SIAM J. DISCRETE MATH.
Vol. 18, No. 1, pp. 1–18


# CODES CLOSED UNDER ARBITRARY ABELIAN GROUP OF PERMUTATIONS*

BIKASH KUMAR DEY† AND B. SUNDAR RAJAN‡

**Abstract.** Algebraic structure of codes over $F_q$, closed under arbitrary abelian group $G$ of permutations with exponent relatively prime to $q$, called $G$-invariant codes, is investigated using a transform domain approach. In particular, this general approach unveils algebraic structure of quasi-cyclic codes, abelian codes, cyclic codes, and quasi-abelian codes with restriction on $G$ to appropriate special cases. Dual codes of $G$-invariant codes and self-dual $G$-invariant codes are characterized. The number of $G$-invariant self-dual codes for any abelian group $G$ is found. In particular, this gives the number of self-dual $l$-quasi-cyclic codes of length $ml$ over $F_q$ when $(m, q) = 1$. We extend Tanner's approach for getting a bound on the minimum distance from a set of parity check equations over an extension field and outline how it can be used to get a minimum distance bound for a $G$-invariant code. Karlin's decoding algorithm for a systematic quasi-cyclic code with a single row of circulants in the generator matrix is extended to the case of systematic quasi-abelian codes. In particular, this can be used to decode systematic quasi-cyclic codes with columns of parity circulants in the generator matrix.

**Key words.** quasi-cyclic codes, permutation group of codes, discrete Fourier transform, self-dual codes

**AMS subject classifications.** 94B60, 11T71

**DOI.** 10.1137/S0895480102416192

## 1. Introduction.

Codes with rich algebraic structure are of strong interest to coding theorists because such codes are easy to design and decode. Classical families of cyclic codes, such as Bose–Chaudhuri–Hocquenghem (BCH) codes and Reed–Muller codes, were the center of attention for a long time. For a cyclic code, the code's permutation group contains a cyclic subgroup generated by the cyclic permutation. A cyclic code can also be viewed as an ideal of the group algebra on the cyclic group of order $n$ (length of the code). More generally, ideals of group algebras on abelian groups are known as abelian codes.

A different direction of generalization gives another class of codes: quasi-cyclic codes. A code of length $n$ is said to be $l$-quasi-cyclic for some $l|n$ if every $l$ times cyclic shift of a codeword is also a codeword. Thus an $l$-quasi-cyclic code can be viewed as a submodule of the $l$-dimensional free module $(F_qC_{\frac{n}{l}})^l$ over the group algebra $F_qC_{\frac{n}{l}}$, where $C_{\frac{n}{l}}$ is a cyclic group of order $\frac{n}{l}$.

A more general, but less popular, class of codes is the class of quasi-abelian codes [15]. For a finite abelian group $G$ and its subgroup $H$, an $F_qH$-submodule of $F_qG$ is called a $G - H$ quasi-abelian code. In fact, for an abelian group $H$ and any positive integer $t$, any submodule of $(F_qH)^t$ can be considered a quasi-abelian code. In that case, any abelian $G \supseteq H$ with $|G| = t|H|$ can be used to define quasi-abelian codes, as in [15]. Thus, such codes will be called $H$-quasi-abelian codes. When $t = 1$, this class

*Received by the editors October 17, 2002; accepted for publication (in revised form) December 12, 2003; published electronically July 2, 2004. Part of this work was presented at the International Symposium on Information Theory (ISIT), June 30–July 5, 2002, Lausanne, Switzerland. An extended abstract appeared in the *Proceedings of ISIT*, IEEE, Piscataway, NJ, 2002, p. 201.
http://www.siam.org/journals/sidma/18-1/41619.html

†International Institute of Information Technology, Hyderabad 500019, India (bikash@iiit.net).
‡Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore 560012, India (bsrajan@ece.iisc.ernet.in).

specializes to abelian codes and, when $H$ is a cyclic group, specializes to the class of quasi-cyclic codes.

Transform techniques for cyclic codes and abelian codes are well known [1, 13]. Transform techniques for repeated root cyclic codes were discussed in [10]. Recently, quasi-cyclic codes were studied in the transform domain [5, 9]. Tanner [14] introduced ways to transform a group invariant parity check matrix into a parity check matrix over an extension field, and he used this technique to get a lower bound on the minimum distance of group invariant codes.

In this paper, the algebraic structure of codes closed under any arbitrary abelian subgroup $G$ of $S_n$ (the group of permutations of $n$ elements) is investigated. We call this class $G$-invariant codes. When special types of $G$ are taken, $G$-invariant codes coincide with the class of quasi-abelian codes, and thus with the classes of quasi-cyclic codes and abelian codes. Figure 1 shows the relation between different classes of codes.

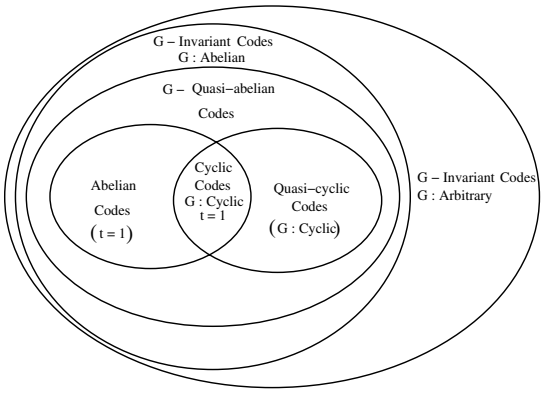


FIG. 1. *Different families of codes and their defining groups of permutations.*

Following are a few examples of some types of permutation groups $G$ shown in Figure 1.

*Example* 1.1. For any $a, b \in F_q$, $a \neq 0$, let $\sigma_{a,b}$ denote the permutation $\sigma_{a,b} : x \mapsto ax + b$. Then $G = \{\sigma_{a,b} | a \in F_q^*, b \in F_q\}$ is a subgroup of $S_q$ and is called the group of affine permutations. For $q > 2$, $G$ is nonabelian and the $G$-invariant codes are known as affine invariant codes.

*Example* 1.2. Figure 2 (ignore the solid, dashed, and dotted boxes for now) shows the cycle structure of the generator $\sigma$ of a permutation group $G = \langle \sigma \rangle \subseteq S_{16}$. Here $G$ is abelian, and $G$-invariant codes cannot be seen as $G$-quasi-abelian codes.

*Example* 1.3. Consider a permutation group $G = \langle \sigma_1, \sigma_2 \rangle \subseteq S_{54}$. Figure 3 shows the cycles of $\sigma_1$ with solid lines with arrows and the cycles of $\sigma_2$ with dashed lines with arrows. Here $G$ is abelian, and $G$-invariant codes are the same as $G$-quasi-abelian codes of length 54.

All abelian codes on an abelian group $G$ are decomposable as a direct sum of minimal abelian codes if and only if the exponent of $G$ is relatively prime to $q$. The same is true for $l$-quasi-cyclic codes if and only if $\frac{n}{l}$ is relatively prime to $q$ [2]. It will be shown that this is true for any $G$-invariant code ($G$ abelian); i.e., for an abelian subgroup $G \subseteq S_n$, any $G$-invariant code of length $n$ can be decomposed as a direct sum of minimal $G$-invariant codes if and only if the exponent of $G$ is relatively prime to $q$.

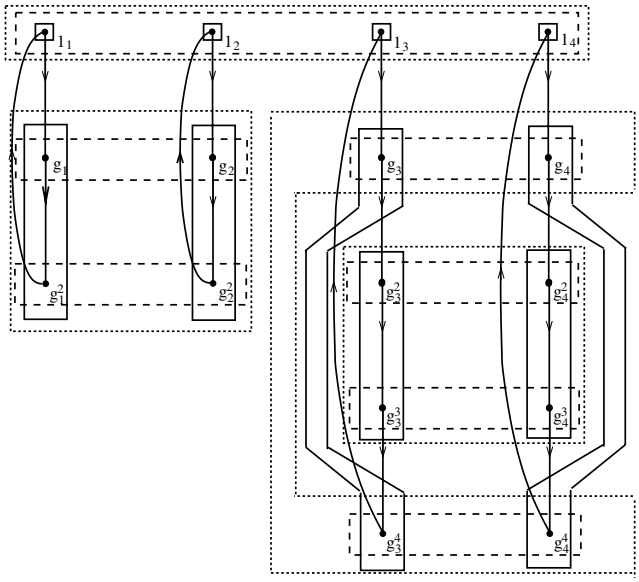


FIG. 2. *Cycle structure of the generator of G in Example* 1.2.

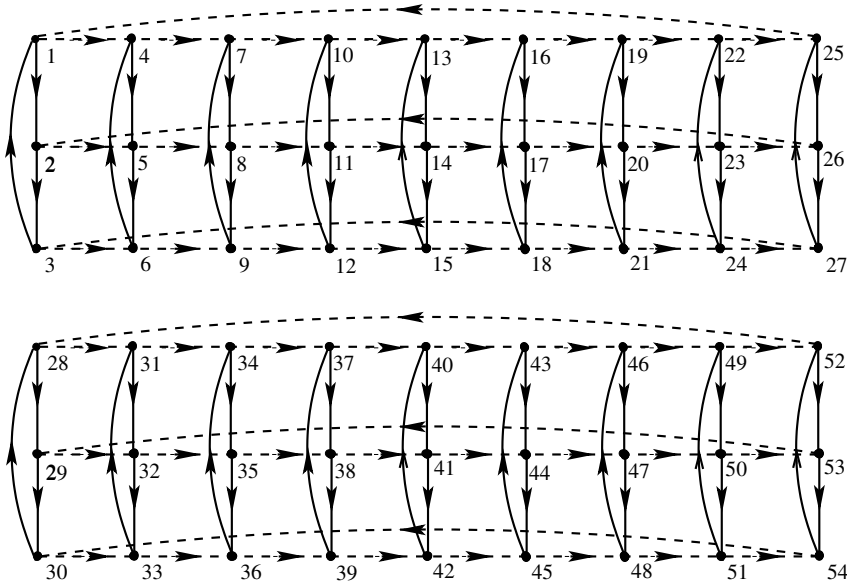


FIG. 3. *Cycle structure of the generators of G in Example* 1.3.

