $G=\sum_g\eta(g)R_g$ is the Gramian of a binary Parseval Γ-frame if and only if $\eta(e)=1$, $\eta=\eta*\eta$, and $\eta(g)=\eta(g^{-1})$ for all $g\in\Gamma$. □

In light of the last theorem, we can replace the necessary conditions (4) with necessary and sufficient conditions for G being the Gramian of a binary Parseval Γ-frame $\mathcal{F}$,

$$G \in \left\{ \sum_{g\in\Gamma} \eta(g) R_g \;\middle|\; \begin{array}{l} \eta(e) = 1 \\ \eta(g) = \eta(g^{-1}) \text{ for all } g \in \Gamma \\ \eta = \eta * \eta \end{array} \right\}, \tag{6}$$

where η is assumed to be a $\mathbb{Z}_2$-valued function on Γ.

3.3. **Binary Parseval frames from orbits of abelian groups.** Next, we focus on the special case of abelian groups.

3.10. **Lemma** (Idempotence from square root condition for abelian groups)**.** *Given a finite abelian group* Γ *and function* $\eta : \Gamma \to \mathbb{Z}_2$*,* η *is idempotent under convolution if and only if*

$$\eta(g) = \sum_{h^2=g} \eta(h) \quad \textit{for all} \quad g \in \Gamma.$$

Proof. Fix $g \in \Gamma$ and partition Γ into $K_g := \{h \in \Gamma : h^2 = g\}$ and $B := \Gamma \backslash K_g$. Since Γ is abelian and by the definition of B, we have that for each element $x \in B$ there is a unique element $x^{-1}g = gx^{-1} \in B$, and $x \neq x^{-1}g$. We refine our partition on Γ by separating B into disjoint sets B_1 and B_2 such that no two elements $x, y \in B_i$ multiply to g, arbitrarily assigning one element from each pair $\{x, x^{-1}g\}$ to B_1 and the other to B_2.

The idempotence under convolution is thus expressed

$$\begin{aligned} \eta(g) &= \sum_{h\in\Gamma} \eta(h)\eta(h^{-1}g) \\ &= \sum_{h\in K_g} \eta(h)\eta(\underbrace{h^{-1}g}_{=h}) + \sum_{x\in B_1} \eta(x)\eta(x^{-1}g) + \sum_{y\in B_2} \eta(y)\eta(y^{-1}g) \\ &= \sum_{h\in K_g} \eta(h)\eta(h) + \sum_{x\in B_1} \left[\eta(x)\eta(x^{-1}g) + \eta(x^{-1}g)\eta(\underbrace{x}_{=(x^{-1}g)^{-1}g})\right] \\ &= \sum_{h\in K_g} \eta(h) + 2\sum_{x\in B_1} \eta(x)\eta(x^{-1}g) \\ &= \sum_{h\in K_g} \eta(h), \end{aligned}$$

where the last two identities follow from noting $z^2 = z$ and $2z = 0$ for all $z \in \mathbb{Z}_2$. □

3.11. *Example* (Binary Parseval group frames of $\mathbb{Z}_6$). We use the preceding lemma to classify the binary Parseval group frames generated by the (abelian) additive group $\Gamma := \mathbb{Z}_6$. Suppose $G = \sum \eta(g) R_g$ is the Gramian of a binary Parseval $\mathbb{Z}_6$-frame $\mathcal{F}$; in the notation of the proof of Lemma 3.10, we have $K_1 = K_3 = K_5 = \emptyset$, for which the "square root condition" asserts $\eta(1) = \eta(3) = \eta(5) = 0$. By the coefficient function characterization of the Gramian, $\eta(0) = 1$, and since $2 + 2 = 4$, we have that either $\eta(2) = \eta(4) = 1$ or G is the identity matrix. It follows, noting that both options induce idempotent matrices, that any binary Parseval $\mathbb{Z}_6$-frame has a Gram matrix that is either I_6 or $G := R_0 + R_2 + R_4$,

$$\underset{G}{\begin{bmatrix} 1&0&1&0&1&0\\ 0&1&0&1&0&1\\ 1&0&1&0&1&0\\ 0&1&0&1&0&1\\ 1&0&1&0&1&0\\ 0&1&0&1&0&1 \end{bmatrix}} = \underset{R_0}{\begin{bmatrix} 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1 \end{bmatrix}} + \underset{R_2}{\begin{bmatrix} 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1\\ 1&0&0&0&0&0\\ 0&1&0&0&0&0 \end{bmatrix}} + \underset{R_4}{\begin{bmatrix} 0&0&0&0&1&0\\ 0&0&0&0&0&1\\ 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0 \end{bmatrix}}.$$

To complete the classification, we note that G and I_6 represent distinct classes, since the Gramians of switching equivalent binary Parseval frames have the same number of nonzero entries. Synthesis matrices for the two classes are given by $\Theta_G^* := \left[\begin{smallmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{smallmatrix}\right]$ and $\Theta_{I_6}^* = I_6$.

In the special case that every element in a group has exactly one square root, an even stronger consequence holds for η. This "unique square root" property is determined solely by the parity of a group's order (see, for example, Proposition 2.1 in [18]), and we recall part of this characterization in the following lemma.

3.12. **Lemma.** *A finite group of odd order has unique square roots.*

Proof. Let Γ be a group such that $|\Gamma| = 2n-1$ for some integer $n \geq 2$, and suppose $a^2 = b^2$ for some $a, b \in \Gamma$. Then $a^{2n-1} = e$, so $a = a \cdot a^{2n-1} = a^{2n} = b^{2n} = b$. □

3.13. **Theorem** (Odd-ordered abelian groups and η)**.** *Let Γ be a finite abelian group of odd order. Then the map $g \mapsto \{g' \in \Gamma : g^{2^m} = g' \text{ for some } m \in \mathbb{N}\}$ partitions Γ, and a function $\eta : \Gamma \to \mathbb{Z}_2$ is idempotent under convolution if and only if η is constant on these sets.*

Proof. Since Γ has odd order, the unique square root property reduces the condition

$$\eta(g) = \sum_{h^2=g} \eta(h) \quad \text{for all} \quad g \in \Gamma$$

to

$$\eta(g^2) = \eta(g) \quad \text{for all} \quad g \in \Gamma;$$

thus, it remains only to show that the map defined in the hypothesis partitions Γ. Let $g \in \Gamma$, and for $j \in \mathbb{N}$, define $\gamma_j := g^{2^j}$. Since Γ finite, we may take N to be the least positive integer such that $\gamma_{N+1} \in \{\gamma_j\}_{j=1}^N$. By Γ's unique square roots, it follows that $\gamma_{N+1} = \gamma_1$, or $g = g^{2^N}$. Now, let $h \in \Gamma$ be distinct from g, and similarly define a sequence by $\hat{\gamma}_j := h^{2^j}$, with minimal M such that $h = h^{2^M}$. It follows that either $\{\gamma_j\}_{j\in\mathbb{N}} = \{\hat{\gamma}_j\}_{j\in\mathbb{N}}$ or $\{\gamma_j\}_{j\in\mathbb{N}} \cap \{\hat{\gamma}_j\}_{j\in\mathbb{N}} = \emptyset$, and the claim is shown. □

3.14. *Example* (Classes of $\mathbb{Z}_{17}$-frames). Suppose $G = \sum_g \eta(g) R_g \in \mathbb{Z}_2[\mathbb{Z}_{17}]$ is the Gramian of a binary Parseval $\mathbb{Z}_{17}$-frame. $\mathbb{Z}_{17}$ satisfies the conditions of Theorem 3.13, so we know that η is constant on each of the sets $\Delta_1 := \{1, 2, 4, 8, 16, 15, 13, 9\}$ and $\Delta_3 := \{3, 6, 12, 7, 14, 11, 5, 10\}$, which are closed under inversion. Thus, G is one of exactly four operators, given by

$$I_{17}, \quad I_{17} + \textstyle\sum_{j\in\Delta_1} R_j, \quad I_{17} + \sum_{j\in\Delta_3} R_j, \quad \text{and } \sum_{j\in\mathbb{Z}_{17}} R_j.$$

In illustrating an application of Theorem 3.13, this example also motivates us to introduce some additional notation.

3.15. **Definition** (Symmetric doubling orbit, symmetric doubling orbit partition, $R_{[g]}$)**.** Let Γ be a finite abelian group having unique square roots. For any element $g \in \Gamma$, the *symmetric doubling orbit* of g is the set

$$[g] := \{h \in \Gamma : g^{2^m} = h \text{ for some } m \in \mathbb{N}\} \cup \{h \in \Gamma : (g^{-1})^{2^m} = h \text{ for some } m \in \mathbb{N}\}.$$

We define

$$R_{[g]} := \sum_{h\in[g]} R_h$$

and say that the collection $\Gamma' = \{[g]\}_{g\in J}$ is the *symmetric doubling orbit partition* of Γ (indexed by representatives $J \subset \Gamma$) if $\bigcup_{g\in J} [g] = \Gamma$ and for distinct $g, h \in J$ we have $[g] \neq [h]$.

3.16. *Remark.* We comment on our terminology. Since Γ is abelian, let us momentarily consider it as an additive group and express it as $\Gamma \cong \bigoplus_{i=1}^{k} \mathbb{Z}_{p_i}$. Modifying the notation in Definition 3.15 accordingly, we have

$$[g] := \{h \in \Gamma : 2^m g = h \text{ for some } m \in \mathbb{N}\} \cup \{h \in \Gamma : 2^m(-g) = h \text{ for some } m \in \mathbb{N}\},$$

which is equivalent to $\{\rho_m g\}_{m=1}^{L} \cup \{\rho_m(-g)\}_{m=1}^{L}$ for some $L \in \mathbb{N}$, where $\rho_m := 2^m I_k$.

It is easy to verify that the matrices $\{2^m I_k\}_{m=1}^{L}$ are representation matrices for the multiplicative subgroup generated by 2 in $\mathbb{Z}_L$, which motivates the "doubling orbit" part of the name *symmetric doubling orbit*: $\{\rho_m g\}_{m=1}^{L}$ is, in fact, the orbit of g under the action of $\langle 2\rangle_{\mathbb{Z}_L}^{\times}$.

We proceed with two results making use of the new notation. The first may be considered a corollary of Theorems 3.9 and 3.13, and the second uses the symmetric doubling orbit partitioning to provide a count of the binary Parseval Γ-frame unitary equivalence classes for our specified groups Γ.

