J. Algebra Comb. Discrete Appl.
5(1) • 5–18

Received: 12 December 2016
Accepted: 6 April 2017

Journal of Algebra Combinatorics Discrete Structures and Applications

Hermitian self-dual quasi-abelian codes

Research Article

Herbert S. Palines, Somphong Jitman, Romar B. Dela Cruz

Abstract: Quasi-abelian codes constitute an important class of linear codes containing theoretically and practically interesting codes such as quasi-cyclic codes, abelian codes, and cyclic codes. In particular, the sub-class consisting of 1-generator quasi-abelian codes contains large families of good codes. Based on the well-known decomposition of quasi-abelian codes, the characterization and enumeration of Hermitian self-dual quasi-abelian codes are given. In the case of 1-generator quasi-abelian codes, we offer necessary and sufficient conditions for such codes to be Hermitian self-dual and give a formula for the number of these codes. In the case where the underlying groups are some p-groups, the actual number of resulting Hermitian self-dual quasi-abelian codes are determined.

2010 MSC: 94B15, 94B60, 16A26

Keywords: Hermitian self-dual codes, Quasi-abelian codes, 1-generator, p-groups

1. Introduction

Quasi-cyclic codes form an important class of linear codes due to their rich algebraic structures, large number of codes with good parameters, and various applications (see [9], [10], [11], [12], [14], [17], and references therein). Let $\mathbb{F}_q$ denote a finite field of order q. It is known that quasi-cyclic codes of length ml and index l over $\mathbb{F}_q$ can be regarded as $\mathbb{F}_q[\mathbb{Z}_m]$-submodules of the $\mathbb{F}_q[\mathbb{Z}_m]$-module $(\mathbb{F}_q[\mathbb{Z}_m])^l$, where $\mathbb{Z}_m$ denotes the cyclic group of order m and $\mathbb{F}_q[\mathbb{Z}_m]$ is the group algebra of $\mathbb{Z}_m$ over $\mathbb{F}_q$ (see [10]).

In a more general setting, quasi-abelian codes are defined by replacing $\mathbb{Z}_m$ with a finite abelian group. Particularly, if G is a finite abelian group and $H \leq G$, then an H-*quasi-abelian code* is defined to be an $\mathbb{F}_q[H]$-submodule of the $\mathbb{F}_q[H]$-module $\mathbb{F}_q[G]$. This class of codes was first introduced in [18] and further studies of their properties have been made in [4, Section 7] and [1]. More recently in [6], via the

Herbert S. Palines; Institute of Mathematical Sciences and Physics, University of the Philippines Los Baños, College, Laguna 4031, Philippines, and Institute of Mathematics, College of Science, University of the Philippines Diliman, Quezon City 1101, Philippines (email: herbertpalines@gmail.com).
Somphong Jitman (Corresponding Author); Department of Mathematics, Faculty of Science, Silpakorn University, Nakhon Pathom 73000, Thailand (email: sjitman@gmail.com).
Romar B. Dela Cruz; Institute of Mathematics, College of Science, University of the Philippines Diliman, Quezon City 1101, Philippines (email: rbdelacruz@math.upd.edu.ph).

Discrete Fourier Transform, the structural characterization of quasi-abelian codes have been established together with the existence of asymptotically good quasi-abelian codes. Quasi-abelian codes serve as the general case for quasi-cyclic codes (if $H \neq G$ is cyclic), abelian codes (if $H = G$), and cyclic codes (if $H = G$ is cyclic). Since the theory of quasi-abelian codes generalizes that of quasi-cyclic codes, a link can be established between 1-generator quasi-abelian codes and irreducible or minimal cyclic codes which plays a central role in the theory of cyclic codes [2].

Self-dual codes form another fascinating family of codes and are known to be closely related with other objects such as lattices and possess variety of practical applications (see [13]). Moreover, both Euclidean and Hermitian self-dual codes have close connection with quantum stabilizer codes [8]. In [6], the authors presented necessary and sufficient conditions for quasi-abelian codes to be Euclidean self-dual and gave enumeration of those codes based on the classification of q-cyclotomic classes of the underlying group. Moreover, they have shown that some class of binary Euclidean self-dual strictly-quasi-abelian codes are asymptotically good.

To the best of our knowledge, no study has been done yet on Hermitian self-dual quasi-abelian codes. It is therefore of natural interest to investigate such family of codes and compare the result of this study with that of [6]. In this work, considering finite abelian groups $H \leq G$, we offer sufficient and necessary conditions for an H-quasi-abelian code in $\mathbb{F}_q[G]$ to be Hermitian self-dual using similar decomposition given in [6, Section 3] (see Proposition 2.3). Consequently, enumeration of Hermitian self-dual H-quasi-abelian codes is presented (see Corollary 3.1). In similar fashion, the sufficient and necessary conditions for a 1-generator quasi-abelian code to be Hermitian self-dual are obtained (see Corollary 4.3). Enumeration of Hermitian self-dual 1-generator quasi-abelian codes is also given. In the case $H \cong (\mathbb{Z}_{p^k})^s$ is a p-group, p is a prime, $k > 0$ and $s > 0$, we classify completely the q-cyclotomic classes of H (see Propositions 3.6 and 3.10) which lead to the actual number of the resulting Hermitian self-dual H-quasi-abelian codes. The asymptotic goodness of Hermitian self-dual strictly-quasi-abelian codes over $\mathbb{F}_{2^{2s}}$ is guaranteed by [6, Section 7] since every code over $\mathbb{F}_{2^{2s}}$ with generator matrix containing only elements from $\mathbb{F}_2$ is Hermitian self-dual if and only if such a matrix generates a Euclidean self-dual code over $\mathbb{F}_2$.

The paper is organized as follows. In Section 2, we recall notations and definitions which are essential to this work as well as the well-known decomposition of semi-simple group algebras. Enumeration of Hermitian self-dual quasi-abelian codes, where the underlying groups are some p-groups, is established in Section 3. Finally in Section 4, we focus on the characterization and enumeration of Hermitian self-dual 1-generator quasi-abelian codes.

2. Preliminaries

For a prime power q and positive integer n, let $\mathbb{F}_q$ denote a finite field of order q and let G be a finite abelian group of order n, written additively. Denote by $\mathbb{F}_q[G]$ the *group algebra* of G over $\mathbb{F}_q$. The elements in $\mathbb{F}_q[G]$ will be written as $\sum_{g\in G} \alpha_g Y^g$, where $\alpha_g \in \mathbb{F}_q$. The addition and the multiplication in $\mathbb{F}_q[G]$ are given as in the usual polynomial rings over $\mathbb{F}_q$ with the indeterminate Y, where the indices are computed additively in G. As convention, Y^0 is treated as the multiplicative identity of $\mathbb{F}_q[G]$, where 0 is the identity of G.

Let R be a finite commutative ring with unity. A linear code of length n over R is defined to be an R-submodule of R^n. A *(linear) code* C in $\mathbb{F}_q[G]$ refers to an $\mathbb{F}_q$-subspace of $\mathbb{F}_q[G]$. This can be viewed as a linear code of length n over $\mathbb{F}_q$ by indexing the n-tuples by the elements of G. For more details, the reader is referred to [6].