Karlin [7] showed a way to decode a class of one-generator quasi-cyclic codes. Heijnen and van Tilborg [6] proposed another decoding technique for the class of one-generator quasi-cyclic codes, which uses the same basic idea as Karlin's technique but achieves some computational advantages by better usage of the quasi-cyclic property of the code. In this paper, Karlin's approach is extended to a class of quasi-cyclic codes, not necessarily one-generator. When restricted to one-generator quasi-cyclic codes, this method reduces to Karlin's method. Moreover, this method also applies

to a class of quasi-abelian codes specified in subsection 7.1.

In section 2, the DFT on abelian group is reviewed, and in section 3 is used to define a DFT for $G$-invariant codes for any abelian group $G$ of permutations with exponent relatively prime to $q$. Such $G$-invariant codes are characterized in the transform domain, and their structural properties are investigated in section 4. Dual codes of $G$-invariant codes and self-dual $G$-invariant codes are characterized in section 5. The number of $G$-invariant self-dual codes for any abelian group $G$ is also found. In section 6, we extend Tanner's approach for getting a bound on the minimum distance from a set of parity check equations over an extension field and outline how it can be used to get a minimum distance bound for $G$-invariant codes. Quasi-abelian codes are discussed in section 7, and Karlin's approach [7] for decoding systematic quasi-cyclic codes with parity circulants in a single row is extended to the case of systematic quasi-abelian codes. In particular, this approach can be used to decode systematic quasi-cyclic codes which are not necessarily one-generator, which was the case left open by Karlin.

**2. Review of the DFT for abelian codes.** Let $G$ be an abelian group with exponent $\nu$ such that $(\nu, q) = 1$. Let $r$ be the smallest positive integer such that $\nu|(q^r - 1)$. Then the group of all distinct $F_{q^r}$-characters of $G$ is isomorphic to $G$. In fact, an isomorphism $x \mapsto \psi_{(x)}$ can be chosen (see, for example, [3] and the references therein) such that $\psi_{(x)}(y) = \psi_{(y)}(x)$. We denote $\psi_{(x)}(y)$ as $\psi(x, y)$, considering it a map $\psi : G \times G \to F_{q^r}$. It satisfies the following properties:

$$\psi(x, yz) = \psi(x, y)\psi(x, z), \tag{1a}$$

$$\psi(x, y) = \psi(y, x), \tag{1b}$$

$$(\psi(x, y) = \psi(x', y)\ \forall y \in G) \iff x = x', \tag{1c}$$

$$\sum_{x \in G} \psi(x, y) = \begin{cases} |G| & \text{if } y = 1, \\ 0 & \text{if } y \neq 1, \end{cases} \tag{1d}$$

where $|G|$ and 1 denote, respectively, the cardinality of $G$ and the identity element in $G$.

The DFT of any element $\mathbf{a} = \sum_{x \in G} a_x x \in F_q G$ is defined as $\mathbf{A} = \sum_{x \in G} A_x x \in F_{q^r} G$ such that $A_x = \sum_{y \in G} \psi(x, y) a_y$. The inverse DFT is obtained as $a_x = |G|^{-1} \sum_{y \in G} \psi(x, y)^{-1} A_y$.

**3. DFT for $G$-invariant codes.** We consider codes of length $n$ over $F_q$ with components indexed by a set $I$. Let $G \subseteq Perm(I)$ be an abelian subgroup of the group of permutations of $I$. Let the characteristic of $F_q$ be $p$.

Suppose $I_1, \ldots, I_t$ are the orbits of $I$ under the action of $G$. Let us denote $G_k = \{g^{(k)} | g \in G\}$ for $k = 1, \ldots, t$, where $g^{(k)} \stackrel{\triangle}{=} g|_{I_k} \in Perm(I_k)$ is the permutation $g$ restricted to $I_k$. Since $G_k$ is abelian and acts on $I_k$ faithfully and transitively, the stabilizer of any $i \in I_k$ is $\{1_k\}$ ($1_k$ denotes the identity element of $G_k$). Thus, for any $i_1 \in I_k$, there is a unique $g \in G_k$, such that $i_1 = g(i)$. This defines a one-to-one correspondence between $G_k$ and $I_k$. Using this, the symbols can be indexed by the elements of $G_k$ instead of $I_k$ by first associating a fixed element $i \in I_k$ with the identity element $1_k$. Hence, the code symbols are indexed by $\mathcal{G} \stackrel{\triangle}{=} \cup_{i=1}^{t} G_i$ instead of $I$. Then the element $g$ of $G$ acts on $\mathcal{G}$ as $x \stackrel{g}{\mapsto} g^{(k)} x$ when $x \in G_k$. For any $\mathbf{a} = (a_x)_{x \in \mathcal{G}} \in F_q^{\mathcal{G}}$, $g \in G$ acts on $\mathbf{a}$ as $\mathbf{a} \stackrel{g}{\mapsto} \mathbf{b} = g(\mathbf{a})$ such that $b_x = a_{g^{(k)-1}x}$ when $x \in G_k$. Henceforth, we'll use the letters $f, g,$ and $h$, possibly with subscripts, to denote elements of $G$, and use the letters $x$, $y$, and $z$ to denote elements of $\mathcal{G}$.

Let the exponent of $G$, $\exp(G) = lcm\,(\{\exp(G_k)|k = 1, \ldots, t\})$ be relatively prime to $q$, and let $r$ be the smallest positive integer such that $\exp(G)$ divides $(q^r - 1)$. Then on each orbit, DFT is defined as discussed in the last section; i.e., the DFT of $\mathbf{a} \in F_q^{\mathcal{G}}$ is defined as $\mathbf{A} = (A_x)_{x\in\mathcal{G}} \in F_{q^r}^{\mathcal{G}}$, where

$$A_x = \sum_{y\in G_k} \psi_k(x, y)a_y \qquad \forall x \in G_k,\ \forall k.$$

Here $\psi_k$ is as defined in the last section for $G_k$. For any two $x, y \in \mathcal{G}$, define

$$\Psi(x, y) = \begin{cases} \psi_k(x, y) & \text{when } x, y \in G_k \text{ for some } k, \\ 0 & \text{when } x \in G_{k_1} \text{ and } y \in G_{k_2}, \text{ s.t. } k_1 \neq k_2. \end{cases}$$

With this notation, the DFT can be rewritten as $A_x = \sum_{y\in\mathcal{G}} \Psi(x, y)a_y \forall x \in \mathcal{G}$. Clearly, $\mathbf{A}$ satisfies $A_{x^q} = A_x^q\ \forall x \in \mathcal{G}$. For any $h \in G$ and $x \in \mathcal{G}$, we define the symbol

$$\langle h, x\rangle \stackrel{\triangle}{=} \psi_k(h^{(k)}, x) \quad \text{when } x \in G_k. \tag{2}$$

It follows from this definition that the DFT of $\mathbf{b} = h(\mathbf{a})$ is given by $B_x = \langle h, x\rangle A_x$. Suppose $h_1, h_2 \in G_k$. Then using (1a) and (1c), we have $\langle g, h_1\rangle^l = \langle g, h_2\rangle\ \forall g \in G$ if and only if $h_1^l = h_2$.

For any element $x \in \mathcal{G}$, it is in $G_k$ for some $k$, and thus a *cyclotomic coset* of $x$ is defined as $[x]^q \stackrel{\triangle}{=} \{y \in G_k|y = x^{q^t} \text{ for some nonnegative } t\}$. Cardinality of $[x]^q$ will be denoted as $r_x$. For any subset $S \subseteq \mathcal{G}$, we define $[S]^q \stackrel{\triangle}{=} \cup_{s\in S}[s]^q$.

Corollary 3.1. *For any $x \in \mathcal{G}$, $r_x$ is the smallest positive integer such that $\langle g, x\rangle^{q^{r_x}} = \langle g, x\rangle\ \forall g \in G$. Thus, $r_x$ is the least common multiple (lcm) of the lengths of the conjugacy classes of $\langle g, x\rangle\ \forall g \in G$.*

The *residue class* of $x \in \mathcal{G}$ is defined as $\widetilde{x} \stackrel{\triangle}{=} \{x_1 \in \mathcal{G}|\langle g, x_1\rangle = \langle g, x\rangle \text{ for each } g \in G\}$. Cardinality of $\widetilde{x}$ will be denoted by $e_x$. For any subset $X = \{x_1, x_2, \ldots, x_k\} \subseteq \mathcal{G}$, $A_X$ denotes the ordered tuple $(A_{x_1}, A_{x_2}, \ldots, A_{x_k})$ with an arbitrary fixed order in $X$. In particular, for any residue class $\widetilde{y_1} = \{y_1, y_2, \ldots, y_l\}$, we denote by $A_{\widetilde{y}}$ the ordered $l$-tuple $(A_{y_1}, A_{y_2}, \ldots, A_{y_l})$ with an arbitrarily chosen fixed order on $\widetilde{y}$. For some ordered tuples $T_1 = (t_{1,1}, \ldots, t_{1,j_1}), \ldots, T_l = (t_{l,1}, \ldots, t_{l,j_l})$ the concatenated tuple $(t_{1,1}, \ldots, t_{1,j_1}, \ldots, t_{l,1}, \ldots, t_{l,j_l})$ is denoted $(T_1, \ldots, T_l)$.

The *cyclotomic residue class* of $x \in \mathcal{G}$ is defined as $(x)^q \stackrel{\triangle}{=} \{x_1 \in \mathcal{G}| \text{ for some nonnegative } t, \langle g, x_1\rangle^{q^t} = \langle g, x\rangle\ \forall g \in G\} = [\widetilde{x}]^q$. Figure 4 shows the relation between a cyclotomic residue class and the cyclotomic cosets and residue classes in it. By the conjugacy constraint, the values of the DFT components in one residue class determine the values of the other transform components in the same cyclotomic residue class. To be specific, $A_{\widetilde{x^{q^i}}} = A_{\widetilde{x}}^{q^i}$ for any $\mathbf{a} \in F_q^{\mathcal{G}}$, where the power of the vector $A_{\widetilde{x}}$ is taken componentwise. Thus, the values of the transform components in one representative residue class from each cyclotomic residue class specify a vector completely.