3.17. **Theorem** (Characterization of binary Parseval Γ-frames for odd order, abelian Γ)**.** *Let Γ be an odd-ordered abelian group with right regular representation R and symmetric doubling orbit partition $\{[g]\}_{g\in J}$. Let G be a linear map $G : \mathbb{Z}_2^{\Gamma} \to \mathbb{Z}_2^{\Gamma}$, then G is the Gramian of a binary Parseval Γ-frame if and only if $G = \sum_{g\in J} \nu([g]) R_{[g]}$ for some $\nu : \Gamma' \to \mathbb{Z}_2$ with $\nu([e]) = 1$.*

Proof. Assume G is the Gramian of a binary Parseval Γ-frame, and let $G = \sum_{g\in\Gamma} \eta(g) R_g$; then η is idempotent under convolution (by Theorem 3.9) and thus constant on symmetric doubling orbits (by Theorem 3.13). It follows that $\nu([g]) := \eta(g)$ is well defined and satisfies $G = \sum_{[g]\in J} \nu([g]) R_{[g]}$ and $\nu([e]) = 1$.

Conversely, assume $G = \sum_{g\in J} \nu([g]) R_{[g]}$ for some ν such that $\nu([e]) = 1$, and define $\eta : \Gamma \to \mathbb{Z}_2$ by assigning $\eta(g) = \nu([g])$, then the conditions of Theorem 3.13 are met and η is idempotent under convolution. Noting that $\eta(e) = 1$, the conditions of Theorem 3.9 hold as well, and G is thereby the Gramian of a binary Parseval Γ-frame. □

3.18. **Corollary** (Enumerating unitary equivalence classes of binary Parseval Γ-frames)**.** *Let the group Γ and the set Γ' be as above and define $k := |\Gamma|$, $k' := |\Gamma'|$, then the number of Gramians of unitarily inequivalent binary Parseval Γ-frames is $2^{k'-1} \le 2^{\frac{1}{2}(k-1)}$.*

Proof. The value $2^{|\Gamma'|-1}$ is the number of functions $\nu : \Gamma' \to \mathbb{Z}_2$ having the property that $\nu([e]) = 1$, thus enumerating the functions delineated in Theorem 3.17. The quantity $2^{\frac{1}{2}(k-1)}$ is achieved if $\Gamma = \mathbb{Z}_3^2$, as well as any other case such that $|[g]| = 2$ for all $g \in \Gamma\backslash\{e\}$. Exceeding this bound implies the existence of $h \in \Gamma\backslash\{e\}$ such that $|[h]| = 1$, which implies $h = h^2$. Since the only idempotent element of a group is the identity element, such an h does not exist. □

Results in [2] justify the use of Gramians as class representatives of binary Parseval frames. For a group of size k, the naive upper bound of 2^{k^2} binary matrices thereby drops to $2^{\frac{1}{2}(k^2-1)}$ symmetric binary matrices with at least one odd column. Theorem 3.1 in this paper puts our Gramians in $\mathbb{Z}_2[\{R_g\}]$, a set of order 2^k. In the case of abelian Γ with unique square roots, Corollary 3.18 gives the number of distinct Gramians of binary Parseval Γ-frames exactly as $2^{|\Gamma'|-1}$, where $|\Gamma'| \le \frac{1}{2}(k+1)$ is the quantity of symmetric doubling orbits of Γ. Thus, for a given abelian group Γ of odd order k, the unitary equivalence classes of binary Parseval frames are classified by computing the ranks of $2^{|\Gamma'|-1} \le 2^{\frac{1}{2}(k-1)}$ Gramians.

Writing the elements of $\mathbb{Z}_p^q$ as vectors suggests plotting subsets of the group for visualization purposes. Noting that inverse elements are obtained by multiplying by $-1 \mod p$, the fact that each symmetric doubling orbit is a collection of scalar multiples of a single element puts each of the points of a given symmetric doubling orbit on a line in $\mathbb{Z}_p^q$ containing the origin.

For many odd-prime/natural-number pairs p, q, in fact, the nontrivial symmetric doubling orbits of $\mathbb{Z}_p^q$ are each identical to that line, minus the origin; this property holds any time the multiplicative subgroup of $\mathbb{Z}_p$ generated by 2 is $\mathbb{Z}_p\backslash\{0\}$, as in the cases of $p \in \{3, 5, 11, 13\}$. It also occurs when $\left|\langle 2\rangle_{\mathbb{Z}_p}^{\times}\right| = \frac{1}{2}(p-1)$ and $(-1) \notin \langle 2\rangle_{\mathbb{Z}_p}^{\times}$, since the *symmetric* part completes the set; the smallest p for which this occurs is 7.

The work in this paper shows that any Gramian in the group algebra of the regular representations yields a binary Parseval $\mathbb{Z}_p^q$-frame for $q \in \mathbb{N}$ and odd prime p if the group elements represented in the sum are the union of a collection of these linear subspaces. However, the converse of this statement is not true, as each Mersenne prime (that is, having the form $2^n - 1$) greater than 7 provides a counter example, as does every Fermat prime (i.e., of the form $2^n + 1$) greater than 5. We illustrate this in Figure 2 with plots of the symmetric doubling orbits of $\mathbb{Z}_p^2$ for the smallest value that demonstrates this behavior, $p = 17$. Each plot shows a pair of orbits (one in red, one in black) that partition a line into two subsets. Any of the 2^{36} linear combinations of coefficients that are constant on these symmetric doubling orbits represents a distinct Gramian of a binary Parseval $\mathbb{Z}_{17}^2$-frame.

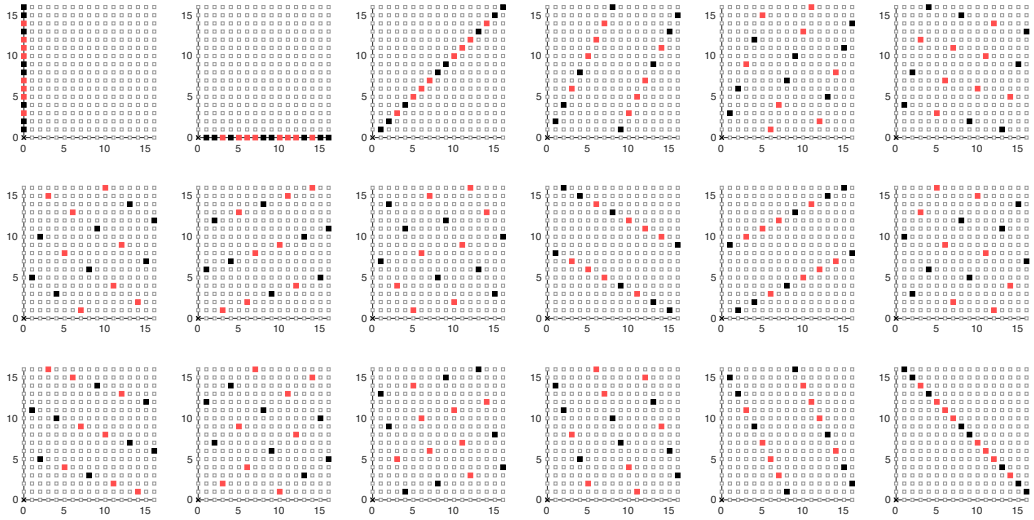

FIGURE 2. Symmetric doubling orbits of $\mathbb{Z}_{17}^2$, plotted in pairs that are complements in one-dimensional subspaces of $\mathbb{Z}_{17}^2$.

3.4. **An algorithm for classifying binary Parseval Γ-frames for abelian Γ of odd order.** For groups of smallest order, the unitary equivalence classes are manageable. However, even for $\mathbb{Z}_3^3$ the enumeration of Parseval frames becomes too tedious to do by hand. One reason is that group automorphisms may lead to different Gramians. The resulting set could be reduced to one representative without losing structural information. We recall that switching offers a coarser equivalence relation that is suitable for removing copies obtained by group automorphisms.

3.19. **Proposition** (Automorphisms on Γ and automorphic switching equivalence)**.** *Let Γ be a finite group with right regular repesentation matrices $\{R_g\}_{g\in\Gamma}$, and let $\mathcal{F} := \{f_g\}_{g\in\Gamma}$ be a binary Parseval Γ-frame with Gramian $G := \sum_g \eta(g)R_g$, then an operator H is the Gramian of a binary Parseval Γ-frame that is automorphically switching equivalent to $\mathcal{F}$ if and only if $H = \sum_g \eta(\sigma(g))R_g$ for some $\sigma \in \mathrm{Aut}(\Gamma)$.*

Proof. Let ρ be the group representation that induces $\mathcal{F}$; we first show that the composition of the coefficent function η with an automorphism induces the Gramian of an automorphically switching equivalent frame.

Let $\sigma \in \mathrm{Aut}(\Gamma)$ and define $H := \sum_g \eta(\sigma(g))R_g$. From $\rho \circ \sigma$ being a group homomorphism, it follows that $\{\rho_{\sigma(g)}f_e\}_{g\in\Gamma}$ is a binary Parseval Γ-frame that is automorphically switching equivalent to $\mathcal{F}$. By Corollary 3.3, the Gramian G' of $\{\rho_{\sigma(g)}f_e\}_{g\in\Gamma}$ admits a coefficient function ν such that $G' = \sum_g \nu(g)R_g$. It remains only to prove that $\nu = \eta \circ \sigma$, so that $G' = H$.

Recall from the proof of Theorem 3.1 that for $a, b \in \Gamma$, $G_{a,b} = \eta(a^{-1}b)$ and $G'_{a,b} = \nu(a^{-1}b)$. We conclude

$$\begin{aligned}\nu(a^{-1}b) &= \left\langle \rho_{\sigma(b)}f_e, \rho_{\sigma(a)}f_e \right\rangle \\ &= G_{\sigma(a),\sigma(b)} \\ &= \eta\left(\sigma(a)^{-1}\sigma(b)\right) \\ &= \eta\left(\sigma(a^{-1}b)\right),\end{aligned}$$

this last identity following from the fact that σ is an automorphism.

Conversely, suppose $\mathcal{F}' := \{f'_g\}_{g\in\Gamma}$ is a Γ-frame that is automorphically switching equivalent to a frame $\mathcal{F}$ induced by a representation ρ. Let the unitary U and $\sigma \in \mathrm{Aut}(\Gamma)$ give $f'_g = Uf_{\sigma(g)} = U\rho_{\sigma(g)}f_e$ for all $g \in \Gamma$. Let the Gramians of $\mathcal{F}$ and $\mathcal{F}'$ be $G = \sum_g \eta(g)R_g$ and $H = \sum_g \nu(g)R_g$, respectively. We equate

$$\begin{aligned}\nu(a^{-1}b) &= \left\langle f'_b, f'_a \right\rangle \\ &= \left\langle U\rho_{\sigma(b)}f_e, U\rho_{\sigma(a)}f_e \right\rangle \\ &= \left\langle \rho_{\sigma(b)}f_e, \rho_{\sigma(a)}f_e \right\rangle \\ &= \eta\left(\sigma(a^{-1}b)\right),\end{aligned}$$

and we see that $H = \sum_g \eta(\sigma(g))R_g$ has the claimed form. □

Next, we study how symmetric doubling orbits behave under automorphisms. Let $g, h \in \Gamma$ and $a \in \mathbb{N}$ such that $g = h^{2^a}$. Under an automorphism $\sigma \in \mathrm{Aut}(\Gamma)$, we identify $\sigma(g) = \sigma(h^{2^a}) = \sigma(h)^{2^a}$. Consequently, if $g \in [h]$, then $\sigma(g) \in [\sigma(h)]$. This means the action of σ on Γ passes to an action on the symmetric doubling orbits.