Consider a subgroup H of G, a code C in $\mathbb{F}_q[G]$ is called an *H-quasi-abelian code* (specifically, an *H-quasi-abelian code of index l*, where $l := [G : H]$) if C is an $\mathbb{F}_q[H]$-module, i.e., C is closed under addition and multiplication by the elements in $\mathbb{F}_q[H]$. If H is a non-cyclic subgroup of G, then we say that C is a *strictly-quasi-abelian code*. If it is clear in the context or if H is not specified, such a code will be called simply a *quasi-abelian code*. An H-quasi-abelian code C is said to be of 1-*generator* if C is a cyclic $\mathbb{F}_q[H]$-module.

Let $\{\mathfrak{g}_1, \mathfrak{g}_2, \dots, \mathfrak{g}_l\}$ be a fixed set of representatives of the cosets of H in G. Let $\mathcal{R} := \mathbb{F}_q[H]$. Define $\Phi : \mathbb{F}_q[G] \to \mathcal{R}^l$ by

$$\Phi\left(\sum_{h\in H}\sum_{i=1}^{l} \alpha_{h+\mathfrak{g}_i} Y^{h+\mathfrak{g}_i}\right) = \left(\boldsymbol{\alpha}_1(Y), \boldsymbol{\alpha}_2(Y), \dots, \boldsymbol{\alpha}_l(Y)\right),$$

where $\boldsymbol{\alpha}_i(Y) = \sum_{h\in H} \alpha_{h+\mathfrak{g}_i} Y^h \in \mathcal{R}$, for all $i = 1, 2, \dots, l$. It is well known that Φ is an $\mathcal{R}$-module isomorphism interpreted as follows.

Lemma 2.1. *The map Φ induces a one-to-one correspondence between H-quasi-abelian codes in $\mathbb{F}_q[G]$ and linear codes of length l over $\mathcal{R}$.*

In $\mathbb{F}_q^n$, the *Euclidean inner product* of $\boldsymbol{u} = (u_1, u_2, \dots, u_n)$ and $\boldsymbol{v} = (v_1, v_2, \dots, v_n)$ is defined to be $\langle \boldsymbol{u}, \boldsymbol{v}\rangle_{\mathrm{E}} := \sum_{i=1}^{n} u_i v_i$. From this point, we assume $q = q_0^2$, where q_0 is a prime power. Consequently, the *Hermitian inner product* of $\boldsymbol{u}$ and $\boldsymbol{v}$ is defined as $\langle \boldsymbol{u}, \boldsymbol{v}\rangle_{\mathrm{H}} := \sum_{i=1}^{n} u_i \overline{v_i}$, where $\bar{\ }$ is the automorphism on $\mathbb{F}_q$ defined by $\alpha \mapsto \alpha^{q_0}$ for all $\alpha \in \mathbb{F}_q$. For a code C of length n over $\mathbb{F}_q$, let $C^{\perp_{\mathrm{E}}}$ and $C^{\perp_{\mathrm{H}}}$ denote its Euclidean dual and Hermitian dual, respectively. The code C is said to be *Euclidean* (resp., *Hermitian*) *self-dual* if $C^{\perp_{\mathrm{E}}} = C$ (resp., $C^{\perp_{\mathrm{H}}} = C$).

The *Hermitian inner product* in $\mathbb{F}_q[G]$ is defined by

$$\langle \boldsymbol{u}, \boldsymbol{v}\rangle_{\mathrm{H}} := \sum_{g\in G} \alpha_g \overline{\beta_g}$$

for all $\boldsymbol{u} = \sum_{g\in G} \alpha_g Y^g$ and $\boldsymbol{v} = \sum_{g\in G} \beta_g Y^g$ in $\mathbb{F}_q[G]$. The *Hermitian dual* of a code $C \subseteq \mathbb{F}_q[G]$ is given by

$$C^{\perp_{\mathrm{H}}} := \{\boldsymbol{u} \in \mathbb{F}_q[G] \mid \langle \boldsymbol{u}, \boldsymbol{v}\rangle_{\mathrm{H}} = 0 \text{ for all } \boldsymbol{v} \in C\}.$$

Similarly, the code C in $\mathbb{F}_q[G]$ is said to be *Hermitian self-dual* if $C^{\perp_{\mathrm{H}}} = C$. Note that without confusion, we use the symbol $\perp_{\mathrm{H}}$ to indicate both the Hermitian dual of a code over $\mathbb{F}_q$ and the Hermitian dual of a code in $\mathbb{F}_q[G]$. All throughout, the self-duality of quasi-abelian codes is studied with respect to the given Hermitian inner product in $\mathbb{F}_q[G]$.

2.1. Decomposition and Hermitian dual codes

The main tool of this work appears in this subsection. The idea is to have a convenient decomposition of quasi-abelian codes using the well-known decomposition of semi-simple group algebras introduced in [16]. Then, combining this technique with the results of [7, Proposition 2.7] and [6, Proposition 4.1], we obtain characterization of Hermitian self-dual quasi-abelian codes (see Proposition 2.3). This will lead to enumeration of such class of codes.

For completeness, we discuss the concepts of q-cyclotomic classes and primitive idempotents as appeared in [7, Section II.C]. Given coprime positive integers i and j, the *multiplicative order of j modulo i*, denoted by $\mathrm{ord}_i(j)$, is defined to be the smallest positive integer s such that i divides $j^s - 1$. For each $a \in H$, denote by $\mathrm{ord}(a)$ the *additive order* of a in H.

From this point, we assume that $\gcd(|H|, q) = 1$. A *q-cyclotomic class* of H containing $a \in H$, denoted by $S_q(a)$, is defined to be the set

$$S_q(a) := \{q^i \cdot a \mid i = 0, 1, \dots\} = \{q^i \cdot a \mid 0 \le i < \mathrm{ord}_{\mathrm{ord}(a)}(q)\},$$

where $q^i \cdot a := \sum_{j=1}^{q^i} a$ in H.

For a positive integer r and $a \in H$, denote by $-r \cdot a$ the element $r \cdot (-a) \in H$. A q-cyclotomic class $S_q(a)$ is said to be of *type I* if $S_q(a) = S_q(-q_0 \cdot a)$ and it is of *type II* if $S_q(-q_0 \cdot a) \neq S_q(a)$. Clearly, $S_q(0)$ is a q-cyclotomic class of type I.

An *idempotent* in a ring is a non-zero element e such that $e^2 = e$, and it is called *primitive idempotent* if, for every other idempotent f, either $ef = e$ or $ef = 0$. The primitive idempotents in $\mathcal{R} := \mathbb{F}_q[H]$ are induced by the q-cyclotomic classes of H (see [5, Proposition II.4]).