*Example* 3.1 (continuation of Example 1.2). The index set has four orbits under the action of $G$ and $G_1 \simeq G_2 \simeq \mathbb{Z}_3$, and $G_3 \simeq G_4 \simeq \mathbb{Z}_5$. Let a set of generators of the groups $G_1, G_2, G_3$, and $G_4$ be $g_1, g_2, g_3$, and $g_4$, respectively. If $\alpha \in F_{q^r}$ is an element of order 15, then we define DFT in $F_q^{16} \simeq F_q^{\mathcal{G}}$ with respect to the maps $\psi_k$ defined by $\psi_1(g_1, g_1) = \psi_2(g_2, g_2) = \alpha^5,\ \psi_3(g_3, g_3) = \psi_4(g_4, g_4) = \alpha^3$. The residue classes in $\mathcal{G}$ are shown in Figure 2 with dashed boxes. The figure shows the cyclotomic cosets with solid boxes and the cyclotomic residue classes with dotted boxes for $q \equiv 2 \bmod 3$, $q \equiv 4 \bmod 5$ (e.g., $q = 29, 59$).

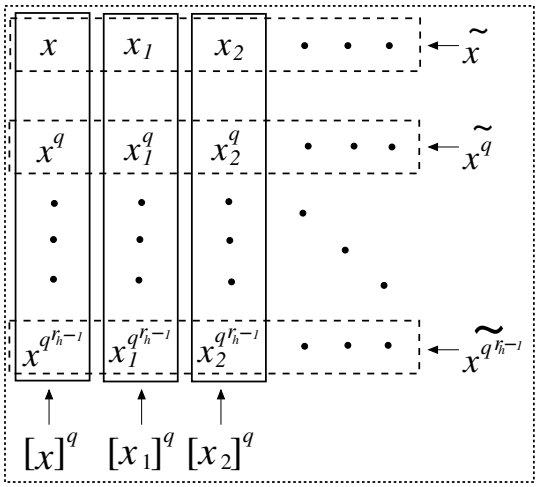


FIG. 4. *A generic cyclotomic residue class* $(x)^q$.

**4. Transform domain characterization of $G$-invariant codes.** A linear code $\mathcal{C} \subseteq F_q^{\mathcal{G}}$ is $G$ invariant if for every codeword $\mathbf{a} \in \mathcal{C}$ and $h \in G$, $h(\mathbf{a}) \in \mathcal{C}$. The equivalent condition in the transform domain is that for any $h \in G$, $\mathbf{A} = DFT(\mathbf{a})$ for some $\mathbf{a} \in \mathcal{C}$ and $\mathbf{B} \in F_{q^r}^{\mathcal{G}}$ with $B_x = \langle h, x\rangle A_x \ \forall x \in \mathcal{G} \Rightarrow \mathbf{B} = DFT(\mathbf{b})$ for some $\mathbf{b} \in \mathcal{C}$.

For any ordered tuple $(x_1, x_2, \ldots, x_l)$ on $\mathcal{G}$, we say $(A_{x_1}, A_{x_2}, \ldots, A_{x_l})$ takes values from $\{(A_{x_1}, A_{x_2}, \ldots, A_{x_l}) \,|\mathbf{a} \in \mathcal{C}\}$ for $\mathcal{C}$. If for $\mathcal{C}$, $(A_{x_1}, A_{x_2}, \ldots, A_{x_l})$ takes values from $V \subseteq F_{q^r}^l$ and $U \subseteq V$, then the subcode $\{\mathbf{a} \in \mathcal{C} |\, (A_{x_1}, A_{x_2}, \ldots, A_{x_l}) \in U\}$ will be referred to as the subcode obtained from $\mathcal{C}$ by restricting $(A_{x_1}, A_{x_2}, \ldots, A_{x_l})$ to $U$.

LEMMA 4.1. *For any $G$-invariant code $\mathcal{C}$ and $x \in \mathcal{G}$, $A_{\widetilde{x}}$ takes values from a subspace of $F_{q^{r_x}}^{e_x}$.*

*Proof.* Suppose $A_{\widetilde{x}}$ takes values from an $F_q$-subspace (since the code is linear) $V \subseteq F_{q^{r_x}}^{e_x}$ for $\mathcal{C}$. When any element $g \in G$ acts on a codeword $\mathbf{a}$, $A_{\widetilde{x}}$ is multiplied by $\langle g, x\rangle$. Since the code is $G$-invariant, $\langle g, x\rangle v \in V$ for each $g \in G$ and $v \in V$. Thus, $V$ is closed under multiplication by elements of $Span_{F_q}(\langle\{\langle g, x\rangle | g \in G\}\rangle) = F_q\left[\{\langle g, x\rangle | g \in G\}\right] = F_{q^{r_x}}$. □

For any $G$-invariant code $\mathcal{C}$ and $x \in \mathcal{G}$, suppose $A_{\widetilde{x}}$ takes values from a subspace $V \subseteq F_{q^{r_x}}^{e_x}$. Then for any subspace $U \subseteq V$, the subcode obtained by restricting $A_{\widetilde{x}}$ to $U$ is also $G$-invariant. For a linear code $\mathcal{C}$, suppose, $A_{\widetilde{x}}$ takes values from a subspace $V \subseteq F_{q^{r_x}}^{e_x}$, and $V = V_1 + V_2$. If the subcodes obtained by restricting $A_{\widetilde{x}}$ to $V_1$ and $V_2$ are, respectively, $\mathcal{C}_1$ and $\mathcal{C}_2$, then $\mathcal{C} = \mathcal{C}_1 + \mathcal{C}_2$.

DEFINITION 4.2. *Let $X_1, X_2, \ldots, X_l$ be some disjoint subsets of $\mathcal{G}$ and suppose $R_{X_j} = \{A_{X_j} | \mathbf{a} \in \mathcal{C}\}$ for $j = 1, 2, \ldots, l$. The sets of transform components $\{A_x | x \in X_j\}$, $1 \leq j \leq l$, are said to be* unrelated *in $\mathcal{C}$ if $\{(A_{X_1}, A_{X_2}, \ldots, A_{X_l}) \,|\mathbf{a} \in \mathcal{C}\} = R_{X_1} \times R_{X_2} \times \cdots \times R_{X_l}$. They are said to be* related *if they are not unrelated.*

Let $\widetilde{x_1}, \widetilde{x_2}, \ldots, \widetilde{x_l}$ be a set of representative residue classes of all the distinct cyclotomic residue classes. Suppose we fix arbitrary subspaces $V_i$, $i = 1, 2, \ldots, l$, of $F_{q^{r_{x_i}}}^{e_{x_i}}$, $i = 1, 2, \ldots, l$, respectively, and consider the code $\mathcal{C} = \left\{\mathbf{a} \in F_q^{\mathcal{G}} | A_{\widetilde{x_i}} \in V_i \text{ for } i = 1, 2, \ldots, l\right\}$. Clearly, the code is $G$-invariant. But it is not clear whether any $G$-invariant code can be obtained this way by choosing suitable $V_i$, $i = 1, 2, \ldots, l$. That is, are $A_{\widetilde{x_i}}$, $i = 1, \ldots, l$, unrelated for any $G$-invariant code? Theorem 4.6 will

answer this question in the affirmative.

If, in a $G$-invariant code, two transform components $A_x$ and $A_y$ are unrelated, then consider the subcodes $\mathcal{C}_1$ and $\mathcal{C}_2$ obtained by restricting, respectively, $A_x$ and $A_y$ to $\{0\}$. Clearly, the original code is the sum of the codes $\mathcal{C}_1$ and $\mathcal{C}_2$. Suppose $S_1, \ldots, S_l$ are some disjoint subsets of the index set such that $x, y \in \cup_{i=1}^{l} S_i$. Then the transform components in $S_1, \ldots, S_l$ are unrelated in $\mathcal{C}$ if and only if they are unrelated in $\mathcal{C}_1$ and $\mathcal{C}_2$. This process can be continued on $\mathcal{C}_1$ and $\mathcal{C}_2$ and repeated on the resulting subcodes to get a set of subcodes whose sum is $\mathcal{C}$ and in each of which either there is only one nonzero transform component or any pair of nonzero transform components is related. So, if the transform components in $S_1, \ldots, S_l$ are related in $\mathcal{C}$, then there is a $G$-invariant subcode of $\mathcal{C}$, where two transform components $A_x, A_y, x \in S_i, y \in S_j, i \neq j$, are related.

Suppose, in a $G$-invariant code, two transform components $A_x$ and $A_y$ are related. Then they must take values from $F_{q^{r_x}}$ and $F_{q^{r_y}}$, respectively. The relation must be by a bijection (so $r_x = r_y$) $\sigma : F_{q^{r_x}} \to F_{q^{r_x}}$ since the subcode obtained by restricting $A_x$ or $A_y$ to $\{0\}$ is $G$-invariant. Since the code is linear $G$-invariant, $\sigma$ must be an $F_q$-linear isomorphism satisfying

$$\sigma(\langle g, x\rangle v) = \langle g, y\rangle \sigma(v) \ \ \forall g \in G, \ \forall v \in F_{q^{r_x}}. \tag{3}$$

For a map $\sigma$ of a finite field, we denote by $f_\sigma(X)$ a polynomial which induces $\sigma$, that is, $\sigma(a) = f_\sigma(a)$.