3.20. **Definition.** For a finite abelian group Γ partitioned into symmetric doubling orbits $\Gamma' = \{[g]\}_{[g]\in J}$ and an automorphism σ, we let $\tilde{\sigma}$ be the associated bijection on Γ' such that $\tilde{\sigma}([g]) = [\sigma(g)]$.

3.21. **Corollary** (Automorphisms on Γ and symmetric doubling orbits)**.** *Let Γ, $\{R_g\}$, $\mathcal{F}$, G and η be as above, and suppose Γ is abelian of odd order. Let Γ' be the symmetric doubling orbit partition of Γ, and $G = \sum_{[g]\in\Gamma'} \tilde{\eta}([g])R_{[g]}$ with $\tilde{\eta} : \Gamma' \to \mathbb{Z}_2$, then an operator H is the Gramian of a binary Parseval Γ-frame that is automorphically switching equivalent to $\mathcal{F}$ if and only if $H = \sum_{[g]\in\Gamma'} \tilde{\eta}(\tilde{\sigma}([g]))R_{[g]}$ for some $\sigma \in \mathrm{Aut}(\Gamma)$.*

Proof. Let $\sigma \in \mathrm{Aut}(\Gamma)$, and $\tilde{\sigma}$ the associated bijection on Γ'. Let $\eta(g) = \tilde{\eta}([g])$, for any $g \in \Gamma$. Consequently, $\sum_{[g]\in\Gamma'} \eta(\tilde{\sigma}([g]))R_{[g]} = \sum_{g\in\Gamma} \eta(\sigma(g))R_g$. Applying Proposition 3.19 completes the proof. □

By identifying Gramians in the group algebra with functions on the group, Corollary 3.3 reduces the search for Gram matrices associated with a given Γ to a search over a subset of $\mathbb{Z}_2$-valued coefficient functions on Γ; Theorem 3.9 specifies that subset. Proposition 3.19 allows a classification of the valid coefficient functions in terms of the automorphism group on Γ. Specialized results for abelian groups summarized in Corollary 3.21 provide us with a concrete method for obtaining

all binary Parseval group frames for abelian, odd-ordered groups. The following result provides theoretical justification for an algorithm guaranteed to produce a list of Gram matrices that contains exactly one representative from each automorphic switching equivalence class.

3.22. **Theorem.** *Given an odd-ordered abelian group Γ and a set $\mathcal{M}$ which generates the automorphism group of Γ, the algorithm described in the Practitioner's Guide below partitions the Gramians of binary Parseval Γ-frames under automorphic switching equivalence.*

Proof. Let Γ' be the symmetric doubling orbit partitioning of Γ. Corollary 3.21 reduces the theorem's partitioning to the comparison of symmetric doubling orbit coefficient functions. In particular, two binary Parseval Γ-frames are automorphically switching equivalent if and only if their Gramians $\sum_{[g]\in\Gamma'} \eta([g])R_{[g]}$ and $\sum_{[g]\in\Gamma'} \nu([g])R_{[g]}$ have the property that $\eta([g]) = \nu(\tilde{\sigma}([g]))$ for all $g \in \Gamma$ and $\tilde{\sigma}$ determined by the action of some $\sigma \in \mathrm{Aut}(\Gamma)$ on the symmetric doubling orbits. Given a coefficient function η, the algorithm does one of two things each time it accesses the multiplication table: it either identifies another coefficient function belonging to the same partition as η, or it terminates the search for coefficient functions in that partition. It thus remains to show that the algorithm exhausts the partition for any such η.

Let $\eta : \Gamma \to \mathbb{Z}_2$ be constant on symmetric doubling orbits. Enumerate $\mathcal{M} = \{M_i\}_{i=1}^N$ and define $M_0 := Id \in \mathrm{Aut}(\Gamma)$, and let $\Omega_0 := \{S_\eta\}$, where $S_\eta := \eta^{-1}(1)$. For $j \in \mathbb{N}$, define the set collection

$$\Omega_j := \{M_i(S) : i = 1, 2, \ldots, N \text{ and } S \in \Omega_{j-1}\}.$$

Note that $\Omega_{j-1} \subseteq \Omega_j$ for all $j \in \mathbb{N}$, since $S \in \Omega_{j-1}$ implies that $M_0(S) \in \Omega_j$. The algorithm produces each Ω_j sequentially and terminates the search for elements in η's partition at the end of identifying the elements of Ω_j if $\Omega_j = \Omega_{j-1}$. Now, if $\nu(g) = \eta(\sigma(g))$ for all $g \in \Gamma$ and some $\sigma \in \mathrm{Aut}(\Gamma)$, then there is a finite sequence $l_1, l_2, \ldots, l_k$ such that $\sigma = M_{l_k} M_{l_{k-1}} \cdots M_{l_1}$. It follows that the partition represpresented by η is the set Ω_L for some $L \in \mathbb{N}$; thus, the algorithm produces the partition of η if and only if there is an integer j_η such that

$$\Omega_1 \subsetneq \Omega_2 \subsetneq \cdots \subsetneq \Omega_{j_\eta} = \Omega_{j_\eta+i} \quad \text{for all} \quad i \in \mathbb{N}. \tag{7}$$

Let $j_0 \in \mathbb{N}$ be such that $\Omega_{j_0-1} = \Omega_{j_0}$; existence follows from the finiteness of $\mathbb{Z}_2[\Gamma]$. To prove that such j_η exists, it is enough to show that the equality $\Omega_{j_0} = \Omega_{j_0-1}$ implies $\Omega_{j_0} = \Omega_{j_0+i}$ for all $i \in \mathbb{N}$.

Let $S' \in \Omega_{j_0+1}$. By the inclusion $\Omega_{j_0} \subseteq \Omega_{j_0+1}$, it is left to show that $S' \in \Omega_{j_0}$. By the definition of Ω_{j_0+1}, we have $S' = M_i(S)$ for some $i \in \{0, 1, \ldots, N\}$ and some $S \in \Omega_{j_0} = \Omega_{j_0-1}$. Since $S \in \Omega_{j_0-1}$, it follows that $S' = M_i(S) \in \Omega_{j_0}$, and the proof is complete. □

A Practitioner's Guide to Generating Gramians of Binary Parseval Γ-Frames for abelian Γ of Odd Order

(1) Produce a set J so that $\{e\} \cup J$ indexes the symmetric doubling orbit partition Γ' of Γ.
(2) Select $\mathcal{M} \subset \mathrm{Aut}(\Gamma)$ to seed a multiplication table. If $\mathcal{M}$ generates $\mathrm{Aut}(\Gamma)$, this algorithm provides a partition of Γ-frames into automorphic switching equivalence classes. *(See Remark 3.23)*
(3) Produce the automorphism multiplication table containing a row for each $M_i \in \mathcal{M}$, with entry (i, j) giving $M_i([g_j])$.
(4) For each $m \leq \frac{1}{2}|\Gamma'|$, apply the method described in Example 3.24 to partition subsets of the collection $\{\bigcup_{g\in K}[g] : K \subset J, |K| = m\}$. For $m > \frac{1}{2}|\Gamma'|$, use the fact that for given indexing sets K, K', the sets $\bigcup_{g\in K}[g]$ and $\bigcup_{g\in K'}[g]$ represent the same class if and only if $\bigcup_{g\in J\setminus K}[g]$ and $\bigcup_{g\in J\setminus K'}[g]$ do.

3.23. *Remark* (Sampling $\mathrm{Aut}(\Gamma)$). Choosing $\mathcal{M} = \mathrm{Aut}(\Gamma)$ guarantees accurate partitioning, although $\mathrm{Aut}(\Gamma)$ may be difficult to calculate. Theorem 3.22 tells us that we can obtain this partitioning as long as $\mathcal{M}$ is a generating set for $\mathrm{Aut}(\Gamma)$. If $\mathcal{M}$ is not known to generate $\mathrm{Aut}(\Gamma)$, the

potential undersampling of the automorphism group may simply lead to the case that some classes are represented multiple times; the number of Gramians is still smaller than $2^{|\Gamma'|-1}$.

The following example demonstrates how the algorithm works.

3.24. *Example* (Classifying binary Parseval $\mathbb{Z}_3^2$-frames). Let the symmetric doubling orbit partition of $\mathbb{Z}_3^2$ given by set $\Gamma' = \{[g] : g \in \{e\} \cup J\}$ with $J := \{\binom{1}{0}, \binom{1}{1}, \binom{0}{1}, \binom{1}{2}\}$. We shall classify binary Parseval $\mathbb{Z}_3^2$-frames up to automorphic switching equivalence by identifying suitable Gramian representatives for each class. These Gramians have the form $I + \sum_{i=1}^{m} R_{[g_i]}$ for some $m \in \{0, 1, 2, 3, 4\}$ and distinct g_i's, and we proceed by considering one value of m at a time. We make use of the fact that for any finite vector space V, $\mathrm{Aut}(V) \equiv \mathrm{GL}(V)$.

m = 0 : The cases of $m = 0$ and $m = 4$ are trivial and listed in the summary.

m = 1 : The matrix $\left[\begin{smallmatrix}1 & 1\\ 1 & 0\end{smallmatrix}\right] \in \mathrm{GL}(\mathbb{Z}_3^2)$ gives

$$\left[\begin{smallmatrix}1 & 1\\ 1 & 0\end{smallmatrix}\right][\binom{1}{0}] = \{\left[\begin{smallmatrix}1 & 1\\ 1 & 0\end{smallmatrix}\right]\binom{1}{0}, \left[\begin{smallmatrix}1 & 1\\ 1 & 0\end{smallmatrix}\right]\binom{2}{0}\} = \{\binom{1}{1}, \binom{2}{2}\} = [\binom{1}{1}];$$

applying the preceding corollary, $I + R_{[\binom{1}{0}]}$ and $I + R_{[\binom{1}{1}]}$ are thus Gramians of automorphically switching equivalent binary Parseval $\mathbb{Z}_3^2$-frames. With this in mind, consider the multiplication table given in Table 1. The first row shows that for $g, h \in J$, $[g] = \left[\begin{smallmatrix}1 & 1\\ 1 & 0\end{smallmatrix}\right]^a [h]$ for some integer a.