Assume that H contains t q-cyclotomic classes. Without loss of generality, let $\{a_1 = 0, a_2, \dots, a_t\}$ be a set of representatives of the q-cyclotomic classes of H such that $\{a_i \mid i = 1, 2, \dots, r_I\}$ and $\{a_{r_I+j}, a_{r_I+r_{II}+j} = -q_0 \cdot a_{r_I+j} \mid j = 1, 2, \dots, r_{II}\}$ are sets of representatives of q-cyclotomic classes of types I and II, respectively, where $t = r_I + 2r_{II}$. Let $\{e_1, e_2, \dots, e_t\}$ be the set of primitive idempotents of $\mathcal{R}$ induced by $\{S_q(a_i) \mid i = 1, 2, \dots, t\}$, respectively. It is well known that $\mathcal{R}e_i$ is isomorphic to an extension field of $\mathbb{F}_q$ of degree $|S_q(a_i)|$ for each $i = 1, 2, \dots, t$.

In [16], $\mathcal{R} := \mathbb{F}_q[H]$ is decomposed in terms of e_i's. Later, the components in the decomposition of $\mathcal{R}$ are rearranged in [7] and obtain the following.

$$\mathcal{R} = \bigoplus_{i=1}^{t} \mathcal{R}e_i \cong \left(\prod_{i=1}^{r_I} \mathbb{E}_i \right) \times \left(\prod_{j=1}^{r_{II}} (\mathbb{K}_j \times \mathbb{K}'_j) \right), \tag{1}$$

where $\mathbb{E}_i \cong \mathcal{R}e_i$, $\mathbb{K}_j \cong \mathcal{R}e_{r_I+j}$, and $\mathbb{K}'_j \cong \mathcal{R}e_{r_I+r_{II}+j}$ are finite extension fields of $\mathbb{F}_q$ for all $i = 1, 2, \dots, r_I$ and $j = 1, 2, \dots, r_{II}$.

Remark 2.2. *It is known that* $\mathbb{E}_i \cong \mathbb{F}_{q^{s_i}}$, $\mathbb{K}_j \cong \mathbb{F}_{q^{t_j}}$ *and* $\mathbb{K}'_j \cong \mathbb{F}_{q^{t'_j}}$, *where* $s_i := |S_q(a_i)|$, $t_j := |S_q(a_{r_I+j})|$, *and* $t'_j := |S_q(a_{r_I+r_{II}+j})|$ *for* $i = 1, 2, \dots, r_I$ *and* $j = 1, 2, \dots, r_{II}$. *Note that* $|S_q(a_{r_I+j})| = |S_q(a_{r_I+r_{II}+j})|$ *for each* $j = 1, 2, \dots, r_{II}$. *Thus,* $\mathbb{K}_j \cong \mathbb{K}'_j$ *for each* $j = 1, 2, \dots, r_{II}$.

From (1), we have

$$\mathbb{F}_q[G] \cong \mathcal{R}^l \cong \left(\prod_{i=1}^{r_I} \mathbb{E}_i^l \right) \times \left(\prod_{j=1}^{r_{II}} (\mathbb{K}_j^l \times {\mathbb{K}'_j}^l) \right), \tag{2}$$

where the isomorphisms are $\mathcal{R}$-module isomorphisms. They can be viewed as $\mathbb{F}_q$-linear isomorphisms as well. Consequently, every quasi-abelian code C in $\mathbb{F}_q[G]$ can be viewed as

$$C \cong \left(\prod_{i=1}^{r_I} C_i \right) \times \left(\prod_{j=1}^{r_{II}} \left(D_j \times D'_j \right) \right), \tag{3}$$

where C_i, D_j and D'_j are linear codes of length l over $\mathbb{E}_i$, $\mathbb{K}_j$, and $\mathbb{K}'_j$, respectively, for all $i = 1, 2, \dots, r_I$ and $j = 1, 2, \dots, r_{II}$.

Using arguments similar to the proofs of [7, Proposition 2.7] and [6, Proposition 4.1], it can be concluded that the Hermitian dual of C is of the form

$$C^{\perp_{\mathrm{H}}} \cong \left(\prod_{i=1}^{r_I} C_i^{\perp_{\mathrm{H}}} \right) \times \left(\prod_{j=1}^{r_{II}} \left((D'_j)^{\perp_{\mathrm{E}}} \times D_j^{\perp_{\mathrm{E}}} \right) \right). \tag{4}$$

From (3) and (4), we have the following necessary and sufficient conditions for quasi-abelian codes to be Hermitian self-dual.

Proposition 2.3. *An H-quasi-abelian code C in $\mathbb{F}_q[G]$ is Hermitian self-dual if and only if, in the decomposition (3),*

i) C_i *is Hermitian self-dual for all* $i = 1, 2, \dots, r_I$, *and*

ii) $D'_j = D_j^{\perp_{\mathrm{E}}}$ *for all* $j = 1, 2, \dots, r_{II}$.

3. Enumeration of Hermitian self-dual quasi-abelian codes

In this section, we enumerate Hermitian self-dual quasi-abelian codes by using the decomposition in (3), Proposition 2.3 and the following formulas. Let $N(q,l)$ (resp., $N_{\rm H}(q,l)$) denote the number of linear codes (resp., Hermitian self-dual codes) of length l over $\mathbb{F}_q$. It is well known (see [15] and [13]) that

$$N(q,l)=\sum_{i=0}^{l}\prod_{j=0}^{i-1}\frac{q^l-q^j}{q^i-q^j}, \tag{5}$$

$$N_{\rm H}(q,l)=\begin{cases}\prod_{i=0}^{\frac{l}{2}-1}(q^{i+\frac{1}{2}}+1) & \text{if } l \text{ is even,}\\ 0 & \text{otherwise,}\end{cases} \tag{6}$$

where the empty product is set to be 1.

In general, to count the number of Hermitian self-dual quasi-abelian codes in $\mathbb{F}_q[G]$, in (3), we count the number of Hermitian self-dual codes C_i of length l over $\mathbb{F}_{q^{s_i}}$ for all $i=1,2,\dots,r_I$ and multiply it with the number of all possible linear codes D_j of length l over $\mathbb{F}_{q^{t_j}}$ for all $j=1,2,\dots,r_{II}$. This technique is clear in the following corollary. Hereafter, the numbers s_i, t_j, and t'_j will appear frequently in the succeeding results. If needed, the reader is referred back to Remark 2.2 for the definitions of s_i, t_j, and t'_j.

Corollary 3.1. *Let $H\le G$ be finite abelian groups such that $\gcd(|H|,q)=1$ and $l=[G:H]$. Assume that $\mathbb{F}_q[H]$ contains r_I (resp., $2r_{II}$) primitive idempotents of type I (resp., II). Assume further that the primitive idempotents of type I are induced by q-cyclotomic classes of size s_i for each $i=1,2,\dots,r_I$ and the primitive idempotents of type II are induced by q-cyclotomic classes of sizes t_j and t'_j, pair-wise, for each $j=1,2,\dots,r_{II}$. Then the number of Hermitian self-dual H-quasi-abelian codes in $\mathbb{F}_q[G]$ is*

$$\prod_{i=1}^{r_I}N_{\rm H}(q^{s_i},l)\prod_{j=1}^{r_{II}}N(q^{t_j},l). \tag{7}$$

We note that $S_q(0)$ is a q-cyclotomic class of H of type I. Then $r_I\ge 1$, and hence, the product $\prod_{i=1}^{r_I}N_{\rm H}(q^{s_i},l)=0$ for all odd positive integers l. Hence, there are no Hermitian self-dual H-quasi-abelian codes if $l=[G:H]$ is odd. Therefore, we have the following result derived from (6) and (7).