LEMMA 4.3. *Let $\alpha, \beta \in F_{q^l}$ be such that the length of the $F_q$-conjugacy class of $\alpha$ is $l_1$. Suppose $a \in F_{q^l}^*$ and $\sigma : aF_{q^{l_1}} \longrightarrow F_{q^l}$ is an $F_q$-linear nonzero map. Then $\sigma$ satisfies $\sigma(\alpha b) = \beta\sigma(b)\ \forall b \in aF_{q^{l_1}}$ if and only if $\beta = \alpha^{q^j}$ and $f_\sigma(X) = cX^{q^j}$ for some unique $c \in F_{q^l}$ and $j < l_1$.*

*Proof.* The reverse implication is obvious. For the forward implication, let us consider the $F_q$-linear map $\sigma' : F_{q^{l_1}} \to F_{q^l}$; $\sigma' : x \mapsto \frac{\sigma(ax)}{\sigma(a)}$. Clearly, $\sigma'(\alpha^i) = \beta^i$ for $i \geq 0$. Thus, $\sigma'$ is a field isomorphism of $F_q[\alpha]$ onto $F_q[\beta]$. So for some $j$, $\sigma'(x) = x^{q^j}$ $\forall x \in F_q[\alpha] = F_{q^{l_1}}$. Therefore,

$$\sigma(x) = \sigma(a)\sigma'\left(\frac{x}{a}\right) = \sigma(a)a^{-q^j}x^{q^j} \text{ for any } x \in aF_{q^{l_1}}. \qquad \square$$

LEMMA 4.4. *Let $\alpha$, $\beta$, and $l_1$ be as in Lemma 4.3 and $V$ be an $h$-dimensional $F_{q^{l_1}}$-subspace of $F_{q^l}$. Suppose $\sigma : V \longrightarrow F_{q^l}$ is a nonzero $F_q$-linear map. If $\sigma$ satisfies $\sigma(\alpha b) = \beta\sigma(b)\ \forall b \in V$, then $\beta = \alpha^{q^j}$ and $f_\sigma(X) = \sum_{i=0}^{h-1} c_i X^{q^{il_1+j}}$ for some unique $c_i \in F_{q^l}$ for $0 \leq i \leq h-1$.*

*Proof.* Suppose $V = \oplus_{i=0}^{h-1} V_i$, where $V_i = s_i F_{q^{l_1}}$. Since $\sigma$ is nonzero, its restriction on at least one of $V_i, 0 \leq i \leq h-1$, is nonzero, and thus by Lemma 4.3, the first statement follows. Suppose $\sigma_i = \sigma|_{V_i}$. Then, $f_{\sigma_i}(X) = c_i' X^{q^j}$ for some unique $c_i'$. Thus,

$$\begin{aligned}
f_\sigma(X) &= \sum_{w=0}^{h-1} c_w X^{q^{wl_1+j}} \\
&\Leftrightarrow c_i'(s_i a)^{q^j} = \sum_{w=0}^{h-1} c_w (s_i a)^{q^{wl_1+j}} \ \ \forall a \in F_{q^{l_1}}, \ \forall i \in [0, h-1] \\
&\Leftrightarrow c_i' s_i' = \sum_{w=0}^{h-1} c_w \left(s_i'\right)^{q^{wl_1}} \ \ \forall i \in [0, h-1], \quad \text{where } s_i' = (s_i)^{q^j}
\end{aligned}$$

$$(4) \qquad \Leftrightarrow \begin{pmatrix} s'_0 & s'^{q^{l_1}}_0 & s'^{q^{2l_1}}_0 & \cdots & s'^{q^{(h-1)l_1}}_0 \\ s'_1 & s'^{q^{l_1}}_1 & s'^{q^{2l_1}}_1 & \cdots & s'^{q^{(h-1)l_1}}_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s'_{h-1} & s'^{q^{l_1}}_{h-1} & s'^{q^{2l_1}}_{h-1} & \cdots & s'^{q^{(h-1)l_1}}_{h-1} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{h-1} \end{pmatrix} = \begin{pmatrix} c'_0 s'_0 \\ c'_1 s'_0 \\ \vdots \\ c'_{h-1} s'_{h-1} \end{pmatrix}.$$

Now, $\{s_0, s_1, s_2, \ldots, s_{h-1}\}$ are linearly independent over $F_{q^{l_1}}$ since $V_j = \oplus_{i=0}^{h-1} s_i F_{q^{l_1}}$. Thus, $\{s'_0, s'_1, s'_2, \ldots, s'_{h-1}\}$ are also linearly independent over $F_{q^{l_1}} \Rightarrow$ the $h \times h$ matrix in (4) is nonsingular, and thus there exists a unique solution of (4) for $c_0, c_1, \ldots, c_{h-1}$. □

LEMMA 4.5. *Let $\alpha_i$, $1 \leq i \leq k$, be some elements of $F_{q^l}$ with length of conjugacy classes $l_i$, $i = 1, \ldots, k$, respectively. Suppose $l' = lcm(l_1, \ldots, l_k)$ and $\sigma : F_{q^{l'}} \longrightarrow F_{q^l}$ is a nonzero $F_q$-linear map. If $\sigma$ satisfies $\sigma(\alpha_i b) = \beta_i \sigma(b)\ \forall b \in F_{q^{l'}}$ for some $\beta_i \in F_{q^l}, i = 1, \ldots, k$, then there exists an integer $j \geq 0$ such that $\beta_i = \alpha_i^{q^j}$ for $i = 1, \ldots k$, and $f_\sigma(X) = cX^{q^j}$ for some unique $c \in F_{q^l}$.*

*Proof.* Suppose $l'_i = \frac{l'}{l_i}$, $i = 1, \ldots, k$. By Lemma 4.4, $\beta_i = \alpha_i^{q^{j_i}}$ for some nonnegative $j_i$, $i = 1, \ldots, k$. Now, $\exists$ a unique polynomial $f_\sigma(X)$ of degree $< q^{l'}$. Applying Lemma 4.4 for each $i$, we see that $\sigma$ is induced by $f_i(X) = \sum_{h_i=0}^{l'_i - 1} c_{i,h_i} X^{q^{h_i l_i + j_i}}$, where $c_{h_i}, 0 \leq h_i \leq l'_i - 1$, are some unique constants. Since all the polynomials $f_i(X)$ are of degree $< q^{l'}$, they have to be the same. In particular, their smallest degree terms are the same, and that means, say, $j = h_1 l_1 + j_1 = \cdots = h_k l_k + j_k$. Now, if there is any nonzero monomial other than $X^{q^j}$, then such a monomial is of degree, say, $j' = h'_1 l_1 + j_1 = \cdots = h'_k l_k + j_k$. Thus,

$$\begin{aligned} (h'_1 - h_1) l_1 = \cdots = (h'_k - h_k) l_k \\ \Rightarrow l' = lcm(l_1, \ldots, l_k) | (h'_1 - h_1) l_1. \end{aligned}$$

This contradicts the fact that $(h'_1 - h_1) < l'_1 = \frac{l'}{l_1}$. Thus, $f_\sigma(X) = cX^{q^j}$ for some unique constant $c$ and $\alpha_i = \beta_i^{q^j}, i = 1, \ldots, k$. □

By (3) and Lemma 4.5, for a linear $G$-invariant code, two transform components cannot be related unless they are in the same cyclotomic residue class. Thus, we have the following theorem.

THEOREM 4.6. *Let $(x_i)^q$, $i = 1, 2, \ldots, k$, be the distinct cyclotomic residue classes. Then for any linear $G$-invariant code, $\{A_x | x \in (x_i)^q\}$, $i = 1, 2, \ldots, k$, are unrelated.*

COROLLARY 4.7. *Let $(x_i)^q$, $i = 1, 2, \ldots, k$, be the distinct cyclotomic residue classes. Then, any linear $G$-invariant code $\mathcal{C}$ is*

$$(5) \qquad \mathcal{C} = \bigoplus_{i=1}^{k} \mathcal{C}_{(x_i)^q},$$

*where $\mathcal{C}_{(x_i)^q}$ denotes the subcode of $\mathcal{C}$ obtained by restricting all the transform components outside $(x_i)^q$ to zero.*

For quasi-cyclic codes, this gives the primary components of a code [8], and for cyclic and abelian codes, these subcodes, when nonzero, are minimal cyclic and abelian codes, respectively.

A nonzero linear $G$-invariant code is called minimal if it does not have any nontrivial linear $G$-invariant subcode. For a minimal $G$-invariant code, transform components in only one cyclotomic residue class $(x)^q$ are nonzero and $A_{\underset{\sim}{x}}$ takes values

from a one-dimensional subspace of $F_{q^{r_x}}^{e_x}$. Since any vector space is a direct sum of one-dimensional vector spaces, we have the following theorem.

THEOREM 4.8. *Any $G$-invariant code is a direct sum of minimal $G$-invariant codes.*

However, the decomposition of a $G$-invariant code in terms of some minimal $G$-invariant codes is not unique, though for the special case of abelian codes, such a decomposition (as a direct sum of minimal abelian codes) is unique.

It is known that if $(\exp(G), q) \neq 1$, then there are abelian codes on that group, which cannot be decomposed as a direct sum of minimal abelian codes. If $(\exp(G), q) \neq 1$, then for some $k$, $(\exp(G_k), q) \neq 1$. Then we can take an abelian code on $G_k$, which cannot be decomposed as a direct sum of minimal abelian codes. That code can be padded with zeros in all other orbits to get a $G$-invariant code, which is not decomposable as a direct sum of minimal $G$-invariant codes.

THEOREM 4.9 (transform domain characterization). *Let $G$ be an abelian group of permutations with order relatively prime to $q$. Then a code is $G$-invariant if and only if the following hold:*

(i) *For any $x \in \mathcal{G}$, $A_{\widetilde{x}}$ takes values from a subspace of $F_{q^{r_x}}^{e_x}$.*

(ii) *If $x_1, \ldots, x_k$ are representatives of the distinct cyclotomic residue classes of $\mathcal{G}$, then $A_{\widetilde{x_1}}, \ldots, A_{\widetilde{x_k}}$ are unrelated.*

**5. Duals of $G$-invariant codes.** To characterize duals of $G$-invariant codes, some generalizations of Euclidean and Hermitian dual codes are needed. Let $\mathbf{v} = (v_1, \ldots, v_l) \subseteq F_q^l$ be a vector with each component nonzero. For any two vectors $\mathbf{a}, \mathbf{b} \in F_q^l$, the $\mathbf{v}$-weighted Euclidean inner product (or $E_{\mathbf{v}}$-inner product) of $\mathbf{a}$ and $\mathbf{b}$ is defined as

$$E_{\mathbf{v}}(\mathbf{a}, \mathbf{b}) = \sum_{x=1}^{l} v_x a_x b_x. \tag{6}$$

Similarly, for any $\mathbf{v} \in F_q^l$, the $\mathbf{v}$-weighted Hermitian inner product, or $H_{\mathbf{v}}$-inner product, of $\mathbf{a} \in F_{q^2}^l$ and $\mathbf{b} \in F_{q^2}^l$ is defined as

$$H_{\mathbf{v}}(\mathbf{a}, \mathbf{b}) = \sum_{x=1}^{l} v_x a_x b_x^q. \tag{7}$$

When $\mathbf{v}$ is an "all-ones" vector, the $\mathbf{v}$-weighted Euclidean inner product and $\mathbf{v}$-weighted Hermitian inner product reduce to the usual Euclidean and Hermitian inner products, respectively.