	$[\binom{1}{0}]$	$[\binom{1}{1}]$	$[\binom{1}{2}]$	$[\binom{0}{1}]$
$\left[\begin{smallmatrix}1 & 1\\ 1 & 0\end{smallmatrix}\right]$	$[\binom{1}{1}]$	$[\binom{1}{2}]$	$[\binom{0}{1}]$	$[\binom{1}{0}]$
$\left[\begin{smallmatrix}2 & 1\\ 1 & 0\end{smallmatrix}\right]$	$[\binom{1}{2}]$	$[\binom{0}{1}]$	$[\binom{1}{1}]$	$[\binom{1}{0}]$
$\left[\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right]$	$[\binom{1}{0}]$	$[\binom{1}{2}]$	$[\binom{0}{1}]$	$[\binom{1}{1}]$

TABLE 1. Multiplication table for selected $M \in \mathrm{GL}(\mathbb{Z}_3^2)$

It follows that the four operators $I + R_{[g]}$ represent the same automorphic switching equivalence class.

m = 2 : Similarly, the first two entries in the first row give

$$\left[\begin{smallmatrix}1 & 1\\ 1 & 0\end{smallmatrix}\right]([\binom{1}{0}] \cup [\binom{1}{1}]) = \left[\begin{smallmatrix}1 & 1\\ 1 & 0\end{smallmatrix}\right][\binom{1}{0}] \cup \left[\begin{smallmatrix}1 & 1\\ 1 & 0\end{smallmatrix}\right][\binom{1}{1}] = [\binom{1}{1}] \cup [\binom{1}{2}],$$

implying

$$I + R_{[\binom{1}{0}]} + R_{[\binom{1}{1}]} \quad \text{and} \quad I + R_{[\binom{1}{1}]} + R_{[\binom{1}{2}]}$$

are representatives of the same equivalence class. Proceeding down the first two columns, we find that Gramians $I + R_{[\binom{1}{2}]} + R_{[\binom{0}{1}]}$ and $I + R_{[\binom{1}{0}]} + R_{[\binom{1}{2}]}$ represent that same class.

Reentering the table with the index pair $\binom{1}{2}, \binom{0}{1}$, we find the sets $[\binom{0}{1}] \cup [\binom{1}{0}]$ and $[\binom{0}{1}] \cup [\binom{1}{1}]$; it follows that each of the six distinct Gramians $I + \sum_{i=1}^{2} R_{[g_i]}$ represent the same class. *Note: If this step had not exhausted the "m = 2" case, we would continue to reenter the multiplication table with each new equivalent* $\bigcup g_i$ *until the class stops growing.*

m = 3 : We make use of set complements. Fixing $g, h \in J$, let a satisfy $[g] = \left[\begin{smallmatrix}1 & 1\\ 1 & 0\end{smallmatrix}\right]^a [h]$. It follows that $\bigcup_{g' \neq g} [g'] = \left[\begin{smallmatrix}1 & 1\\ 1 & 0\end{smallmatrix}\right]^a \bigcup_{h' \neq h} [h']$, since each $M \in \mathrm{GL}(\mathbb{Z}_3^2)$ is a bijection on $\bigcup_{g' \in J} [g']$. We conclude that each of the sums $I + \sum_{i=1}^{3} R_{[g_i]}$ represents the same equivalence class, since g and h were chosen arbitrarily.

Summary: The binary Parseval $\mathbb{Z}_3^2$-frames partition into five automorphic switching equivalence classes, with representative Gramians given by the identity operator, the 9×9 matrix of 1's, and three more representatives

$$I + R_{[\binom{1}{0}]}, \quad I + R_{[\binom{1}{0}]} + R_{[\binom{0}{1}]}, \text{ and } \quad I + R_{[\binom{1}{0}]} + R_{[\binom{1}{1}]} + R_{[\binom{0}{1}]}.$$

Hence, the nontrivial Gramians turn out to have ranks 3 ($m = 1$), 5 ($m = 2$), and 7 ($m = 3$). The Gram matrices belonging to a given rank are equivalent, so we partitioned the fourteen nontrivial Gramians $I + \sum_{i=1}^{m} R_{[g_i]}$ into three equivalence classes.

4. Binary Parseval group frames as codes

One motivating application of binary Parseval group frames is their use as codes. The range of the analysis operator Θ is the so-called code book in $\mathbb{Z}_2^k$. Each codeword y in this codebook is the image of a unique vector $x \in \mathbb{Z}_2^n$ which is obtained by $x = \Theta^* y$.

When $k > n$, the redundancy introduced by the embedding Θ makes it possible to accurately recover x from a *corrupted* codeword $\tilde{y} := E\Theta x + \epsilon$, provided the diagonal error matrix E and error vector ϵ are known to meet certain specified conditions.

For our binary case, we consider two types of errors: *erasures* ($\tilde{y} = E\Theta x$, $E_{i,i} \in \{0, 1\}$) and *bit-flips* ($\tilde{y} = \Theta x + \epsilon$, $\epsilon \in \mathbb{Z}_2^J$). We say that a binary Parseval frame $\mathcal{F}$ is *robust to m erasures* if for every diagonal binary matrix E having at most m zeros on the diagonal, the operator $E\Theta$ admits a left inverse. This is equivalent to the condition that the Hamming distance between any two vectors in the image of Θ (or, equivalently, of the Gramian of $\mathcal{F}$) is at least $m + 1$, since any pair of vectors that differ in only m entries are indistinguishable if those entries are "erased." By the linearity of Θ, this is also equivalent to the condition that each nonzero vector in $\Theta\mathbb{Z}_2^n$ has weight exceeding m.

On the other hand, we say that $\mathcal{F}$ is *robust to m bit-flips* if $\|\Theta x_1 - \Theta x_2\|_0 \geq 2m + 1$ for all $x_1, x_2 \in \mathbb{Z}_2^n$, $x_1 \neq x_2$. This notion of "robustness to error" implies the ability to identify each vector in the set $B := \{\Theta x + \epsilon : x \in \mathbb{Z}_2^n, \|\epsilon\|_0 \leq m\}$ as the (corrupted) image of a unique vector in $\mathbb{Z}_2^n$. Note that if $\|\Theta x_1 - \Theta x_2\|_0 = 2m$ for some pair $x_1, x_2 \in \mathbb{Z}_2^n$, then there exist m-weighted error vectors ϵ_1 and ϵ_2 such that $\Theta x_1 + \epsilon_1 = \Theta x_2 + \epsilon_2$. Now suppose that for any distinct $y_1, y_2 \in \Theta\mathbb{Z}_2^n$, we have $\|y_1 - y_2\|_0 \geq 2m + 1$, and let $\tilde{y} \in B$; by the triangle inequality, there is exactly one point $y \in \Theta\mathbb{Z}_2^n$ such that $\|y - \tilde{y}\|_0 \leq m$. Thus, we may recover the intended signal y by identifying the nearest point in $\Theta\mathbb{Z}_2^n$ to $\tilde{y}$, and recovery of $x = \Theta^* y$ follows.

Again appealing to the linearity of Θ, both robustness conditions are expressed in terms of the minimum weight among nonzero vectors in the range of Θ. For Parseval frames, the range of the analysis operator coincides with that of the Gramian, so it can be stated equivalently in terms of the range of the Gramian.

4.1. **Definition** (Code weight of a Gramian or frame)**.** Given an operator $G : \mathbb{Z}_2^J \to \mathbb{Z}_2^J$, the *code weight* of G is the value $\min_{y \in G(\mathbb{Z}_2^J) \setminus \{0\}} \|y\|_0$.

In the following section, we compare $\mathbb{Z}_p^q$-frames with $\mathbb{Z}_{p^q}$-frames. The final major result in this paper is a proof that every binary Parseval $\mathbb{Z}_{p^q}$-frame is switching equivalent to a $\mathbb{Z}_p^q$-frame. We also include a number of examples in which the classes of Z_{p^q}-frames are mapped to their switching equivalent $\mathbb{Z}_p^q$ frames for select p's and q's and show that in addition to subsuming binary Parseval $\mathbb{Z}_{p^q}$-frames, there are examples of $\mathbb{Z}_p^q$-frames that outperform them as codes.

4.1. **Comparing frames generated with $\mathbb{Z}_{p^q}$ vs. $\mathbb{Z}_p^q$.** Fix $m \in \mathbb{N}$, and let $\mathcal{F}_1$ and $\mathcal{F}_2$ be switching equivalent binary Parseval frames. Theorem 4.9 in [2] establishes that this equivalence implies that $\mathcal{F}_1$ is robust to m erasures if and only if $\mathcal{F}_2$ is. By the Gramian code weight characterization of robustness to each type of error, it follows that $\mathcal{F}_1$ is robust to m bit-flips if and only if $\mathcal{F}_2$ is. Theorem 4.11 in [5] characterizes switching equivalence between binary Parseval frames as permutation equivalence between their Gramians G_1 and G_2:

$$\mathcal{F}_1 \cong_{\text{sw}} \mathcal{F}_2 \quad \text{if and only if} \quad G_1 = P^* G_2 P \text{ for some permutation matrix } P.$$

Hence, for the purposes of evaluating binary Parseval group frames as codes, whether we are concerned about erasures or bit-flips, we may restrict our attention to permutation equivalence classes of the Gramians of such frames.

Applying the techniques in this paper, we have classified binary Parseval group frames for each of the groups below, using Gramians as class representatives. Recalling that the quantity of vectors in a group frame is given by the size of the group, and that the rank of the Gramian is the dimension of the inducing frame, we can directly compare the performance of several frames as error-correcting codes. To facilitate comparing $\mathbb{Z}_{p^q}$ and $\mathbb{Z}_p^q$ for a given pair p, q, we combine details for the two groups in a single table; in each of the comparisons below, $\mathbb{Z}_p^q$-frames perform at least as well as $\mathbb{Z}_{p^q}$-frames, and they often outperform their $\mathbb{Z}_{p^q}$ counterparts. In fact, the exhaustive search of best performing codes associated with binary Parseval frames generated with $\mathbb{Z}_p^q$ is guaranteed to be at least as good as the best codes generated with $\mathbb{Z}_{p^q}$, as shown in Theorem 4.6 below.

We now provide a sequence of results which culmintate in the proof of Theorem 4.6, which states that, given an odd prime p and $q \in \mathbb{N}$, any binary Parseval $\mathbb{Z}_{p^q}$-frame is switching equivalent a binary Parseval $\mathbb{Z}_p^q$-frame. Practically, this reduces to showing that the Gramian of a binary Parseval $\mathbb{Z}_{p^q}$-frame satisfies the Gram characterization for a $\mathbb{Z}_p^q$-frame for some reindexing. We accomplish this by showing that the symmetric doubling orbits of $\mathbb{Z}_{p^q}$ partition those of $\mathbb{Z}_p^q$, in the sense that for each $n \in \mathbb{Z}_{p^q}$, the matrix $R_{[n]}$ can be written as the sum of matrices in $\{R_{[g]}\}_{g \in \mathbb{Z}_p^q}$.