Lemma 3.2. *There exists a Hermitian self-dual H-quasi-abelian code in $\mathbb{F}_q[G]$ if and only if the index $l=[G:H]$ is even.*

Remark 3.3. *From Lemma 3.2, it is apparent that given a finite abelian group G and $q=q_0^2$, the existence of Hermitian self-dual H-quasi-abelian codes in $\mathbb{F}_q[G]$ depends only on the choice of H, particularly on index l being even.*

In the theory of quasi-cyclic codes, it is practical to use a relatively small fixed value of the index l mainly for the purpose of efficient decoding [3]. Moreover, this case contains the known case of double circulant codes (see [10, Section VI.A] and [12, Section II.A]). Since the theory of quasi-abelian codes generalizes that of quasi-cyclic codes, we can adopt those concepts. Note that a quasi-cyclic code is cyclic when $l=1$. Thus $l=2$ is the smallest index such that a code is quasi-cyclic. Specifically for $l=2$, one can talk about self-dual 1-generator quasi-abelian codes (see Section 4). Consider the example below for the number of quasi-abelian codes of index 2.

Example 3.4. *Let $H\le G$ be finite abelian groups such that $\gcd(|H|,q)=1$ and $l=[G:H]=2$. Assume that $\mathbb{F}_q[H]$ contains r_I (resp., $2r_{II}$) primitive idempotents of type I (resp., II). Assume further that the primitive idempotents of type I are induced by q-cyclotomic classes of size s_i for each $i=1,2,\dots,r_I$ and the primitive idempotents of type II are induced by q-cyclotomic classes of sizes t_j and t'_j, pair-wise, for* *each $j = 1, 2, \ldots, r_{II}$. Then the number of Hermitian self-dual H-quasi-abelian codes of index 2 in $\mathbb{F}_q[G]$ is*

$$\prod_{i=1}^{r_I}(q_0^{s_i}+1)\prod_{j=1}^{r_{II}}(q^{t_j}+3).$$

In the next two subsections, we consider the case where the subgroups H of G are some p-groups. It is interesting to see that for this particular case, the cardinality and the number of q-cyclotomic classes of H can be explicitly determined. Hence, one can obtain the actual number of resulting Hermitian self-dual H-quasi-abelian codes. In this regard, we offer sufficient and necessary conditions for a q-cyclotomic class of H to be of type I or type II.

3.1. $H \cong (\mathbb{Z}_{2^k})^s$

The succeeding discussion is instrumental in determining the explicit forms of r_I and r_{II}. Let $H \cong (\mathbb{Z}_{p^k})^s$, where k and s are positive integers, and p is prime such that $\gcd(p, q) = 1$. Define

$$H_{p^i} := \{h \in H |\, \mathrm{ord}(h) = p^i\},$$

for each $0 \le i \le k$. Observe that $H_1, H_p, \ldots, H_{p^k}$ are pair-wise disjoint and $H = H_1 \cup H_p \cup \cdots \cup H_{p^k}$, where $H_1 = \{0\}$. For each $1 \le i \le k$, it is not difficult to see that $H_{p^i} = \left(p^{k-i}\mathbb{Z}_{p^k}\right)^s \setminus \left(p^{k-(i-1)}\mathbb{Z}_{p^k}\right)^s$. Consequently, we have $|H_1| = 1$ and, via inclusion-exclusion principle,

$$|H_{p^i}| = p^{is} - p^{(i-1)s},$$

for each $i = 1, 2, \ldots, k$. Recall that $q = q_0^2$ where q_0 is a prime power. Hereafter, let $\nu_{p^i} := \mathrm{ord}_{p^i}(q)$ and $\mu_{p^i} := \mathrm{ord}_{p^i}(q_0)$, for $i = 0, 1, \ldots, k$. Note that if $h \in H_{p^i}$, $|S_q(h)| = \mathrm{ord}_{\mathrm{ord}(h)}(q) = \nu_{p^i}$.

Now, consider the case where q is odd and $p = 2$, i.e., $H \cong (\mathbb{Z}_{2^k})^s$. Suppose $h \in H_2$. Since $\mathrm{ord}(h) = 2$ for all $h \in H_2$, $q \equiv \pm 1 \pmod{\mathrm{ord}(h)}$ and $q_0 \equiv \pm 1 \pmod{\mathrm{ord}(h)}$, then we have $h = q \cdot h = q_0 \cdot h = q_0 \cdot (-h) = -q_0 \cdot h$. Then $S_q(h) = S_q(-q_0 \cdot h)$ is of type I and having cardinality equal to 1. For the case where $h \in H_{2^i}$, $2 \le i \le k$, we have the same result. Suppose $h \in H_{2^i}$, for a given $2 \le i \le k$, and assume $S_q(h)$ is of type I. Then $|S_q(h)| = \nu_{2^i}$ is odd (see [7, Remark 2.6 (2)]). Moreover, the elements of H_{2^i} are partitioned into q-cyclotomic classes of the same type and size (see [7, Remark 2.5 (ii)]). Thus, ν_{2^i} divides $|H_{2^i}|$. In particular, ν_{2^i} divides $|2^{k-i}\mathbb{Z}_{2^k} \setminus 2^{k-i+1}\mathbb{Z}_{2^k}| = 2^i - 2^{i-1} = 2^{i-1}$. Since ν_{2^i} is odd, it must be 1.

Furthermore, it can be shown that $\mu_{2^i} = 2$ for all $i = 2, 3, \ldots, k$. Note that $2^i \mid (q-1)$ since $\nu_{2^i} = 1$ and thus, $2^i \mid (q_0^2 - 1)$. We show that indeed, $\mu_{2^i} = 2$. Suppose contrary, i.e., $\mu_{2^i} = 1 = \nu_{2^i}$. It implies that $q_0 \cdot h = h$ and $-h = -q_0 \cdot h = q \cdot h = h$, since $S_q(h)$ is assumed to be of type I. It implies that $h = 0$ or $\mathrm{ord}(h) = 2$ which contradicts that $h \in H_{2^i}$, $i = 2, 3, \ldots, k$. We state these observations in the following lemma.

Lemma 3.5. *Let $h \in H_{2^i}$, for a given $0 \le i \le k$. If $S_q(h)$ is of type I, then $\nu_{2^i} = 1$. Moreover, $\mu_{2^i} = 2$ for all $i = 2, 3, \ldots, k$.*

In the next proposition, we give the necessary and sufficient conditions for a q-cyclotomic class of H to be of type I or type II. Since all q-cyclotomic classes in H_{2^i} are of the same type and size, we characterize the q-cyclotomic classes of H through its subsets H_{2^i}, for $0 \le i \le k$, keeping in mind that $S_q(h)$ is always of type I, for all $h \in H_1 \cup H_2$.