Two vectors are called orthogonal w.r.t. an inner product if the inner product of the vectors is zero. Two linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are called the dual of each other with respect to an inner product if $\mathcal{C}_2$ is the set of all the vectors which are orthogonal to every vector in $\mathcal{C}_1$. When no inner product is specified, it is assumed to be a Euclidean inner product. A code is called self-dual when it is the dual of itself.

For any $x \in \mathcal{G}$, $\tau_x$ will denote the cardinality of the orbit containing $x$. For any residue class $\widetilde{x}$, $\tau_{\widetilde{x}}$ will denote the $e_x$-tuple with components $\tau_y$, $y \in \widetilde{x}$, in the same order as $A_y$ in $A_{\widetilde{x}}$. With abuse of notation, $\tau_{\widetilde{x}}^{-1}$ will denote the componentwise inverse (in $F_p \subseteq F_q$) of $\tau_{\widetilde{x}}$.

THEOREM 5.1. *For a $G$-invariant code $\mathcal{C}$, a vector $\mathbf{b} \in F_q^{\mathcal{G}}$ is orthogonal to $\mathcal{C}$ if*

*and only if* $\forall \mathbf{a} \in \mathcal{C}$,

$$\sum_{y \in \widetilde{x}} \tau_y^{-1} A_y B_{y^{-1}} = 0 \quad \forall \text{ cyclotomic residue classes } (x)^q. \tag{8}$$

*Proof.* Clearly, $\mathbf{b}$ is orthogonal to $\mathcal{C}$ if and only if

$$\begin{aligned}
\mathbf{a} \perp \mathbf{b} \forall \mathbf{a} \in \mathcal{C} &\iff \sum_{y \in \mathcal{G}} a_y b_y = 0 && \forall \mathbf{a} \in \mathcal{C} \\
&\iff \sum_{y \in \mathcal{G}} \tau_y^{-1} A_y B_{y^{-1}} = 0 && \forall \mathbf{a} \in \mathcal{C} \\
&\iff \sum_{i=0}^{r_x - 1} \sum_{y \in \widetilde{x}} \tau_y^{-1} A_{y^{q^i}} B_{\left(y^{q^i}\right)^{-1}} = 0 && \text{for each } (x)^q,\ \forall \mathbf{a} \in \mathcal{C} \qquad (9) \\
&\iff \sum_{i=0}^{r_x - 1} \left( \sum_{y \in \widetilde{x}} \tau_y^{-1} A_y B_{y^{-1}} \right)^{q^i} = 0 && " \\
&\iff Tr_{F_{q^{r_x}}/F_q} \left( \sum_{y \in \widetilde{x}} \tau_y^{-1} A_y B_{y^{-1}} \right) = 0 && " \\
&\iff \sum_{y \in \widetilde{x}} \tau_y^{-1} A_y B_{y^{-1}} = 0 && " \ . \qquad (10)
\end{aligned}$$

To get (9), we use the fact that the transform components in different cyclotomic residue classes are unrelated for a $G$-invariant code, and to obtain (10) we use the fact that $A_{\widetilde{x}}$ takes values from a subspace of $F_{q^{r_x}}^{e_x}$. ∎

Note that if (8) is satisfied for a residue class $\widetilde{x}$, then it is also satisfied for any other residue class in the same cyclotomic residue class. Thus, it is sufficient to consider only one representative residue class in each cyclotomic residue class. When two residue classes $\widetilde{x}$ and $\widetilde{x^{-1}}$ are considered, compatible orders are taken in them; i.e., if we take

$$A_{\widetilde{x}} = \left( A_x, A_{x_1}, \ldots, A_{x_{e_x - 1}} \right),$$

then we also take

$$A_{\widetilde{x^{-1}}} = (A_{x^{-1}}, A_{x_1^{-1}}, \ldots, A_{x_{e_x - 1}^{-1}}).$$

Let $\{x_1, x_2, \ldots, x_l\}$ be a set of representatives of the distinct cyclotomic residue classes of $\mathcal{G}$. Suppose, for the codes $\mathcal{C}_1$ and $\mathcal{C}_2$, $A_{\widetilde{x}}$ takes values from $V_x$ and $U_x$, respectively. Then $V_x$ and $U_x$ can also be considered linear codes of length $e_x$ over $F_{q^{r_x}}$. Using Theorem 5.1, the dual code of a $G$-invariant code can be characterized as follows.

THEOREM 5.2. *Two $G$-invariant codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are the dual of each other if and only if for each $x_i$, $i = 1, 2, \ldots, l$, $V_{x_i}$ and $U_{x_i^{-1}}$ are the $E_{\tau_{\widetilde{x}_i}^{-1}}$-dual of each other.*

**5.1. Self-dual $G$-invariant codes.** Let us classify the cyclotomic residue classes into the following three types:

1. Type A: Self-inverse cyclotomic residue classes $(x)^q$ with $x = x^{-1}$. In this case, suppose $x = x^{-1} \in G_k$, i.e., $x^2 = 1_k$. Then either $x = 1_k$ or order of $G_k$ is even $\Rightarrow q$ is odd (since $(q, |G_k|) = 1) \Rightarrow x^q = x \Rightarrow r_x = 1$.

2. Type B: Self-inverse cyclotomic residue classes $(x)^q$ with $x \neq x^{-1}$. In this case,

$$x^{-1} = x^{q^i} \text{ for some } i < r_x, \quad i \neq 0.$$

Thus,

$$x = \left(x^{-1}\right)^{-1} = \left(x^{q^i}\right)^{-1} = \left(x^{-1}\right)^{q^i} = x^{q^{2i}} \Rightarrow r_x | 2i \Rightarrow 2 | r_x \text{ and } i = \frac{r_x}{2}.$$

3. Type C: Cyclotomic residue classes $(x)^q$ which are not self-inverse, i.e., $x^{-1} \notin (x)^q$.

The cyclotomic cosets are also assigned a "type" based on the type of cyclotomic residue classes they are in. Let us denote the distinct cyclotomic residue classes as

$$\begin{aligned}
&\text{Type A: } (x_1)^q, \ldots, (x_{i_1})^q, \\
&\text{Type B: } (y_1)^q, \ldots, (y_{i_2})^q, \\
&\text{Type C: } (z_1)^q, (z_1^{-1})^q \ldots, (z_{i_3})^q, (z_{i_3}^{-1})^q.
\end{aligned}$$

THEOREM 5.3. *Let $\mathcal{C}$ be a $G$-invariant code, where $A_{\underset{\sim}{x_i}}$, $A_{\underset{\sim}{y_j}}$, $A_{\underset{\sim}{z_k}}$, and $A_{\underset{\sim}{z_k^{-1}}}$ take values from the subspaces $V_{x_i}$, $V_{y_j}$, $V_{z_k}$, and $V_{z_k^{-1}}$, respectively, for $i = 1, \ldots, i_1$, $j = 1, \ldots, i_2$, $k = 1, \ldots, i_3$. The code is self-dual if and only if*

(i) *$V_{x_i}$ is an $E_{\underset{\sim}{\tau^{-1}}_{x_i}}$-self-dual code for $i = 1, \ldots, i_1$.*

(ii) *$V_{y_j}$ is an $H_{\underset{\sim}{\tau^{-1}}_{y_j}}$-self-dual code for $j = 1, \ldots, i_2$.*

(iii) *$V_{z_k}$ is the $E_{\underset{\sim}{\tau^{-1}}_{z_k}}$-dual code of $V_{z_k^{-1}}$ for $k = 1, \ldots, i_3$.*

*Proof.* If the code is self-dual, then by Theorem 5.2, $V_{y_j}$ is the $E_{\underset{\sim}{\tau^{-1}}_{x_i}}$-dual of $V_{y_j^{-1}}$. Now,

$$V_{y_j} \text{ is } E_{\underset{\sim}{\tau^{-1}}_{x_i}}\text{-dual of } V_{y_j^{-1}} \iff V_{y_j} = \left\{ \mathbf{v} \in F_{q^{r_{y_j}}}^{e_{y_j}} | E_{\underset{\sim}{\tau^{-1}}_{x_i}}(\mathbf{v}, \mathbf{u}) = 0 \ \forall \mathbf{u} \in V_{y_j^{-1}} \right\}.$$

But,

$$V_{y_j^{-1}} = \left\{ \left( u_1^{q^{\frac{r_{y_j}}{2}}}, \ldots, u_{e_{y_j}}^{q^{\frac{r_{y_j}}{2}}} \right) \middle| \mathbf{u} \in V_{y_j} \right\}.$$

Thus,

$$\begin{aligned}
V_{y_j} \text{ is } E_{\underset{\sim}{\tau^{-1}}_{x_i}}\text{-dual of } V_{y_j^{-1}} &\iff V_{y_j} = \left\{ \mathbf{v} \in F_{q^{r_{y_j}}}^{e_{y_j}} | H_{\underset{\sim}{\tau^{-1}}_{x_i}}(\mathbf{v}, \mathbf{u}) = 0 \ \forall \mathbf{u} \in V_{y_j} \right\} \\
&\iff V_{y_j} \text{ is } H_{\underset{\sim}{\tau^{-1}}_{y_j}} \text{ self-dual.}
\end{aligned}$$

The rest of the proof follows directly from Theorem 5.2. ∎

Let $N_{E_{\mathbf{v}}}(q,l)$ and $N_{H_{\mathbf{v}}}(q,l)$ denote the number of, respectively, $E_{\mathbf{v}}$-self-dual codes and $H_{\mathbf{v}}$-self-dual codes of length $l$ over $F_q$. Also, let $N(q,l)$ denote the number of subspaces of $F_q^l$. All these numbers are known [11, 12] when $\mathbf{v}$ is all-ones and the values are as given below.

$$N(q,l) = \sum_{i=0}^{l} \prod_{j=0}^{i-1} \frac{q^l - q^j}{q^i - q^j}, \tag{11}$$

$$N_{E_{\mathbf{1}}}(q,l) = \begin{cases} \prod_{i=1}^{\frac{l}{2}-1}(q^i+1) & \text{for } q \text{ and } l \text{ even}, \\ 2\prod_{i=1}^{\frac{l}{2}-1}(q^i+1) & \text{for } q \equiv 1 \bmod 4,\ l \text{ even}, \\ 2\prod_{i=1}^{\frac{l}{2}-1}(q^i+1) & \text{for } q \equiv 3 \bmod 4,\ l \text{ is divisible by 4}, \\ 0 & \text{otherwise}, \end{cases} \tag{12}$$

$$N_{H_{\mathbf{1}}}(q,l) = \begin{cases} \prod_{i=0}^{\frac{l}{2}-1}(q^{i+\frac{1}{2}}+1), & \text{when } l \text{ is even}, \\ 0, & \text{otherwise}. \end{cases} \tag{13}$$

Theorem 5.3 directly gives Theorem 5.4.