The map which produces this reindexing is the inverse of the function $\phi : \mathbb{Z}_p^q \to \mathbb{Z}_{p^q}$ given by

$$\phi(g) := \sum_{i=1}^{q} p^{i-1} g_i, \tag{8}$$

where the arithmetic is carried out in $\mathbb{Z}_{p^q}$; this mapping is akin to converting from numbers written in base p. It is worth noting that for a given $i \in \{1, 2, \ldots, q-1\}$ and $g \in \mathbb{Z}_p^q$, we have that p^i divides $\phi(g)$ if and only if the first i entries of g are zero; if p^i divides $\phi(g)$ and p^{i+1} does not, then the j-th entry of g, denoted g_j, is nonzero.

We recall a few fundamental properties of finite multiplicative groups in the context of this work. For a given $n \in \mathbb{N}$, we may consider $\mathbb{Z}_n$ as the ring $(\mathbb{Z}_n, \cdot, +)$, in which case the subset of elements having multiplicative inverses forms the multiplicative group $\mathbb{Z}_n^\times := (\mathbb{Z}/n\mathbb{Z})^\times$. The elements of $\mathbb{Z}_n$ that provide elements in $\mathbb{Z}_n^\times$ are those coprime with n.

Here we shall denote the multiplicative subgroup of $\mathbb{Z}_n^\times$ generated by element k as $\langle k \rangle_n^\times := \langle k \rangle_{\mathbb{Z}_n}^\times$.

4.2. **Proposition.** *Let $p, q, k \in \mathbb{N}$ with p prime and $1 < k < p$. Then $\left|\langle k \rangle_{p^q}^\times\right| = p^{q-1} \left|\langle k \rangle_p^\times\right|$ and $x \in \langle k \rangle_{p^q}^\times$ if and only if $x (\mathrm{mod}\, p) \in \langle k \rangle_p^\times$.*

Proof. Note that $\mathbb{Z}_p^\times \cong \mathbb{Z}_{p-1}$, since each nonzero element of $\mathbb{Z}_p$ is coprime with p. Recalling that a finite cyclic group of order mn is isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n$ if m and n are coprime, we have that

$$\mathbb{Z}_{p^q}^\times \cong \mathbb{Z}_{p^{q-1}(p-1)} \cong \mathbb{Z}_{p^{q-1}} \times \mathbb{Z}_{p-1} \cong \mathbb{Z}_{p^{q-1}} \times \mathbb{Z}_p^\times.$$

It follows that $\left|\mathbb{Z}_p^\times\right| = p - 1$ and $\left|\mathbb{Z}_{p^q}^\times\right| = p^{q-1}(p-1)$. We consider now the subgroups $\langle k \rangle_p^\times \leq \mathbb{Z}_p^\times$ and $\langle k \rangle_{p^q}^\times \leq \mathbb{Z}_{p^q}^\times$.

Note that $x \in \langle k \rangle_{p^q}^\times$ implies that $x (\mathrm{mod}\, p) \in \langle k \rangle_p^\times$, so that each element in $\langle k \rangle_{p^q}^\times$ may be written in the form $mp + t$ for some $m \in \{0, 1, \ldots, p^{q-1} - 1\}$ and some $t \in \langle k \rangle_p^\times$ considered as an element of $\mathbb{Z}$. It follows that $\left|\langle k \rangle_{p^q}^\times\right| \leq p^{q-1} \left|\langle k \rangle_p^\times\right|$. We shall show equality holds by demonstrating that the reverse inequality holds; the resulting equality will imply that *every* element of $\mathbb{Z}_{p^q}^\times$ of the form $mp + t$ as above is an element of $\langle k \rangle_{p^q}^\times$, completing the characterization $\langle k \rangle_p^\times = \{x (\mathrm{mod}\, p) \mid x \in \langle k \rangle_p^\times\}$.

Let

$$\begin{aligned} \gamma_q : \langle k \rangle_{p^q}^\times &\to \mathbb{Z}_{p^{q-1}} \times \langle k \rangle_p^\times \\ k^j &\mapsto j \times k^j, \end{aligned}$$

where we consider $\mathbb{Z}_{p^{q-1}} \times \langle k\rangle_p^\times$ as a group in the natural way, inheriting its group operation componentwise. For $i, j \in \mathbb{N}$, we have

$$\gamma_q(k^i k^j) = \gamma_q(k^{i+j}) = (i+j, k^{i+j}) = (i, k^i)(j, k^j) = \gamma_q(k^i)\gamma_q(k^j),$$

and thus γ_q is a group homomorphism. Since the orders of the cyclic groups $\mathbb{Z}_{p^{q-1}}$ and $\langle k\rangle_p^\times$ are coprime, it follows that γ_q exhausts its range and that $\left|\gamma_q(\langle k\rangle_{p^q}^\times)\right| = \left|\mathbb{Z}_{p^{q-1}}\right|\left|\langle k\rangle_p^\times\right|$. This implies $\left|\langle k\rangle_{p^q}^\times\right| \geq p^{q-1}\left|\langle k\rangle_p^\times\right|$. We conclude that $\left|\langle k\rangle_{p^q}^\times\right| = p^{q-1}\left|\langle k\rangle_p^\times\right|$ and that $x \in \langle k\rangle_{p^q}^\times$ if and only if $x \pmod p \in \langle k\rangle_p^\times$. □

4.3. **Corollary.** *Let $p, q, k \in \mathbb{N}$ with p prime and $1 < k < p$. Then for each $y \in \mathbb{Z}_{p^q}^\times$,*

$$\left|y\langle k\rangle_{p^q}^\times\right| = p^{q-1}\left|\langle k\rangle_p^\times\right|$$

and $x \in y\langle k\rangle_{p^q}^\times$ if and only if $x \pmod p \in y\langle k\rangle_p^\times \pmod p$.

Proof. Fix $y \in \mathbb{Z}_{p^q}^\times$. Since the cosets of a subgroup partition a group into equal sized sets, the preceding proposition yields $\left|y\langle k\rangle_{p^q}^\times\right| = \left|\langle k\rangle_{p^q}^\times\right| = p^{q-1}\left|\langle k\rangle_p^\times\right|$.

Now, if $x \in y\langle k\rangle_{p^q}^\times$, then $x \pmod p \in y\langle k\rangle_p^\times$. Since $\left|\{x \in \mathbb{Z}_{p^q}^\times : x \pmod p \in y\langle k\rangle_p^\times\}\right| = p^{q-1}\left|\langle k\rangle_p^\times\right|$, It follows that

$$y\langle k\rangle_{p^q}^\times = \{x \in \mathbb{Z}_{p^q}^\times : x \pmod p \in y\langle k\rangle_p^\times\},$$

and the proof is complete. □

4.4. **Theorem.** *Given $p, q, k \in \mathbb{N}$ with p prime and $1 < k < p$, let $x, y \in \mathbb{Z}_{p^q}$ and define nonnegative integers x', y', j_x, j_y such that $x = x'p^{j_x}$, $y = y'p^{j_y}$, and p divides neither x' nor y'. Then $x \in y\langle k\rangle_{p^q}^\times$ if and only if $j_x = j_y$ and $x' \pmod p \in y'\langle k\rangle_p^\times \pmod p$.*

Proof. Suppose $x \in y\langle k\rangle_{p^q}^\times$, so that $x'p^{j_x} = k^l y' p^{j_y}$ for some $l \in \mathbb{N}$. Then $j_x = j_y$, since k and p are coprime and p is coprime with each of x' and y'. Next, set $r := j_x = j_y$ and write

$$x'p^r \equiv k^l y' p^r \pmod{p^q}. \tag{9}$$

Since x and y may be seen as elements in $p^r\mathbb{Z}_{p^p} \cong \mathbb{Z}_{p^{q-r}}$, we may also identify x' and y' as elements of $\mathbb{Z}_{p^{q-r}}^\times \leq Z_{p^{q-r}}$ and note that congruence (9) implies

$$x' \equiv k^l y' \pmod{p^{q-r}}.$$

Then, using $y' \in \mathbb{Z}_{p^{q-r}}^\times$, Corollary 4.3 yields $x' \pmod p \in y'\langle k\rangle_p^\times \pmod p$.

Conversely, assume $j_x = j_y =: r$ and $x' \pmod p \in y'\langle k\rangle_p^\times \pmod p$. Then the conditions of Corollary 4.3 are met for $x, y \in \mathbb{Z}_{p^{q-r}}^\times$ and $x' \equiv k^{l'} y' \pmod{p^{q-r}}$ for some $l' \in \mathbb{N}$. Embedding $y'\langle k\rangle_{p^{q-r}}^\times$ into Z_{p^q} by $g \mapsto p^r g$ for $g \in y'\langle k\rangle_{p^{q-r}}^\times$, we have that $x = x'p^r \equiv 2^{l'} y' p^r \pmod{p^q} = 2^{l'} y$. □

The following lemma makes precise the claim that the map ϕ given by (8) maps the doubling orbits of $\mathbb{Z}_p^q$ into those of $\mathbb{Z}_{p^q}$.

4.5. **Lemma.** *Given $p, q \in \mathbb{N}$ with p an odd prime, let $x \in \mathbb{Z}_{p^q}$. If $g \in \phi^{-1}(x\langle 2\rangle_{p^q}^\times)$, then for $h \in \mathbb{Z}_p^q$, we have that $\phi(g\langle 2\rangle_p^\times + h) \subseteq x\langle 2\rangle_{p^q}^\times + \phi(h)$. As a consequence, $\phi(\phi^{-1}(x\langle 2\rangle_{p^q}^\times) + h) = x\langle 2\rangle_{p^q}^\times + \phi(h)$.*

Proof. We begin by proving the lemma for the case that $h = 0$. Let x, p and q be as in the hypothesis, and let $g = \phi^{-1}(x)$. Since $\langle 2\rangle_p^\times$ is cyclic, it suffices to show that for each $g' \in \phi^{-1}(x\langle 2\rangle_{p^q}^\times)$ there exists $k \in \mathbb{N}$ such that $\phi(2g') = 2^k x$; since $\langle 2\rangle_{p^q}^\times$ is cyclic, it suffices to demonstrate this for the case $g' = g$.

If $x = 0$ then $g = (0)_{i=1}^q$, and the claim is shown; assume, then, that $x \neq 0$ and define nonnegative integers x' and r such that $x = x'p^r$ and p does not divide x'. Note that r gives the quantity of leading zeros in the sequence $(g_i)_{i=1}^q$.