Proposition 3.6. *Let $h \in H_{2^i}$, for a given $0 \le i \le k$. Then $S_q(h)$ is of type I if and only if $q_0 \equiv -1 \pmod{2^i}$. Equivalently, $S_q(h)$ is of type II if and only if $q_0 \not\equiv -1 \pmod{2^i}$.*

Proof. Clearly, the proposition holds for the case where $h \in H_1 \cup H_2$. Now, consider $h \in H_{2^i}$, for a given $2 \le i \le k$, and assume $S_q(h)$ is of type I. From Lemma 3.5, $\nu_{2^i} = 1$ and $\mu_{2^i} = 2$. Thus, $q \equiv 1 \pmod{2^i}$ and $q_0 \not\equiv 1 \pmod{2^i}$. Hence, $q_0 \equiv -1 \pmod{2^i}$.

On the other hand, assume $q_0 \equiv -1 \pmod{2^i}$. Thus, for each $h \in H_{2^i}$, $-q_0 \cdot h = h \in S_q(h)$. Hence, $S_q(h)$ is of type I. □

Remark 3.7. *Using Proposition 3.6, we can completely classify the sets H_{2^i}, $0 \le i \le k$, that contain q-cyclotomic classes of type I or type II. Choose the largest integer $0 \le r' \le k$ such that $2^{r'} | (q_0 + 1)$. Hence, by Proposition 3.6 H_{2^i} contains q-cyclotomic classes of type I for all $i = 0, 1, \ldots, r'$ and the rest of the sets H_{2^j} contain elements of type II, for $j = r' + 1, \ldots, k$. This will lead to a decomposition of $\mathbb{F}_q[H]$.*

Let r' be a positive integer as described in Remark 3.7. Since $\nu_{2^i} = 1$ for all $0 \le i \le r'$, then

$$r_I = \sum_{i=0}^{r'} \frac{|H_{2^i}|}{\nu_{2^i}} = 2^{r's}$$

and

$$r_{II} = \sum_{r=r'+1}^{k} \frac{|H_{2^r}|}{2\nu_{2^r}} = \sum_{r=r'+1}^{k} \frac{2^{rs} - 2^{(r-1)s}}{2\nu_{2^r}}.$$

Thus, from (1), this will give the following decomposition,

$$\mathbb{F}_q[H] \cong \left(\prod_{i=1}^{2^{r's}} \mathbb{F}_q \right) \times \left(\prod_{r=r'+1}^{k} \left(\prod_{j'=1}^{\frac{2^{rs}-2^{(r-1)s}}{2\nu_{2^r}}} (\mathbb{F}_{q^{\nu_{2^r}}} \times \mathbb{F}_{q^{\nu_{2^r}}}) \right) \right).$$

Similar with (3), every H-quasi-abelian code C in $\mathbb{F}_q[G]$ can be written as

$$C \cong \left(\prod_{i=1}^{2^{r's}} C_i \right) \times \left(\prod_{r=r'+1}^{k} \left(\prod_{j'=1}^{\frac{2^{rs}-2^{(r-1)s}}{2\nu_{2^r}}} (D_{r,j'} \times D'_{r,j'}) \right) \right), \tag{8}$$

where C_i, $D_{r,j'}$ and $D'_{r,j'}$ are linear codes of length l over $\mathbb{F}_q$, $\mathbb{F}_{q^{\nu_{2^r}}}$ and $\mathbb{F}_{q^{\nu_{2^r}}}$, respectively, for $i = 1, 2, \ldots, 2^{r's}$, $r = r' + 1, \ldots, k$, and $j' = 1, 2, \ldots, (2^{rs} - 2^{(r-1)s})/2\nu_{2^r}$. Given the decomposition of C in (8), we deduce the next proposition.

Proposition 3.8. *Let $H \le G$ be finite abelian groups such that $H \cong (Z_{2^k})^s$, $\gcd(|H|, q) = 1$ and $l = [G : H]$. Let $0 \le r' \le k$ be the largest integer such that $2^{r'} | (q_0 + 1)$. The number of Hermitian self-dual H-quasi-abelian codes in $\mathbb{F}_q[G]$ is*

$$\begin{cases} \left(\prod_{i=0}^{\frac{l}{2}-1} (q^{i+\frac{1}{2}} + 1)^{2^{r's}} \right) \left(\prod_{r=r'+1}^{k} \left(\sum_{i=0}^{l} \prod_{j=0}^{i-1} \frac{(q^{\nu_{2^r}})^l - (q^{\nu_{2^r}})^j}{(q^{\nu_{2^r}})^i - (q^{\nu_{2^r}})^j} \right)^{\frac{2^{rs}-2^{(r-1)s}}{2\nu_{2^r}}} \right) & \text{if } l \text{ is even,} \\ 0 & \text{if } l \text{ is odd.} \end{cases}$$

Proof. The result follows from (8) and Proposition 2.3 by counting the number of all possible Hermitian self-dual linear codes C_i over $\mathbb{F}_q$ of length l and linear codes $D_{r,j'}$ over $\mathbb{F}_{q^{\nu_{2^r}}}$ of length l, for $i = 1, 2, \ldots, r's$, $r = r' + 1, \ldots, k$, and $j' = 1, 2, \ldots, (2^{rs} - 2^{(r-1)s})/2\nu_{2^r}$, then apply formulas (5) and (6). □

A specific case of Proposition 3.8 is given in the example below, where $H \cong (\mathbb{Z}_2)^s$ (i.e., $r' = k = 1$) is an elementary 2-group.

Example 3.9. *Let $H \leq G$ be finite abelian groups such that $H \cong (\mathbb{Z}_2)^s$, $\gcd(|H|, q) = 1$ and $l = [G : H]$. The number of Hermitian self-dual H-quasi-abelian codes in $\mathbb{F}_q[G]$ is*

$$\begin{cases} \prod_{i=0}^{\frac{l}{2}-1} (q^{i+\frac{1}{2}} + 1)^{2^s} & \text{if } l \text{ is even,} \\ 0 & \text{if } l \text{ is odd.} \end{cases}$$

Table 3.1 illustrates Proposition 3.8 when $q = 9$, $l = 2$, for $k = 1, 2$ and $s = 1, 2$. Note that in the last column, $A \cdot B$ gives the number of the resulting codes. Moreover, since the value of $k \leq 2$ and $q_0 = 3$, then $r' = k$, for $k = 1, 2$. Hence, the second factor in the formula given by B is empty and set to be 1. In other words, all cyclotomic classes of H is of type I, for $k = 1, 2$. In this case, the numbers in the last column of the table also gives the number of Hermitian self-dual 1-generator H-quasi-abelian codes as presented in Corollary 4.5 (i).