THEOREM 5.4. *The number of self-dual $G$-invariant codes over $F_q$ is*

$$\prod_{i=1}^{i_1} N_{E_{\underset{\sim}{\tau}^{-1}_{x_i}}}(q^{r_{x_i}}, e_{x_i}) \prod_{j=1}^{i_2} N_{H_{\underset{\sim}{\tau}^{-1}_{y_j}}}(q^{r_{y_j}}, e_{y_j}) \prod_{k=1}^{i_3} N(q^{r_{z_k}}, e_{z_k}),$$

*where the empty product is* 1 *by convention.*

When $|G_1| \equiv |G_2| \equiv \cdots \equiv |G_t| \bmod p$, the $E_{\underset{\sim}{\tau}^{-1}_{x_i}}$-duality and $H_{\underset{\sim}{\tau}^{-1}_{y_j}}$-duality are the same as the Euclidean and Hermitian dualities, respectively. So in that case,

$$N_{E_{\underset{\sim}{\tau}^{-1}_{x_i}}}(q^{r_{x_i}}, e_{x_i}) = N_{E_{\mathbf{1}}}(q^{r_{y_j}}, e_{x_i}),$$
$$N_{H_{\underset{\sim}{\tau}^{-1}_{x_i}}}(q^{r_{y_j}}, e_{y_j}) = N_{H_{\mathbf{1}}}(q^{r_{y_j}}, e_{y_j}).$$

*Example* 5.1 (continuation of Example 3.1). In the following, the number of self-dual $G$-invariant codes is found for different $q$ s.t. $|G_1| \equiv |G_2| \equiv \cdots \equiv |G_t| \bmod p$.

$q \equiv 1 \bmod 3$, $q \equiv 4 \bmod 5$, and $3 \equiv 5 \bmod p$ (e.g., $q = 4$): Different types of cyclotomic residue classes are Type A $\{1_1, 1_2, 1_3, 1_4\}$; Type B $\{g_3^2, g_4^2, g_3^3, g_4^3\}$, $\{g_3, g_4, g_3^4, g_4^4\}$; and Type C $\{g_1, g_2\}$, $\{g_1^2, g_2^2\}$. So the number of self-dual $G$-invariant codes over $F_q$ is $N_E(q,4)N(q,2)(N_H(q^2,2))^2$.

The number of self-dual $G$-invariant codes over $F_q$ for other values of $q$ can be calculated similarly as follows.

$q \equiv 1 \bmod 3$, $q \equiv 1 \bmod 5$, and $3 \equiv 5 \bmod p$ (e.g., $q = 16$): $N_E(q,4)\,(N(q,2))^3$.

$q \equiv 2 \bmod 3$, $q \equiv 2$ or $3 \bmod 5$, and $3 \equiv 5 \bmod p$ (e.g., $q = 2, 8$): $N_E(q,4)N_H(q^2,2)$ $N_H(q^4,2)$.

The values of $N_{E_{\mathbf{v}}}(q,l)$ and $N_{H_{\mathbf{v}}}(q^2,l)$ are not known for arbitrary $\mathbf{v}$. The following theorem allows computation of these quantities for certain cases.

THEOREM 5.5. *If either all components of $\mathbf{v} \in F_q^l$ are quadratic residues in $F_q$ or all components are quadratic nonresidues in $F_q$, then* (1) $N_{E_{\mathbf{v}}}(q,l) = N_E(q,l)$ *and* (2) $N_{H_{\mathbf{v}}}(q^2,l) = N_H(q^2,l)$.

*Proof.* If all the components of $\mathbf{v}$ are quadratic nonresidues in $F_q$, then this vector can be divided by one of its components to get a scalar multiple of the vector, in which each component is a quadratic residue. So, it is sufficient to assume that the components of $\mathbf{v}$ are quadratic residues. Suppose $\mathbf{v} = (v_1, \ldots, v_l) = (s_1^2, \ldots, s_l^2)$.

We shall give a one-to-one correspondence between the $E_{\mathbf{v}}$-self-dual codes and the Euclidean self-dual codes to prove the first part of the result. Let $U \subseteq F_q^l$ be an $E_{\mathbf{v}}$-self-dual code of length $l$ over $F_q$. Then it will be shown that the subspace $W \stackrel{\triangle}{=} \{(s_1a_1, \ldots, s_la_l) | \mathbf{a} = (a_1, \ldots, a_l) \in V\}$ is a Euclidean self-dual code. Suppose $(s_1a_1, \ldots, s_la_l), (s_1b_1, \ldots, s_lb_l) \in W$. Then, $\sum_{i=1}^{l} v_i a_i b_i = 0 \Rightarrow \sum_{i=1}^{l} (s_i a_i)(s_i b_i) = 0$. Thus, any two vectors in $W$ are orthogonal w.r.t. the Euclidean inner product, and since the dimension of $W$ is the same as the dimension of $V$, which is $\frac{l}{2}$, $W$ is a Euclidean self-dual code. The second part follows similarly. □

COROLLARY 5.6. *If $G$ is such that $|G_1| \equiv \cdots \equiv |G_t| \bmod p$ and there is a self-inverse cyclotomic coset $[x]^q \subseteq \mathcal{G}$ with $e_x$ odd, then there is no self-dual $G$-invariant code over $F_q$.*

*Proof.* Both $N_{E_1}(q^{r_x}, e_x)$ and $N_{H_1}(q^{r_x}, e_x)$ are 0 when $e_x$ is odd, and thus the result follows. □

COROLLARY 5.7. *If $G$ is such that $|G_1| \equiv \cdots \equiv |G_t| \bmod p$ and the number $t$ of orbits is odd, then there is no self-dual $G$-invariant code.*

*Proof.* The result follows by applying Corollary 5.6 to the cyclotomic residue class $\{0_j | j = 1, \ldots, t\}$. □

**6. Minimum distance of $G$-invariant codes.** Tanner used a BCH-like argument [14] to estimate minimum distance bounds from the parity check equations over an extension field. The same concept was used to get minimum distance bounds for quasi-cyclic codes from the transform domain description of $F_q$-linear cyclic codes over $F_{q^m}$ [4]. A natural generalization of the results is given here. This can be used to guarantee some minimum distance by viewing the code as a shortened code of an abelian code. For $s$ vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s$ over $F_{q^r}$ of lengths $n_1, n_2, \ldots, n_s$, respectively, let $\mathbf{v}_1 \boxtimes \mathbf{v}_2 \boxtimes \ldots \boxtimes \mathbf{v}_s$ denote the $n_1 \times n_2 \times \cdots \times n_s$ array, known as the Kronecker product of $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s$, with $(i_1, i_2, \ldots, i_s)$th element $v_{1,i_1} v_{2,i_2} \ldots v_{s,i_s}$. The following theorem is available in [4] for the special case of $s = 1$. Here, *power of a vector* will mean the componentwise power, and $I_l$ will denote the set $\{0, 1, \ldots, l-1\}$.

THEOREM 6.1. *Let $r$ be an arbitrary positive integer and the components of each of the vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s$ of lengths $n_1, n_2, \ldots, n_s$, respectively, be nonzero and distinct. If the components of a code $\mathcal{C}$ can be arranged in an $n_1 \times n_2 \times \cdots \times n_s$ array, and if $S$ is a subset of $I_{q^r-1}^s$ such that for each $\mathbf{k} = (k_1, \ldots, k_s) \in S$, the array $\mathbf{v}_1^{k_1} \boxtimes \mathbf{v}_2^{k_2} \boxtimes \ldots \boxtimes \mathbf{v}_s^{k_s}$ is in the span of a set of parity check equations over $F_{q^r}$, then the minimum distance of the code is at least that of the $s$-dimensional cyclic code*

$$\mathcal{C}_c = \left\{ f(X_1, \ldots, X_s) \in \frac{F_{q^r}[X_1, \ldots, X_s]}{((X_1^{q^r-1} - 1), \ldots, (X_s^{q^r-1} - 1))} | f(\beta^{k_1}, \ldots, \beta^{k_s}) = 0 \right.$$
$$\left. \forall (k_1, \ldots, k_s) \in S \right\},$$

*where $\beta$ is a primitive element of $F_{q^r}$.*

*Proof.* Suppose $\mathbf{v}_l = (v_{l,0}, v_{l,1}, \ldots, v_{l,n_l-1})$ with $v_{l,i} = \beta^{\lambda_{l,i}}$, where $\lambda_{l,i} \neq \lambda_{l,j}$ for $i \neq j$ , $\forall l$. For any $\mathbf{a} \in \mathcal{C}$ with weight $\omega_H(\mathbf{a}) = d$, we construct

$$\mathbf{a}' = \sum_{(j_1,\ldots,j_s)\in I^s_{q^r-1}} a_{j_1,\ldots,j_s} X_1^{j_1} \ldots X_s^{j_s} \in \mathcal{C}_c$$

as

$$a'_{\lambda_{1,i_1},\ldots,\lambda_{s,i_s}} = a_{i_1,\ldots,i_s} \text{ for } (i_1,\ldots,i_s) \in I_{n_1} \times I_{n_2}, \times \cdots \times I_{n_s},$$
$$a'_{j_1,\ldots,j_s} = 0 \text{ when } (j_1,\ldots,j_s) \neq (\lambda_{1,i_1},\ldots,\lambda_{s,i_s}) \ \forall (i_1,\ldots,i_s) \in I_{n_1} \times I_{n_2}, \times \cdots \times I_{n_s}.$$