Expressing this equality in terms of the definition of ϕ,

$$\sum_{i=1}^{q} p^{i-1}(2g_i \,(\mathrm{mod}\, p)) \equiv 2^k x \,(\mathrm{mod}\, p^q),$$

where $2g_i \,(\mathrm{mod}\, p)$ is considered as an element of $\mathbb{Z}$. For each $i \in \{1, 2, \ldots, q\}$, we may express $2g_i \,(\mathrm{mod}\, p)$ as $2g_i - \delta_i p$ for some $\delta_i \in \{0, 1\}$, since the value is either $2g_i$ or $2g_i - p$. Since $i \leq r$ implies $g_i = 0$, it follows that $\delta_i = 0$ for such i. Thus

$$\begin{aligned}
\phi(2g) &\equiv \sum_{i=1}^{q} p^{i-1}(2g_i - \delta_i p) \pmod{p^q} \\
&\equiv 2\sum_{i=1}^{q} p^{i-1} g_i - \sum_{i=1}^{q} \delta_i p^i \pmod{p^q} \\
&\equiv 2\phi(g) - \sum_{i=r+1}^{q} \delta_i p^i \pmod{p^q}.
\end{aligned}$$

It follows that $2\phi(g) - \sum_{i=r+1}^{q} \delta_i p^i \equiv 2\phi(g) \,(\mathrm{mod}\, p^r)$. The conditions given in Theorem 4.4 are thus satisfied for x and $\phi(2g)$, implying $\phi(2g) \in 2\phi(g)\langle 2\rangle_{p^q}^{\times} = 2x\langle 2\rangle_{p^q}^{\times} = x\langle 2\rangle_{p^q}^{\times}$. We conclude that $\phi(2^j g) \in x\langle 2\rangle_{p^q}^{\times}$ for all $j \in \mathbb{N}$.

We now consider the general case, letting $h \in \mathbb{Z}_p^q$. Again, since $\langle 2\rangle_p^{\times}$ and $\langle 2\rangle_{p^q}^{\times}$ are cyclic, we may assume that $g = \phi^{-1}(x)$. We must show that $\phi(g + h) = 2^j x + \phi(h)$ for some j. Similar to the $h = 0$ case, we define δ_i' so that $g_i + h_i - \delta_i' p \in \{0, 1, \ldots, p-1\}$ for each $i \in \{1, 2, \ldots, q\}$. Recalling that the value r gives the number of leading zeros of g, we note that $\delta_i = \delta_i' = 0$ for $i \leq r$. Then

$$\begin{aligned}
\phi(g + h) &\equiv \sum_{i=1}^{q} p^{i-1}(g_i + h_i - \delta_i' p) \pmod{p^q} \\
&\equiv \phi(g) + \phi(h) - \sum_{i=1}^{q} \delta_i' p^i \pmod{p^q} \\
&\equiv x - \sum_{i=r+1}^{q} \delta_i' p^i + \phi(h) \pmod{p^q} \\
&\in x\langle 2\rangle_{p^q}^{\times} + \phi(h),
\end{aligned}$$

by Theorem 4.4, since $x - \sum_{i=r+1}^{q} \delta_i' p^i \equiv x \,(\mathrm{mod}\, p^r)$. We conclude that $\phi(g\langle 2\rangle_p^{\times} + h) \subseteq x\langle 2\rangle_{p^q}^{\times} + \phi(h)$ for all $g \in \phi^{-1}(x\langle 2\rangle_{p^q}^{\times})$ and $h \in \mathbb{Z}_p^q$.

It follows that $\phi(\phi^{-1}(x\langle 2\rangle_{p^q}^{\times}) + h) \subseteq x\langle 2\rangle_{p^q}^{\times} + \phi(h)$. Set equality follows from the fact that ϕ is a bijection, since both sides of the inclusion have the same number of elements. □

We are ready to prove the section's main result. We wish to show that for each Gramian of a binary Parseval $\mathbb{Z}_{p^q}$-frame, the corresponding Gramian indexed by $\mathbb{Z}_p^q$, as obtained from the reindexing given by ϕ^{-1}, is in the group algebra $\mathbb{Z}_2[\mathbb{Z}_p^q]$; this is sufficient to show that the underlying frame is a binary Parseval $\mathbb{Z}_p^q$-frame, since the Gramian retains idempotence, symmetry and the weights of range vectors under switching.

4.6. **Theorem.** *Let $p, q \in \mathbb{N}$ with p an odd prime and define $\phi : \mathbb{Z}_p^q \to \mathbb{Z}_{p^q}$ by $\phi(g) := \sum_{i=1}^{q} p^{i-1} g_i$, carrying out the arithmetic in $\mathbb{Z}_{p^q}$. If $\mathcal{F} = \{f_x\}_{x \in \mathbb{Z}_{p^q}}$ is a binary Parseval $\mathbb{Z}_{p^q}$-frame for $\mathbb{Z}_2^n$, then $\mathcal{F}' := \{f_{\phi^{-1}(x)}\}_{x \in \mathbb{Z}_{p^q}}$ is a binary Parseval $\mathbb{Z}_p^q$-frame.*

Proof. Let $\mathcal{F} = \{f_x\}_{x \in \mathbb{Z}_{p^q}}$ be a binary Parseval $\mathbb{Z}_{p^q}$-frame for $\mathbb{Z}_2^n$. Denote the frame's analysis matrix and Gramian by $\Theta_{\mathcal{F}}$ and G, respectively, and let $\Theta_{\mathcal{F}'}$ and G' denote those of $\mathcal{F}'$. Since G

and G' are switching equivalent, G' inherits symmetry, idempotence and column weights from G. By the characterization of binary Parseval group frames given by Theorem 3.4, it is then left to show that G' is a element of the group algebra of the right regular representation of $\mathbb{Z}_p^q$, denoted $\mathbb{Z}_2[\{R'_g\}]$.

Let $R := \{R_x\}_{x\in\mathbb{Z}_{p^q}}$ be the right regular representation of $\mathbb{Z}_{p^q}$ and let η be the binary coefficient function such that $G = \sum_{x\in\mathbb{Z}_{p^q}} \eta(x)R_x$, as guaranteed by Theorem 3.9. Since $\mathbb{Z}_{p^q}$ is an odd-ordered abelian group and η is idempotent under convolution, Theorem 3.13 provides that η is constant on cosets of the the multiplicative subgroup $\langle 2\rangle_{p^q}^{\times}$. We shall demonstrate that ϕ induces an isomorphism between the sets $\{\sum_{y\in x\langle 2\rangle_{p^q}^{\times}} R_y\}_{x\in\mathbb{Z}_{p^q}}$ and $\{\sum_{y\in x\langle 2\rangle_{p^q}^{\times}} R'_{\phi^{-1}(y)}\}_{x\in\mathbb{Z}_{p^q}}$,

Let $\Phi : \mathbb{Z}_2^{Z_p^q} \to \mathbb{Z}_2^{Z_{p^q}}$ be defined on standard basis elements by $\Phi e'_g = e_{\phi(g)}$, where we use the $'$ (prime) to distinguish basis elements of the domain from those in the range. We wish to show that for each $x, z \in \mathbb{Z}_{p^q}$, the following holds:

$$\sum_{y\in x\langle 2\rangle_{p^q}^{\times}} R_y e_z = \Phi\Big(\sum_{y\in x\langle 2\rangle_{p^q}^{\times}} R'_{\phi^{-1}(y)} e'_{\phi^{-1}(z)}\Big). \tag{10}$$

As described in Section 2.4, we may explicitly express the image a function φ under R_y by $R_y\varphi : z \mapsto \varphi(y+z)$, and equation (10) becomes

$$\begin{aligned}\sum_{y\in x\langle 2\rangle_{p^q}^{\times}} e_{y+z} &= \Phi\Big(\sum_{y\in x\langle 2\rangle_{p^q}^{\times}} e'_{\phi^{-1}(y)+\phi^{-1}(z)}\Big)\\ &= \sum_{y\in x\langle 2\rangle_{p^q}^{\times}} e'_{\phi(\phi^{-1}(y)+\phi^{-1}(z))}.\end{aligned}$$

Thus, we are left to show that $x\langle 2\rangle_{p^q}^{\times} + z = \phi(\phi^{-1}(x\langle 2\rangle_{p^q}^{\times}) + \phi^{-1}(z))$ for any $x, z \in \mathbb{Z}_{p^q}$. Taking $h := \phi^{-1}(z)$, this is exactly the content of Lemma 4.5, and the proof is complete. □

We illustrate this statement with some examples. It is worth noting ahead of the examples that there is an important distinction between the symmetric doubling orbit partitionings of $\mathbb{Z}_p^q$ and $\mathbb{Z}_{p^q}$. For an odd prime p, it is a simple exercise to show that each $[x]$ in $\mathbb{Z}_p^q$ that is not $[e]$ has the same order as the symmetric doubling orbit of 1 in $\mathbb{Z}_p$. In contrast, according to Theorem 4.4, $\mathbb{Z}_{p^q}$ partitions into kq nontrivial orbits for some $k \in \mathbb{N}$, k of each of q different sizes. Since automorphisms preserve symmetric doubling orbits (Proposition 3.19), they also preserve orbit size; it follows that the computational savings offered by applying Corollary 3.21 as in Example 3.24 do not apply or are significantly reduced when the group under consideration is $\mathbb{Z}_{p^q}$. In fact, for the values of p and q we explore here, the 2^q binary Parseval $\mathbb{Z}_{p^q}$-frame unitary equivalence classes promised by Corollary 3.18 coincide with automorphic switching equivalence classes. As we note in our closing remarks regarding $\mathbb{Z}_{17^q}$, this does not hold in general. Of course, the number of symmetric doubling orbits of $\mathbb{Z}_{p^q}$ grows linearly in q and may be considered as subsets of symmetric doubling orbits of Z_p^q (Theorem 4.6), whose number grows exponentially as $(p^q-1)/\left|[g]\right|$ for any $g \in \mathbb{Z}_p^q\backslash\{e\}$.

The next step is to compute the code weight of each of the Gramians. We pause to reflect on the computational savings made available by the methods developed thus far. Results in [2] justify the use of Gramians as class representatives of binary Parseval frames as codes; for a group of size k, the naive upper bound of 2^{k^2} binary matrices thereby drops to $2^{\frac{1}{2}k(k-1)}(2^k-1)$ symmetric binary matrices with at least one odd column. Theorem 3.1 in this paper puts our Gramians in $\mathbb{Z}_2[\{R_g\}]$, a set whose size is of order 2^k. In the case of abelian Γ with unique square roots, Corollary 3.18 gives the number of Gramians of binary Parseval Γ-frames exactly as $2^{|\Gamma'|-1}$, where $|\Gamma'| \leq \frac{1}{2}(k+1)$ is the quantity of symmetric doubling orbits of Γ. Thus, for a given abelian group Γ of odd order

k, we must process no more than $2^{|\Gamma'|-1} \leq 2^{\frac{1}{2}(k-1)}$ Gramians to determine code weights, and these matrices can be computed directly. We may process even fewer Gramians if we reduce the set to representatives of automorphic switching equivalence classes. Note that in determining the code weight of a $k \times k$ Gramian G, the $2^{\operatorname{rank}(G)}$ vectors in the operator's range may be obtained by taking all linear combinations of up to $\operatorname{rank}(G)$ columns of G, for a total $\sum_{i=1}^{\operatorname{rank}(G)} \binom{k}{i}$ operations; comparing this combinatorial problem with the algorithm above, it is evident that computational savings result from any reduction in the quantity of Gramians we are to process.