Table 1. Number of Hermitian self-dual H-quasi-abelian codes in $\mathbb{F}_q[G]$, $H \cong (\mathbb{Z}_{2^k})^s$, $l = [G : H] = 2$ and $q = 9$.

s	k	$\|H\|$	$\|G\|$	r'	$A = (q_0 + 1)^{2^{r'}s}$	$B = \prod_{r=r'+1}^{k} (q^{\nu_{2^r}} + 3)^{\|H_{2^r}\|/2\nu_{2^r}}$	$A \cdot B$
1	1	2	4	1	16	1	16
	2	4	8	2	256	1	256
2	1	4	8	1	256	1	256
	2	16	32	2	4^{16}	1	4^{16}

3.2. $H \cong (\mathbb{Z}_{p^k})^s$, where p is an odd prime

To complete our characterization, consider $H \cong (\mathbb{Z}_{p^k})^s$, $k, s > 0$, where p is an odd prime and $\gcd(p, q) = 1$. Recall that in the case $p = 2$, there is a chance that the q-cyclotomic classes of H are divided exactly into classes of type I and type II. It is interesting to note that it is a totally different situation when p is odd. Specifically, we show that all non-zero elements in H belong to just one type of q-cyclotomic classes. Moreover, the necessary and sufficient conditions for them to be of type I or type II are determined. Recall that H_{p^i} is the set containing all elements of H of order p^i, $i = 0, 1, \ldots, k$ and $H = H_1 \cup H_p \cup \cdots \cup H_{p^k}$. Note that $S_q(0) = \{0\} = H_1$ is of type I. We start with H_p the characterization of q-cyclotomic classes of H.

Proposition 3.10. *Let $h \in H_p$. Then $S_q(h)$ is of type I if and only if $\mathrm{ord}_p(q)$ is odd and $\mathrm{ord}_p(q_0)$ is even. Equivalently, $S_q(h)$ is of type II if and only if $\mathrm{ord}_p(q)$ is even or $\mathrm{ord}_p(q_0)$ is odd.*

Proof. Following the notation introduced above, let $\nu_p = \mathrm{ord}_p(q)$. If $h \in H_p$, then $q^{\nu_p} \cdot h = h$.

Assume $S_q(h)$ is of type I. Then $-q_0 \cdot h = q^i \cdot h = q_0^{2i} \cdot h$ for some $0 \leq i < \nu_p$. It follows that $h = -q_0^{2i-1} \cdot h = -q_0^{2i-2}(q_0 \cdot h) = -q_0^{2i-2}(-q_0^{2i} \cdot h) = q_0^{2(2i-1)} \cdot h = q^{(2i-1)} \cdot h$ which implies $\nu_p | (2i - 1)$. Hence, ν_p is odd. We note that $\mathrm{ord}_p(q_0) \in \{\nu_p, 2\nu_p\}$. If $\mathrm{ord}_p(q_0) = \nu_p$, then $h = q_0^{\nu_p} \cdot h = q_0^{2i-1} \cdot h = -h$, which implies that $h = 0$, a contradiction. Hence, $\mathrm{ord}_p(q_0) = 2\nu_p$, which is even.

Conversely, assume that $\mathrm{ord}_p(q)$ is odd and $\mathrm{ord}_p(q_0)$ is even. It follows that $\mathrm{ord}_p(q) = \nu_p$ and $\mathrm{ord}_p(q_0) = 2\nu_p$. Then $h = q^{\nu_p} \cdot h = q_0^{2\nu_p} \cdot h$, i.e., $(q_0^{\nu_p} - 1)(q_0^{\nu_p} + 1) \cdot h = 0$. Since $\mathrm{ord}_p(q_0) = 2\nu_p$, we have $p \nmid (q_0^{\nu_p} - 1)$, and hence, $(q_0^{\nu_p} + 1) \cdot h = 0$. It follows that $q_0(q_0^{\nu_p} + 1) \cdot h = (q^{\frac{\nu_p+1}{2}} + q_0) \cdot h = 0$. Since ν_p is odd, $\nu_p + 1$ is even. Which implies that $-q_0 \cdot h = q^{\frac{\nu_p+1}{2}} \cdot h \in S_q(h)$. Therefore, $S_q(h)$ is of type I as desired. □

Next, we show that all q-cyclotomic classes of $H \setminus \{0\}$ are of the same type. Because of this, the q-cyclotomic classes of H are completely characterized.

Proposition 3.11. *Let $a \in H_p$ and $b \in H_{p^i}$, for any given $1 \leq i \leq k$. Then, $S_q(a)$ is of type I if and only if $S_q(b)$ is of type I. Equivalently, $S_q(a)$ is of type II if and only if $S_q(b)$ is of type II.*

Proof. Let $a \in H_p$ and assume that $S_q(a)$ is of type I. Then, by Proposition 3.10, $\nu_p = \mathrm{ord}_p(q)$ is odd and $\mu_p = \mathrm{ord}_p(q_0) = 2\nu_p$ is even. We show that $p^i \mid \left(q^{\nu_p \cdot p^{i-1}} - 1\right)$ by induction on i. It is clear when $i = 1$. Now, assume $p^{i-1} \mid \left(q^{\nu_p \cdot p^{i-2}} - 1\right)$, for $1 < i \leq k$. Then, $q^{\nu_p \cdot p^{i-2}} \equiv 1 \,(\mathrm{mod}\ p^{i-1})$ and hence, $q^{\nu_p \cdot p^{i-2} \cdot j} \equiv 1 \,(\mathrm{mod}\ p^{i-1})$ for all $j \geq 0$. Thus, $\sum_{j=0}^{p-1} q^{\nu_p \cdot p^{i-2} \cdot j} \equiv \sum_{j=0}^{p-1} 1 \,(\mathrm{mod}\ p^{i-1})$. This implies that $p \mid \left(\sum_{j=0}^{p-1} q^{\nu_p \cdot p^{i-2} \cdot j}\right)$. Since $q^{\nu_p \cdot p^{i-1}} - 1 = \left(q^{\nu_p \cdot p^{i-2}} - 1\right)\left(\sum_{j=0}^{p-1} q^{\nu_p \cdot p^{i-2} \cdot j}\right)$, $p^{i-1} \mid \left(q^{\nu_p \cdot p^{i-2}} - 1\right)$ and $p \mid \left(\sum_{j=0}^{p-1} q^{\nu_p \cdot p^{i-2} \cdot j}\right)$, it follows that $p^i \mid \left(q^{\nu_p \cdot p^{i-1}} - 1\right)$. Therefore, $\nu_{p^i} \mid \nu_p \cdot p^{i-1}$ and means ν_{p^i} is odd. Note that $\mu_{p^i} \in \{\nu_{p^i}, 2\nu_{p^i}\}$. Since μ_p is even, ν_{p^i} is odd and $\mu_p \mid \mu_{p^i}$ hence, $\mu_{p^i} = 2\nu_{p^i}$. Hence, $p^i \mid \left(q_0^{2\nu_{p^i}} - 1\right)$ and $p^i \nmid \left(q_0^{\nu_{p^i}} - 1\right)$. It follows that $p^i \mid \left(q_0^{\nu_{p^i}} + 1\right)$. In other words, $q_0(q_0^{\nu_{p^i}} + 1) \cdot b = 0$ or $-q_0 \cdot b = q_0^{\nu_{p^i}+1} \cdot b = q^{\frac{\nu_{p^i}+1}{2}} \cdot b \in S_q(b)$ for each $b \in H_{p^i}$.