Clearly, $\omega_H(\mathbf{a}') = d$. Now,

$$\begin{aligned}
\mathbf{a} \in \mathcal{C} &\Rightarrow \sum_{i_1=0}^{n_1-1} \cdots \sum_{i_s=0}^{n_s-1} a_{i_1,\ldots,i_s} v_{1,i_1}^{k_1} \ldots v_{s,i_s}^{k_s} = 0 \ \forall \ (k_1,\ldots,k_s) \in S \\
&\Rightarrow \sum_{j_1=0}^{q^r-1} \cdots \sum_{j_s=0}^{q^r-1} a'_{j_1,\ldots,j_s} \beta^{j_1 k_1} \ldots \beta^{i_s k_s} = 0 \qquad \text{”} \\
&\Rightarrow \mathbf{a}' \in \mathcal{C}_c. \qquad \square
\end{aligned}$$

If $(x_1)^q, \ldots, (x_k)^q$ denote the distinct cyclotomic residue classes, then we know that any $G$-invariant code $\mathcal{C}$ is specified by the subspaces $V_{x_1}, \ldots, V_{x_k}$ of

$$F_{q^{r_{x_1}}}^{e_{x_1}}, \ldots, F_{q^{r_{x_k}}}^{e_{x_k}},$$

respectively, from which $A_{\widetilde{x_1}}, \ldots, A_{\widetilde{x_k}}$ take values. Now, each $V_x$ , $x = x_1, \ldots, x_k$, can be considered a linear code over $F_{q^{r_x}}$ of length $e_x$. Thus, $V_x$ is determined by a set of parity check equations. Suppose $\widetilde{x} = \{y_1, \ldots, y_l\}$, where $x = y_i$ for some $i$ and $l = e_x$. Let $\sum_{i=1}^{l} c_i A_{y_i} = 0$ be a parity check equation of $V_x$. Then,

$$\sum_{y\in\mathcal{G}} \left( \sum_{i=1}^{l} c_i \Psi(y, y_i) \right) a_y = 0.$$

Clearly, this gives a parity check equation of $\mathcal{C}$ over $F_{q^{r_x}}$. The componentwise conjugate vectors of the parity check vectors obtained this way and the vectors in their span are also parity check vectors of the code.

Although Theorem 6.1 gives a way to get a minimum distance bound of any linear code, for which a set of parity check equations over an extension field is known, it is very difficult to know which arrangement of the code components, in how many dimensions, and what choice of $\mathbf{v}_l$ will give the maximum bound on the minimum distance. Even for the one-dimensional ($s = 1$) case it is very difficult to choose the best $\mathbf{v}_1$ and arrangement of code components because of the huge number of choices.

**7. Quasi-abelian codes.** For any abelian group $G$, the $G$-quasi-abelian codes of length $t|G|$ (which are submodules of $(F_qG)^t$) are closed under the action of $G$ on the coordinates. So such codes are invariant under the coordinate permutations induced by the elements of $G$. However, this case has a more organized structure in that all the orbits of the coordinates under the action of $G$ are of the same size $|G|$, and there are $t$ such orbits. This raises the following natural reverse question: For a given abelian group $G$ of permutations on code coordinates, when can we view

the $G$-invariant codes as $G$-quasi-abelian codes? The following theorem answers this question.

THEOREM 7.1. *The $G$-invariant codes are $G$-quasi-abelian codes, i.e., they can be viewed as submodules of $(F_qG)^t$ for some $t$ if and only if $|G| = |G_k| \forall k$.*

*Proof.* The forward implication is obvious. If $|G| = |G_k|$, then $g \mapsto g^{(k)}$ is an isomorphism of $G$ onto $G_k$. Thus, any $G$-invariant code can be viewed as a submodule of $(F_qG)^t$. □

Note that to see the $G$-invariant codes as $G$-quasi-abelian codes, $G_{k_1} \simeq G_{k_2} \forall k_1$, $k_2 \in I_t$, is not sufficient.

*Example* 7.1. Consider the group of permutations $G = \langle\{\sigma_1, \sigma_2\}\rangle$ of $\{1, 2, \ldots, 54\}$, where $\sigma_1$ and $\sigma_2$ are as shown in Figure 5. The solid lines with arrows represent the cycles of $\sigma_1$ and the dashed lines with arrows represent the cycles of $\sigma_2$. The order of the group $G$ is 81, whereas the two groups $G_1$ and $G_2$ of restricted permutations are isomorphic to each other and of order 27. So, $G$-invariant codes cannot be seen as $G$-quasi-abelian codes in this case.

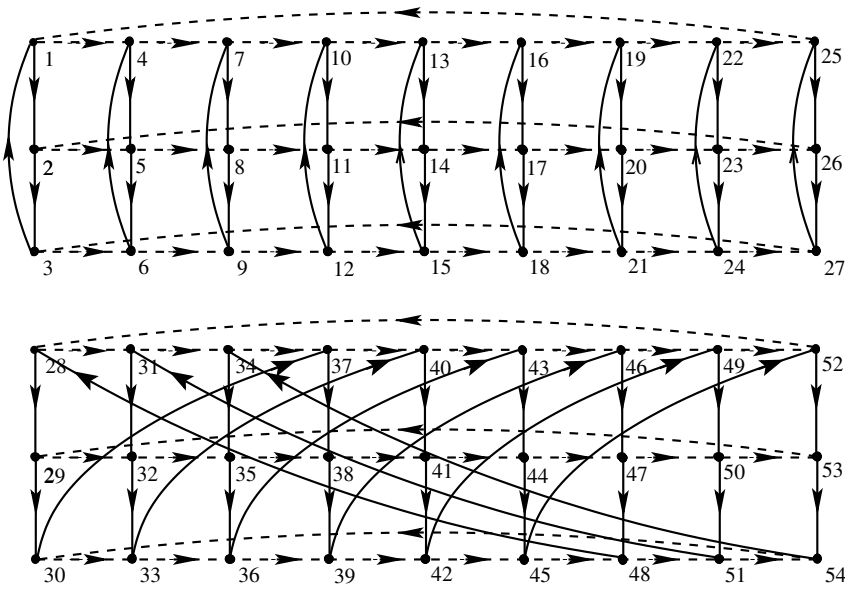


FIG. 5. *Cycle structures of $\sigma_1$ and $\sigma_2$ of Example* 7.1.

For $G$-quasi-abelian codes, we can index the coordinates in different orbits by copies $G_1, \ldots, G_t$ of the same group $G$. Thus, for any element $g \in G$, we have an element $g^{(i)} \in G_i$ for each $i$. So every residue class is of the form $\{g^{(1)}, \ldots, g^{(t)}\}$. We'll denote it by $\widetilde{g}$ instead of $\widetilde{g^{(i)}}$.

If, for a $G$-quasi-abelian code, symbols in some orbits form a set of information symbols and the symbols in the other orbits are the parity check symbols, then the code is called a *systematic $G$-quasi-abelian code*. For a systematic $G$-quasi-abelian code $\mathcal{C} \subseteq (F_qG)^t$ of dimension $k|G|$ $(k \leq t)$, without loss of generality we can assume that the first $k$ orbits are information symbols and the rest are parity check symbols. Then there exist some $\mathbf{c}_{l,j} \in F_qG, l = 1, \ldots, t-k, , j = 1, \ldots, k$, such that each

codeword is of the form

$$\left(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k, \sum_{j=1}^{k} \mathbf{a}_j \mathbf{c}_{1,j}, \sum_{j=1}^{k} \mathbf{a}_j \mathbf{c}_{2,j}, \ldots, \sum_{j=1}^{k} \mathbf{a}_j \mathbf{c}_{t-k,j}\right) \in (F_q G)^t .$$

If the DFTs of $\mathbf{a}_j$ and $\mathbf{c}_{i,j}$ are denoted by $\mathbf{A}_j$ and $\mathbf{C}_{i,j}$, respectively, then each codeword in the transform domain is of the form

$$\left(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_k, \sum_{j=1}^{k} \mathbf{A}_j \odot \mathbf{C}_{1,j}, \sum_{j=1}^{k} \mathbf{A}_j \odot \mathbf{C}_{2,j}, \ldots, \sum_{j=1}^{k} \mathbf{A}_j \odot \mathbf{C}_{t-k,j}\right) \in (F_q G)^t ,$$

where $\odot$ represents the componentwise product.

**7.1. Decoding of systematic quasi-abelian codes.** For a systematic $G$-quasi-abelian code with one information orbit, there are $\mathbf{c}_j \in F_q G$, $j = 1, \ldots, t-1$, such that every codeword is of the form $(\mathbf{a}, \mathbf{c}_1\mathbf{a}, \mathbf{c}_2\mathbf{a}, \ldots, \mathbf{c}_{t-1}\mathbf{a})$. For quasi-cyclic codes, i.e., for cyclic $G$ and when $\mathbf{c}_j$ is a unit in $F_q G$ for $j = 1, \ldots, t-1$, Karlin [7] used alternate syndromes based on $\mathbf{c}_j$, $j = 1, \ldots, t-1$, and their inverses to gain considerable reduction in decoding operations. In the following, Karlin's approach is extended for systematic $G$-quasi-abelian codes with multiple information orbits. This is a two-step generalization of Karlin's algorithm: from quasi-cyclic codes to quasi-abelian codes and from one information orbit, i.e., one-generator codes to multiple generator codes.

For a systematic $G$-quasi-abelian code $\mathcal{C} \subseteq (F_q G)^t$ of dimension $k|G|$ $(k \leq t)$, there exist some $\mathbf{c}_{l,j} \in F_q G, l = 1, \ldots, t-k, j = 1, \ldots, k$, such that each codeword is of the form $\mathbf{a} = (\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k, \mathbf{a}_{k+1}, \ldots, \mathbf{a}_t) \in (F_q G)^t$, where $\mathbf{a}_{k+i} = \sum_{j=1}^{k} \mathbf{a}_j \mathbf{c}_{i,j}$. We restrict our attention to the case where $\mathbf{c}_{i,j}, i = 1, \ldots, t-k, j = 1, \ldots, k$, are such that any $k \times k$ submatrix of the transposed generator matrix

$$M = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ \mathbf{c}_{1,1} & \mathbf{c}_{1,2} & \cdots & \mathbf{c}_{1,k} \\ \mathbf{c}_{2,1} & \mathbf{c}_{2,2} & \cdots & \mathbf{c}_{2,k} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{c}_{t-k,1} & \mathbf{c}_{t-k,2} & \cdots & \mathbf{c}_{t-k,k} \end{pmatrix}$$

is invertible over $F_q G$. That is, any $k$ orbits form a set of information symbols. For any subset $X \subseteq [1, t]$, the $|X| \times k$ submatrix comprising the corresponding rows of $M$ is denoted by $M_X$. Similarly, $\mathbf{a}_X$ will denote the vector of length $|X|$ comprising the components $\mathbf{a}_i \in F_q G$, $i \in X$. We denote the complement $[1, t] \setminus X$ by $\bar{X}$. Thus, if we know $k$ components of a codeword $\mathbf{a}$, i.e., $\mathbf{a}_X$ for some $X$ of size $k$, then we can solve uniquely for the others as $\mathbf{a}_{\bar{X}} = M_{\bar{X}} M_X^{-1} \mathbf{a}_X$.