Let us first consider the work for $\mathbb{Z}_3^2$ and $\mathbb{Z}_3^3$ to illustrate this.

4.7. *Example.* The nontrivial Gramians in Example 3.24 turn out to have ranks 3 ($m = 1$), 5 ($m = 2$), and 7 ($m = 3$), and thus require $\binom{9}{3}$, $\binom{9}{5}$, and $\binom{9}{7}$ computations to exhaust linear combinations of columns as described. For the cost of producing a 3×4 multiplication table and a computing a handful of table look-ups and comparisons, we partitioned the fourteen nontrivial Gramians $I + \sum_{i=1}^{m} R_{[g_i]}$ into three classes; the return on that cost in the form of having fewer Gramians to weight-check was the reduction from $4{\cdot}\binom{9}{3}+6{\cdot}\binom{9}{5}+4{\cdot}\binom{9}{7} = 1236$ computations to $\binom{9}{3}+\binom{9}{5}+\binom{9}{7} = 246$.

The group $\mathbb{Z}_3^3$ has 14 symmetric doubling orbits, including $[e]$. The characterization of automorphic switching equivalence classes given by Corollary 3.21, provides that the 2^{13} unique Gramians of binary Parseval $\mathbb{Z}_3^3$-frames reduce to only thirty representatives. The resulting computational savings are substantial even before taking into account the cost of finding code weights, which has grown to $\sum_{i=1}^{\operatorname{rank}(G)} \binom{27}{i}$ operations per Gramian.

4.1.1. *Format of comparison tables.* Each comparison table contains representatives of switching equivalence classes of binary Parseval Γ-frames for each of the groups we compare. For each such class, we provide the rank and code weight of the representing Gramian. After the first table, we exclude the trivial Gramians given by the identity and the matrix of all ones; the Gramians themselves are encoded as indexing elements of their symmetric doubling orbit summands. Whenever a class in $\mathbb{Z}_{p^q}$ matches the performance of a class in $\mathbb{Z}_p^q$, the two classes are described in the same row of the associated table. In many such cases, the two classes represent switching equivalent frames.

In the comparison of $\mathbb{Z}_3^2$ and $\mathbb{Z}_9$, for example, the Gramians given by $G_1 = \sum_{g\in J_1} R_{[g]}$ with $J_1 = \{\binom{0}{0}, \binom{1}{0}, \binom{1}{1}, \binom{0}{1}\} \subset \mathbb{Z}_3^2$ and $G_2 = \sum_{g\in J_2} R_{[g]}$ with $J_2 = \{0, 1\} \subset \mathbb{Z}_9$ each have rank 7 and code weight 2, and thus are listed in the same row.

4.8. *Example* ($\mathbb{Z}_9$ vs. $\mathbb{Z}_3^2$). The symmetric doubling orbit partitioning of $\mathbb{Z}_9$ consists of $[0]$, $[3] = \{3, 6\}$, and $[1] = \{1, 2, 4, 5, 7, 8\}$. In this case, each of the four binary Parseval $\mathbb{Z}_9$-frames is switching equivalent to one of the five binary Parseval $\mathbb{Z}_3^2$-frames delineated in Example 3.24. Apart from the trivial cases of the Gramian being the identity matrix or the matrix of all 1's, this correspondence

$$I + R_{[\binom{1}{0}]} = I + R_{[3]} \text{ and } \quad I + R_{[\binom{1}{0}]} + R_{[\binom{1}{1}]} + R_{[\binom{0}{1}]} = I + R_{[1]},$$

assumes an appropriate identification of group elements. Table 2 provides the implications for the performance of codes.

Gram rank	Code weight	$J \subset \mathbb{Z}_3^2$	$J \subset \mathbb{Z}_9$
1	1	$\{\binom{0}{0}, \binom{1}{0}, \binom{1}{1}, \binom{0}{1}, \binom{1}{2}\}$	$\{0, 1, 3\}$
3	3	$\{\binom{0}{0}, \binom{1}{0}\}$	$\{0, 3\}$
5	3	$\{\binom{0}{0}, \binom{1}{0}, \binom{1}{1}\}$	–
7	2	$\{\binom{0}{0}, \binom{1}{0}, \binom{1}{1}, \binom{0}{1}\}$	$\{0, 1\}$
9	1	$\{\binom{0}{0}\}$	$\{0\}$

TABLE 2. Comparing Parseval frames with Gramians $G = \sum_{g\in J} R_{[g]}$ obtained from groups $\mathbb{Z}_3^2$ and $\mathbb{Z}_9$, together with their code weights. See Example 4.8 for details.

Gram rank	Code weight	$J \subset \mathbb{Z}_3^3$	$J \subset \mathbb{Z}_{27}$
3	9	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0, \binom{0}{1}_1, \binom{0}{1}_2\right\}$	{0,3,9}
5	9	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0, \binom{1}{0}_0, \binom{1}{0}_1, \binom{1}{0}_2, \binom{1}{1}_0, \binom{1}{2}_0\right\}$	–
7	6	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_1, \binom{0}{1}_2, \binom{1}{0}_0, \binom{1}{0}_1, \binom{1}{0}_2, \binom{1}{1}_0, \binom{1}{1}_1, \binom{1}{2}_0, \binom{1}{2}_1\right\}$	{0,1,9}
7	9	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0, \binom{0}{1}_2, \binom{1}{0}_1, \binom{1}{1}_0, \binom{1}{1}_1\right\}$	–
9	3	$\left\{\binom{0}{0}_0, \binom{0}{0}_1\right\}$	{0,9}
9	6	$\left\{\binom{0}{0}_0, \binom{0}{1}_0, \binom{0}{1}_2, \binom{1}{0}_2, \binom{1}{1}_0, \binom{1}{1}_1\right\}$	–
9	8	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0, \binom{1}{0}_0, \binom{1}{0}_1, \binom{1}{0}_2, \binom{1}{1}_0, \binom{1}{1}_1, \binom{1}{1}_2, \binom{1}{2}_0\right\}$	–
11	3	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_1, \binom{0}{1}_2, \binom{1}{0}_0, \binom{1}{0}_1, \binom{1}{1}_0, \binom{1}{1}_1, \binom{1}{2}_1\right\}$	–
11	6	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0, \binom{0}{1}_2, \binom{1}{0}_1\right\}$	–
11	6	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0, \binom{0}{1}_2, \binom{1}{0}_0, \binom{1}{0}_2, \binom{1}{1}_0, \binom{1}{1}_2, \binom{1}{2}_0\right\}$	–
13	3	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0, \binom{1}{0}_1, \binom{1}{0}_2, \binom{1}{1}_0, \binom{1}{1}_2, \binom{1}{2}_0\right\}$	–
13	4	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0, \binom{0}{1}_1, \binom{0}{1}_2, \binom{1}{0}_0, \binom{1}{0}_1, \binom{1}{0}_2, \binom{1}{1}_0, \binom{1}{1}_2, \binom{1}{2}_0, \binom{1}{2}_1\right\}$	–
13	6	$\left\{\binom{0}{0}_0, \binom{0}{1}_0, \binom{0}{1}_2, \binom{1}{0}_0\right\}$	–
13	6	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0, \binom{0}{1}_2, \binom{1}{0}_0, \binom{1}{1}_0, \binom{1}{1}_2, \binom{1}{2}_0\right\}$	–
15	3	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0\right\}$	–
15	3	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0, \binom{1}{0}_0, \binom{1}{0}_1, \binom{1}{1}_0, \binom{1}{2}_0\right\}$	–
15	4	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0, \binom{1}{0}_0, \binom{1}{0}_2, \binom{1}{1}_0, \binom{1}{2}_0\right\}$	–
15	5	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0, \binom{0}{1}_1, \binom{1}{0}_0, \binom{1}{0}_1, \binom{1}{0}_2, \binom{1}{1}_0, \binom{1}{1}_1, \binom{1}{2}_0, \binom{1}{2}_1\right\}$	–
17	3	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0, \binom{1}{0}_0, \binom{1}{0}_1, \binom{1}{1}_1\right\}$	–
17	3	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_1, \binom{0}{1}_2, \binom{1}{0}_0, \binom{1}{0}_1, \binom{1}{0}_2, \binom{1}{1}_0, \binom{1}{1}_1, \binom{1}{2}_1\right\}$	–
17	4	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0, \binom{0}{1}_1, \binom{0}{1}_2, \binom{1}{0}_1\right\}$	–
19	2	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0, \binom{0}{1}_1, \binom{0}{1}_2, \binom{1}{0}_0, \binom{1}{0}_1, \binom{1}{0}_2, \binom{1}{1}_0, \binom{1}{1}_1, \binom{1}{1}_2, \binom{1}{2}_0, \binom{1}{2}_1\right\}$	{0,1,3}
19	3	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0, \binom{1}{0}_0, \binom{1}{1}_1\right\}$	–
19	3	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0, \binom{1}{0}_0, \binom{1}{0}_1, \binom{1}{0}_2, \binom{1}{1}_0, \binom{1}{1}_2, \binom{1}{2}_0\right\}$	–
21	2	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0, \binom{0}{1}_2\right\}$	{0,3}
21	3	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0, \binom{0}{1}_1, \binom{1}{0}_0, \binom{1}{0}_1, \binom{1}{1}_1, \binom{1}{2}_0\right\}$	–
23	2	$\left\{\binom{0}{0}_0, \binom{0}{1}_0, \binom{0}{1}_2, \binom{1}{0}_0, \binom{1}{0}_2, \binom{1}{1}_0, \binom{1}{1}_1\right\}$	–
25	2	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_1, \binom{0}{1}_2, \binom{1}{0}_0, \binom{1}{0}_1, \binom{1}{1}_0, \binom{1}{1}_1, \binom{1}{2}_0, \binom{1}{2}_1\right\}$	{0,1}

TABLE 3. Comparing Parseval frames with Gramians $G = \sum_{g \in J} R_{[g]}$ obtained from groups $\mathbb{Z}_3^3$ and $\mathbb{Z}_{27}$, together with their code weights. See Example 4.9.