Conversely, assume that $S_q(b)$ is of type I, for all $b \in H_{p^i}$. Then, $-q_0 \cdot b = q^j \cdot b$ for some $0 \leq j < \nu_{p^i}$. It follows that $-q_0(p^{i-1} \cdot b) = q^j(p^{i-1} \cdot b)$, which implies $S_q(p^{i-1} \cdot b)$ is of type I. Since $p^{i-1} \cdot b \in H_p$, $S_q(a)$ and $S_q(p^{i-1} \cdot b)$ are of the same type. □

Combining Propositions 3.10 and 3.11, the corollary below follows immediately.

Corollary 3.12. *Let h be a non-zero element in $H \cong (\mathbb{Z}_{p^k})^s$, p is odd and $\gcd(p, q) = 1$. Then $S_q(h)$ is of type I if and only if $\mathrm{ord}_p(q)$ is odd and $\mathrm{ord}_p(q_0)$ is even. Equivalently, $S_q(h)$ is of type II if and only if $\mathrm{ord}_p(q)$ is even or $\mathrm{ord}_p(q_0)$ is odd.*

We are now ready to obtain a decomposition for $\mathbb{F}_q[H]$. This entails computing for r_I and r_{II}. If there exists $h \in H \setminus \{0\}$ such that $S_q(h)$ is of type I, then by Corollary 3.12, $r_{II} = 0$ and

$$r_I = \sum_{i=0}^{k} \frac{|\ H_{p^i}\ |}{\nu_{p^i}} = \sum_{i=0}^{k} \frac{p^{is} - p^{(i-1)s}}{\nu_{p^i}},$$

where $\nu_{p^0} = \nu_1 = 1$ and $p^{is} - p^{(i-1)s}$ is equal to 1 when $i = 0$. On the other hand, if there exists $h \in H \setminus \{0\}$ such that $S_q(h)$ is of type II, then Corollary 3.12 implies that $r_I = |H_1| = 1$ and

$$r_{II} = \sum_{i=1}^{k} \frac{|\ H_{p^i}\ |}{2\nu_{p^i}} = \sum_{i=1}^{k} \frac{p^{is} - p^{(i-1)s}}{2\nu_{p^i}}.$$

Recall that $\nu_p := \mathrm{ord}_p(q)$ and $\mu_p := \mathrm{ord}_p(q_0)$. From the above calculations, together with Corollary 3.12 and (1), we have

$$\mathbb{F}_q[H] \cong \begin{cases} \mathbb{F}_q \times \left(\prod_{i=1}^{k} \left(\prod_{j'=1}^{\frac{2^{is} - 2^{(i-1)s}}{\nu_{p^i}}} \mathbb{F}_{q^{\nu_{p^i}}} \right) \right) & \text{if } \nu_p \text{ is odd and } \mu_p \text{ is even,} \\ \mathbb{F}_q \times \left(\prod_{i=1}^{k} \left(\prod_{j=1}^{\frac{2^{is} - 2^{(i-1)s}}{2\nu_{p^i}}} \left(\mathbb{F}_{q^{\nu_{p^i}}} \times \mathbb{F}_{q^{\nu_{p^i}}} \right) \right) \right) & \text{if } \nu_p \text{ is even or } \mu_p \text{ is odd.} \end{cases}$$

It also implies that an H-quasi-abelian code C in $\mathbb{F}_q[G]$ can be decomposed as

$$C \cong \begin{cases} C_1 \times \left(\prod_{i=1}^{k} \left(\prod_{j'=1}^{\frac{2^{is}-2^{(i-1)s}}{\nu_{p^i}}} C_{i,j'} \right) \right) & \text{if } \nu_p \text{ is odd and } \mu_p \text{ is even,} \\ C_1 \times \left(\prod_{i=1}^{k} \left(\prod_{j=1}^{\frac{2^{is}-2^{(i-1)s}}{2\nu_{p^i}}} (D_{i,j} \times D'_{i,j}) \right) \right) & \text{if } \nu_p \text{ is even or } \mu_p \text{ is odd,} \end{cases} \tag{9}$$

where C_1 and $C_{i,j'}$ are linear codes of length l over $\mathbb{F}_q$ and $\mathbb{F}_{q^{\nu_{p^i}}}$, respectively, for $i = 1, 2, \ldots, k$ and $j' = 1, 2, \ldots, (2^{is} - 2^{(i-1)s})/\nu_{p^i}$. Similarly, both $D_{i,j}$ and $D'_{i,j}$ are linear codes of length l over $\mathbb{F}_{q^{\nu_{p^i}}}$, for $i = 1, 2, \ldots, k$ and $j = 1, 2, \ldots, (2^{is} - 2^{(i-1)s})/2\nu_{p^i}$. The above decomposition of the code C will lead us to the following proposition.

Proposition 3.13. *Let $H \leq G$ be finite abelian groups such that $H \cong (Z_{p^k})^s$, p is odd, $\gcd(|H|, q) = 1$ and $l = [G : H]$ is even. The number of Hermitian self-dual H-quasi-abelian codes in $\mathbb{F}_q[G]$ is*

$$\begin{cases} \left(\prod_{i=0}^{\frac{l}{2}-1} (q^{i+\frac{1}{2}} + 1) \right) \left(\prod_{i=1}^{k} \left(\prod_{r=0}^{\frac{l}{2}-1} \left((q^{\nu_{p^i}})^{r+\frac{1}{2}} + 1 \right) \right)^{\frac{p^{is}-p^{(i-1)s}}{\nu_{p^i}}} \right) & \textit{if } \nu_p \textit{ is odd and } \mu_p \textit{ is even,} \\ \left(\prod_{i=0}^{\frac{l}{2}-1} (q^{i+\frac{1}{2}} + 1) \right) \left(\prod_{i=1}^{k} \left(\sum_{r=0}^{l} \prod_{j=0}^{r-1} \frac{(q^{\nu_{p^i}})^l - (q^{\nu_{p^i}})^j}{(q^{\nu_{p^i}})^r - (q^{\nu_{p^i}})^j} \right)^{\frac{p^{is}-p^{(i-1)s}}{2\nu_{p^i}}} \right) & \textit{if } \nu_p \textit{ is even or } \mu_p \textit{ is odd.} \end{cases}$$

Proof. Apply the same arguments as in the proof of Proposition 3.8 to (9). □

An example is given when $H \cong (\mathbb{Z}_p)^s$ is an elementary p-group.