Suppose $\mathbf{a} = (\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_t)$ is the transmitted codeword and the received vector is $\mathbf{a}' = (\mathbf{a}'_1, \mathbf{a}'_2, \ldots, \mathbf{a}'_t)$. Let $\mathbf{e} = (\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_t) = \mathbf{a}' - \mathbf{a}$ denote the error vector. Suppose the code's known minimum distance is $2l + 1$ and a vector is received with at most $l$ errors, that is, the Hamming weight of the error, $\sum_{i=1}^{t} wt_H(\mathbf{e}_i) \leq l$. Then

the transmitted vector is the only vector of the form

$$\left(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k, \sum_{j=1}^{k} \mathbf{a}_j \mathbf{c}_{1,j}, \sum_{j=1}^{k} \mathbf{a}_j \mathbf{c}_{2,j}, \ldots, \sum_{j=1}^{k} \mathbf{a}_j \mathbf{c}_{t-k,j}\right)$$

having distance from the received vector $\leq l$.

Given a received vector $\mathbf{a}'$, for each $X \subseteq [1,t]$ of size $k$ a syndrome $S_X = M_{\bar{X}} M_X^{-1} \mathbf{a}'_X + \mathbf{a}'_{\bar{X}} = M_{\bar{X}} M_X^{-1} (\mathbf{a}_X + \mathbf{e}_X) + \mathbf{a}_{\bar{X}} + \mathbf{e}_{\bar{X}} = M_{\bar{X}} M_X^{-1} \mathbf{e}_X + \mathbf{e}_{\bar{X}}$ can be computed. Thus, given $\mathbf{e}_X$, $\mathbf{e}_{\bar{X}}$ can be calculated as $\mathbf{e}_{\bar{X}} = S_X - M_{\bar{X}} M_X^{-1} \mathbf{e}_X$. Now, if the error is of weight less than $l$, then there is at least one subset $X$ of size $k$ such that the weight of $\mathbf{e}_X$ is at most $\lfloor \frac{kl}{t} \rfloor$. Thus, if we presume an $\mathbf{e}_X$ of weight at most $\lfloor \frac{kl}{t} \rfloor$, and $wt_H\left(\mathbf{e}_X, S_X - M_{\bar{X}} M_X^{-1} \mathbf{e}_X\right) \leq l$, then $\mathbf{e}_X$ and $\mathbf{e}_{\bar{X}} = S_X - M_{\bar{X}} M_X^{-1} \mathbf{e}_X$ give the actual error.

Now, any $\mathbf{e}_X \in (F_q G)^{|X|}$ can be considered as a vector of length $|X||G|$ over $F_q$. If $\mathbf{e}_X^{(1)}, \mathbf{e}_X^{(2)} \in (F_q G)^{|X|}$ are such that $\mathbf{e}_X^{(1)} = \mathbf{e}_X^{(2)} g$ for some $g \in G$, then we call them equivalent. Let us call the equivalence classes the $G$-quasi-abelian equivalence classes. All the elements of an equivalence class have the same Hamming weight. If we compute $M_{\bar{X}} M_X^{-1} \mathbf{e}_X$ for one representative of an equivalence class, then for any $\mathbf{e}'_X = \mathbf{e}_X g$ in the same equivalence class, $M_{\bar{X}} M_X^{-1} \mathbf{e}'_X = g M_{\bar{X}} M_X^{-1} \mathbf{e}_X$ can be computed from $M_{\bar{X}} M_X^{-1} \mathbf{e}_X$ just by permuting its components.

Using these concepts, the decoding algorithm can be performed as follows.

1. For each subset $X \subseteq [1,t]$ of size $k$ calculate $S_X$.
2. For $i = 0$ to $\lfloor \frac{kl}{t} \rfloor$
3. For each subset $X \subseteq [1,t]$ of size $k$
4. For each $G$-quasi-abelian equivalence class of Hamming weight $i$, take a representative $\mathbf{e}_X$. Compute $M_{\bar{X}} M_X^{-1} \mathbf{e}_X$.
5. For each $g \in G$
6. Compute $\mathbf{e}_{\bar{X}} = S_X - g M_{\bar{X}} M_X^{-1} \mathbf{e}_X$
7. Check if Hamming weight of $\mathbf{e}_{\bar{X}}$ is less than or equal to $t - i$. If so, take $(\mathbf{e}_X, \mathbf{e}_{\bar{X}})$ as the error and quit. Otherwise, continue with the loops.

The number of syndromes (in $(F_q G)^{t-k}$) calculated by this algorithm is $\binom{t}{k}$. If $k = 1$ and $G$ is cyclic, then it specializes to the algorithm proposed by Karlin [7] and Heijnen and van Tilborg [6] for decoding systematic quasi-cyclic codes with a single row of circulants in the generator matrix, i.e., one-generator systematic quasi-cyclic codes. For $t = 2$, it further specializes to the single parity circulant case.

**8. Discussion.** The class of codes considered in this paper is a generalization of cyclic codes, quasi-cyclic codes, abelian codes, and quasi-abelian codes. All these special families of codes are defined as codes closed under one or more permutations of the code components. The algebraic structures of these special families of codes were investigated by different authors and, in all the cases, there seemed to exist some common structure. It is shown in this paper that such structures are not specific to those codes, but these structures are present in the family of $G$-invariant codes for any abelian group $G$ of permutations with order of $G$ relatively prime to $q$.

Also, a twofold extension of Karlin's decoding algorithm for quasi-cyclic codes is given. It is an extension from the case of one-generator systematic quasi-cyclic codes to arbitrary systematic quasi-cyclic codes and also from the case of quasi-cyclic codes to quasi-abelian codes. However, since the algebraic structure of $G$-invariant codes for any arbitrary abelian $G$ (with order relatively prime to $q$) is only as complex as that

of quasi-cyclic codes and quasi-abelian codes, it would be interesting to see whether this decoding algorithm can be extended to cover this general class of codes.

The results of section 5 give as special cases all the results of [9] regarding existence and enumeration of self-dual quasi-cyclic codes. Theorem 5.4 gives the number of self-dual $G$-invariant codes in terms of the number of weighted self-dual codes and weighted Hermitian self-dual codes. Theorem 5.5 enables computation of these numbers in terms of the known numbers for some special cases of weight vectors. It remains an open problem to compute the values of $N_{E_{\mathbf{v}}}(q,l)$ and $N_{H_{\mathbf{v}}}(q,l)$ for arbitrary weight vector $\mathbf{v}$, and thus enable computation of the number of self-dual $G$-invariant codes for arbitrary abelian group $G$ of permutations.

**Acknowledgments.** The authors are very grateful to the anonymous referees for their very careful reading of the manuscript and for their constructive comments towards improving the final version.

REFERENCES

[1] R. E. Blahut, *Algebraic Codes for Data Transmission*, Cambridge University Press, Cambridge, UK, 2003.
[2] J. Conan and G. Seguin, *Structural properties and enumeration of quasi-cyclic codes*, Appl. Algebra Engrg. Comm. Comput., 4 (1993), pp. 25–39.
[3] P. Delsarte, *Automorphisms of abelian codes*, Philips Res. Rep., 25 (1970), pp. 389–403.
[4] B. K. Dey and B. S. Rajan, *$F_q$-linear cyclic codes over $F_{q^m}$: DFT approach*, Des. Codes Cryptogr. to appear.
[5] B. K. Dey and B. S. Rajan, *DFT domain characterization of quasi-cyclic codes*, Appl. Algebra Engrg. Comm. Comput., 13 (2003), pp. 453–474.
[6] P. Heijnen and H. C. A. van Tilborg, *The decoding of binary quasi-cyclic codes*, in Communications and Coding, M. Darnell and B. Honary, eds., Research Studies Press, Taunton, UK, 1998, pp. 146–159.
[7] M. Karlin, *Decoding of circulant codes*, IEEE Trans. Inform. Theory, 16 (1970), pp. 797–802.
[8] K. Lally and P. Fitzpatrick, *Algebraic structure of quasi-cyclic codes*, Discrete Appl. Math., 111 (2001), pp. 157–175.
[9] S. Ling and P. Solé, *On the algebraic structure of quasi-cyclic codes* I*: Finite fields*, IEEE Trans. Inform. Theory, 47 (2001), pp. 2751–2760.
[10] P. Mathys, *Frequency domain description of repeated-root (cyclic) codes*, in Proceedings of the IEEE International Symposium on Information Theory, Trondheim, Norway, 1994, p. 47.
[11] V. Pless, *On the uniqueness of the Golay codes*, J. Combin. Theory Ser. A, 5 (1968), pp. 215–228.
[12] E. M. Rains and N. J. A. Sloane, *Self-dual codes*, in Handbook of Coding Theory, V. S. Pless and W. C. Huffman, eds., Elsevier Science, New York, 1998, pp. 177–294.
[13] B. S. Rajan and M. U. Siddiqi, *Transform domain characterization of Abelian codes*, IEEE Trans. Inform. Theory, 38 (1992), pp. 1817–1821.
[14] R. M. Tanner, *A transform theory for a class of group-invariant codes*, IEEE Trans. Inform. Theory, 34 (1988), pp. 752–775.
[15] S. K. Wasan, *Quasi Abelian codes*, Publ. Inst. Math. (Beograd) N.S., 21 (1977), pp. 201–206.