$\lvert J\rvert$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$N_{\lvert J\rvert}$	1	1	1	2	3	5	12	22	42	92	174	296	476	669	832	948

$\lvert J\rvert$	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$N_{\lvert J\rvert}$	948	832	669	476	296	174	92	42	22	12	5	3	2	1	1	1

TABLE 4. Number of nonzero terms $|J|$ summed in $\sum_{g\in J} R_{[g]}$ and number $N_{|J|}$ of resulting automorphic switching equivalence classes.

4.9. *Example* ($\mathbb{Z}_{27}$ vs. $\mathbb{Z}_3^3$, see Table 3). The symmetric doubling orbit partitioning of $\mathbb{Z}_{27}$ consists of $[0]$, $[9] = \{9, 18\}$, $[3] = \{3, 6, 12, 15, 21, 24\}$, and $[1] = \mathbb{Z}_{27}\backslash([0] \cup [9] \cup [3])$. The eight resulting Gramians each represent a distinct automorphic switching equivalence class of binary Parseval $\mathbb{Z}_{27}$-frames. The group $\mathbb{Z}_3^3$, as mentioned in Example 4.7, has 13 nontrivial symmetric doubling orbits and generates 30 automorphic switching equivalence classes of binary Parseval group frames.

4.10. *Example* ($\mathbb{Z}_{125}$ vs. $\mathbb{Z}_5^3$, see Table 5). The symmetric doubling orbit partitioning of $\mathbb{Z}_{125}$ consists of $[0]$ and three orbits, having orders $|[25]| = 4$, $|[5]| = 20$, $|[1]| = 100$. As with with the other $\mathbb{Z}_{p^q}$ cases thus far, the symmetric doubling orbits of $\mathbb{Z}_{125}$ are invariant under automorphism on $\mathbb{Z}_{125}$. It follows that the eight distinct Gramians induced by the three nontrivial symmetric doubling orbits represent eight distinct classes of binary Parseval $\mathbb{Z}_{125}$-frames.

The symmetric doubling orbit partitioning of $\mathbb{Z}_5^3$ consists of $[e]$ and 31 orbits of order 4. The 2^{31} distinct Gramians, each representing a distinct unitary equivalence class of binary Parseval $\mathbb{Z}_5^3$-frames, reduce to 7152 automorphic switching equivalence classes. Obtained by applying the algorithm described in this paper implemented in Matlab [22], Table 4 gives a breakdown of the these classes by the size of J: The $\boxed{\begin{smallmatrix}0\\1\end{smallmatrix}}$ entry corresponds to the identity matrix; the bottom row, which gives the total number of automorphically switching equivalent classes per quantity of nontrivial symmetric doubling orbit summands, sums to 7152.

For obvious reasons, we do not list representatives from each of the 7152 automorphism equivalence classes. Instead, the comparisons in Table 5 place each of the six nontrivial Gramians of binary Parseval $\mathbb{Z}_{125}$-frames next to a $\mathbb{Z}_5^3$ representative of the same rank and having maximal code weight among binary Parseval $\mathbb{Z}_5^3$-frames of the same dimension.

REFERENCES

[1] Baker, Z. J., Bodmann, B. G., Bullock, M. G., Branum, S. N., and McLaney, J. E.; What is odd about binary Parseval frames? Involve **11** (2018), no. 2, 219–233.

[2] Bodmann, B. G., Camp, B., and Mahoney, D.; Binary frames, graphs and erasures, Involve **7** (2014), no. 2, 151–169.

[3] Betten, A., Braun, M., Fripertinger, H., Kerber, A., Kohnert, A., and Wassermann, A.; *Error-correcting linear codes*, in: Algorithms and Computation in Mathematics **18**, Springer-Verlag, Berlin, 2006.

[4] Bodmann, B. G. and Paulsen, V. I.; *Frames, graphs and erasures*, Linear Algebra Appl. **404** (2005), 118–146.

[5] Bodmann, B. G., Le, M., Reza, L., Tobin, M., and Tomforde, M.; *Frame theory for binary vector spaces*, Involve **2** (2009), no. 5, 589–602.

[6] Casazza P. G. and Kutyniok, G., (eds.); *Finite frames*, Applied and Numerical Harmonic Analysis, Birkhäuser/Springer, New York, 2013, Theory and applications.

[7] Chien, T.-Y., and Waldron, S.; A classification of the harmonic frames up to unitary equivalence. Appl. Comput. Harmon. Anal. 30 (2011), 307–318

[8] Chien, T.-Y. and Waldron, S.; A characterization of projective unitary equivalence of finite frames and applications, SIAM J. Discrete Math. **30** (2016), no. 2, 976–994.

Gram rank	Code weight	$J \subset \mathbb{Z}_5^3$	Code weight	$J \subset \mathbb{Z}_{125}$
5	25	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{1}{1}_0, \binom{1}{1}_1, \binom{1}{1}_2, \binom{1}{1}_3, \binom{1}{1}_4\right\}$	25	{0,5,25}
21	25	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{1}{0}_0, \binom{1}{0}_1, \binom{1}{0}_2, \binom{1}{0}_3, \binom{1}{1}_3, \binom{1}{1}_4, \binom{1}{2}_0, \binom{1}{2}_1, \binom{1}{3}_0\right\}$	10	{0,1,25}
25	25	$\left\{\binom{0}{0}_0, \binom{0}{1}_0, \binom{0}{1}_3, \binom{1}{0}_1, \binom{1}{0}_2, \binom{1}{1}_3, \binom{1}{1}_4, \binom{1}{2}_0, \binom{1}{2}_2, \binom{1}{3}_2\right\}$	5	{0,25}
101	5	$\left\{\binom{0}{0}_0, \binom{0}{0}_1, \binom{0}{1}_0, \binom{1}{0}_4, \binom{1}{1}_3, \binom{1}{2}_1, \binom{1}{3}_0\right\}$	2	{0,1,5}
105	5	$\left\{\binom{0}{0}_0, \binom{0}{1}_0, \binom{0}{1}_1, \binom{0}{1}_2, \binom{0}{1}_3, \binom{0}{1}_4, \binom{1}{0}_4, \binom{1}{1}_0, \binom{1}{1}_1, \binom{1}{1}_2, \binom{1}{2}_2, \binom{1}{2}_3, \binom{1}{2}_4, \binom{1}{3}_1, \binom{1}{3}_2, \binom{1}{3}_3, \binom{1}{3}_4, \binom{1}{4}_0, \binom{1}{4}_1, \binom{1}{4}_2, \binom{1}{4}_3, \binom{1}{4}_4\right\}$	2	{0,5}
121	2	$\left\{\binom{0}{0}_0, \binom{0}{1}_0, \binom{0}{1}_1, \binom{0}{1}_2, \binom{0}{1}_3, \binom{0}{1}_4, \binom{1}{0}_0, \binom{1}{0}_1, \binom{1}{0}_2, \binom{1}{0}_3, \binom{1}{0}_4, \binom{1}{2}_0, \binom{1}{2}_1, \binom{1}{2}_2, \binom{1}{2}_3, \binom{1}{2}_4, \binom{1}{3}_0, \binom{1}{3}_1, \binom{1}{3}_2, \binom{1}{3}_3, \binom{1}{3}_4, \binom{1}{4}_0, \binom{1}{4}_1, \binom{1}{4}_2, \binom{1}{4}_3, \binom{1}{4}_4\right\}$	2	{0,1}

TABLE 5. Comparing groups $\mathbb{Z}_5^3$ and $\mathbb{Z}_{125}$ as generators of binary Parseval frames, best performers for each given rank of the Gramian. See Example 4.10.

[9] Christensen, O.; *An Introduction to Frames and Riesz Bases*, Birkhäuser, Boston, (2003).

[10] Goyal, V. K., Kovačević, J., and Kelner, J. A.; *Quantized frame expansions with erasures, Appl. Comput. Harmon. Anal.*, vol. 10, pp. 203–233, 2001.

[11] Han, D. and Larson, D. R.; Frames, bases and group representations, Mem. Amer. Math. Soc. **147**, 2000.

[12] Hay, N., Waldron, S.: On computing all harmonic frames of n vectors in $\mathbb{C}^d$. Appl. Comput. Harmon. Anal. 21 (2006), 168–181.

[13] Holmes, R. B., and Paulsen, V.I.; Optimal frames for erasures. Linear Algebra Appl. **377** (2004), 31–51.

[14] Hotovy, R., Larson, D. R., and Scholze, S.; Binary frames, Houston J. Math. **41** (2015), no. 3, 875–899.

[15] Kalra, D.; Complex equiangular cyclic frames and erasures. Linear Algebra Appl. 419, 373–399 (2006)

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

[17] Kovačević, J., and Chebira, A.; Life beyond bases: The advent of frames (Part II), IEEE Signal Processing Magazine **24** (2007), no. 5, 15-125.

[18] Lucido, M.S., and Pournaki, M.R.; Elements with square roots in finite groups., Algebra Colloq. **12** (2005), no. 4, 677–690 (English).

[19] MacWilliams, F. J. and Sloane, N. J.; *The Theory of Error-Correcting Codes*, North Holland, Amsterdam, 1977.

[20] Marshall, T., J.; Coding of real-number sequences for error correction: A digital signal processing problem. IEEE Journal on Selected Areas in Communications **2** (1984), no. 2, 381–392.

[21] Marshall, T.; Fourier transform convolutional error-correcting codes. In: Signals, Systems and Computers, 1989. Twenty-Third Asilomar Conference on, vol. 2, pp. 658–662 (1989).

[22] Mendez, R. P.; Supporting Matlab programs repository, `http://math.uh.edu/~rpmendez/binaryParsevalGroupFrames/`, Verified April 4, 2017.

[23] Püschel, M., and Kovačević, J.; Real, tight frames with maximal robustness to erasures. In: Data Compression Conference, 2005. Proceedings. DCC 2005, pp. 63–72 (2005).

[24] Rath, G., and Guillemot, C.; Performance analysis and recursive syndrome decoding of DFT codes for bursty erasure recovery, IEEE Trans. on Signal Processing, vol. 51 (2003), no. 5, 1335-1350.
[25] Rath, G., and Guillemot, C.; Frame-theoretic analysis of DFT codes with erasures, IEEE Transactions on Signal Processing, vol. 52 (2004), no. 2, 447-460.
[26] Schwinger, J.; Unitary operator bases, Proc. Nat. Acad. Sci. U.S.A. **46** (1960), 570–579.
[27] Vale, R., and Waldron, S.; Tight frames and their symmetries. Constr. Approx. 21, 83–112 (2005)
[28] Vale, R., and Waldron, S.; Tight frames generated by finite nonabelian groups, Numerical Algorithms **48** (2008), no. 1, 11–27.
[29] Waldron, S.; *Group frames*, pp. 171–191, in: *Finite frames*, Casazza P. G. and Kutyniok, G., (eds.), Applied and Numerical Harmonic Analysis, Birkhäuser/Springer, New York, 2013.