Example 3.14. *Let $H \leq G$ be finite abelian groups such that $H \cong (\mathbb{Z}_p)^s$, p is odd, $\gcd(|H|, q) = 1$ and the index $l = [G : H]$ is even. Then the number of Hermitian self-dual H-quasi-abelian codes in $\mathbb{F}_q[G]$ is*

$$\begin{cases} \prod_{i=0}^{\frac{l}{2}-1} (q^{i+\frac{1}{2}} + 1) \left((q^{\nu_p})^{i+\frac{1}{2}} + 1 \right)^{\frac{p^s-1}{\nu_p}} & \textit{if } \nu_p \textit{ is odd and } \mu_p \textit{ is even,} \\ \left(\prod_{i=0}^{\frac{l}{2}-1} (q^{i+\frac{1}{2}} + 1) \right) \left(\sum_{r=0}^{l} \prod_{j=0}^{r-1} \frac{(q^{\nu_p})^l - (q^{\nu_p})^j}{(q^{\nu_p})^r - (q^{\nu_p})^j} \right)^{\frac{p^s-1}{2\nu_p}} & \textit{if } \nu_p \textit{ is even or } \mu_p \textit{ is odd.} \end{cases}$$

See Table 3.2 for the number of Hermitian self-dual H-quasi-abelian codes when $p = 3$, $q = 4$, $l = 2$, for $k = 1, 2$ and $s = 1, 2$. In this case, $\nu_p = 1$ and $\mu_p = 2$. Then the q-cyclotomic classes of H are all of type I, and hence, this table also illustrates the 1-generator case given in Corollary 4.5 (ii), type I case.

4. Hermitian self-dual 1-generator quasi-abelian codes

In this section, we study 1-generator H-quasi-abelian codes in $\mathbb{F}_q[G]$, a cyclic $\mathbb{F}_q[H]$-module of $\mathbb{F}_q[G]$, where $H \leq G$ are finite abelian groups such that $\gcd(|H|, q) = 1$. The main idea here is to use [6, Theorem 6.1] and combine it with the characterization of Hermitian self-dual H-quasi-abelian codes obtained in

Table 2. Number of Hermitian self-dual H-quasi-abelian codes in $\mathbb{F}_q[G]$, $H \cong (\mathbb{Z}_{3^k})^s$, $l = [G : H] = 2$ and $q = 4$.

s	k	$\|H\|$	$\|G\|$	$A = (q_0 + 1)$	$B = \prod_{i=1}^{k} (q^{\nu_{p^i}} + 1)^{\|H_{p^i}\|/\nu_{p^i}}$	$A \cdot B$
1	1	3	6	3	9	27
	2	9	18	3	729	2187
2	1	9	18	3	6561	19683
	2	81	162	3	$3^8 \cdot 9^{24}$	$3 \cdot 3^8 \cdot 9^{24}$

Proposition 2.3. We also consider the case where $H \cong (\mathbb{Z}_{p^k})^s$, for $p = 2$ or p is odd, and obtain explicit enumeration.

From [6], we have the following characterization of 1-generator quasi-abelian codes.

Theorem 4.1 ([6, Theorem 6.1])**.** *Let q be a prime power and let $H \leq G$ be finite abelian groups with $l = [G : H]$ and $\gcd(|H|, q) = 1$. Let $e_1, e_2, \ldots, e_t$ be the primitive idempotents of $\mathbb{F}_q[H]$. In the light of (3), let*

$$C \cong \prod_{i=1}^{t} C_i$$

be an H-quasi-abelian code in $\mathbb{F}_q[G]$, where C_i is a linear code of length l over $\mathbb{L}_i \cong \mathbb{F}_q[H]e_i$. Then C is 1-generator if and only if the $\mathbb{L}_i$-dimension of C_i is at most 1, for each $i = 1, 2, \ldots, t$.

Since the $\mathbb{F}_q$-dimension of a 1-generator H-quasi-abelian code C in $\mathbb{F}_q[G]$ cannot exceed $|H|$, $C^{\perp_H}$ could never be a 1-generator if $[G : H] > 2$. In the case where $[G : H] = 2$, we have the following characterization.

Corollary 4.2. *Assume the notation in Theorem 4.1. In addition, we assume that $[G : H] = 2$. If C is a 1-generator H-quasi-abelian code in $\mathbb{F}_q[G]$, then the following statements are equivalent.*

i) $C^{\perp_H}$ is a 1-generator H-quasi-abelian code.

ii) C_i has $\mathbb{L}_i$-dimension 1 for all $i = 1, 2, \ldots, t$.

iii) The $\mathbb{F}_q$-dimension of C is $|H|$.

Proof. The corollary follows immediately from Theorem 4.1 and observations similar to those in [12, Corollary 3.2]. □

Combining Proposition 2.3 and Corollary 4.2, we conclude the following characterization for Hermitian self-dual 1-generator quasi-abelian codes (*cf.* [12, Theorem 3.3]).

Corollary 4.3. *A 1-generator H-quasi-abelian code C in $\mathbb{F}_q[G]$ is Hermitian self-dual if and only if $[G : H] = 2$ (i.e., $G = \mathbb{Z}_2 \times H$) and, in (3), C is decomposed as*

$$C \cong \left(\prod_{i=1}^{r_I} C_i \right) \times \left(\prod_{k=1}^{r_{II}} \left(D_j \times D_j^{\perp_E} \right) \right),$$

where

i) C_i is Hermitian self-dual of length 2 over $\mathbb{E}_i$ for all $i = 1, 2, \ldots, r_I$, and

ii) D_j is a linear code of dimension 1 and length 2 over $\mathbb{K}_j$ for all $j = 1, 2, \ldots, r_{II}$.

The enumeration of Hermitian self-dual 1-generator quasi abelian codes immediately follows.

Corollary 4.4. *Let $H \leq G$ be finite abelian groups such that $\gcd(|H|, q) = 1$, and $[G : H] = 2$. Assume that $\mathbb{F}_q[H]$ is decomposed as in (1) and contains r_I (resp., $2r_{II}$) primitive idempotents of type I (resp., II). Assume further that the primitive idempotents of type I are induced by q-cyclotomic classes of size s_i for each $i = 1, 2, \dots, r_I$ and the primitive idempotents of type II are induced by q-cyclotomic classes of sizes t_j and t'_j, pair-wise, for each $j = 1, 2, \dots, r_{II}$. Then the number of Hermitian self-dual 1-generator H-quasi-abelian codes in $\mathbb{F}_q[G]$ is*

$$\prod_{i=1}^{r_I}(q_0^{s_i}+1)\prod_{j=1}^{r_{II}}(q^{t_j}+1).$$

Proof. The corollary follows from Corollary 4.3, (6), and the fact that the number of 1-dimensional subspaces of $\mathbb{F}_{q^{t_j}}^2$ is $q^{t_j}+1$. □

We end this paper by considering the case of Hermitian self-dual 1-generator H-quasi-abelian codes where H are some p-groups.

Corollary 4.5. *Let $H \leq G$ be finite abelian groups such that $H \cong (Z_{p^k})^s$, $\gcd(|H|, q) = 1$ and $l = [G : H] = 2$ (i.e., $G = \mathbb{Z}_2 \times H$). Then one of the following statements holds.*

i) If $p = 2$, q is odd and $0 \leq r' \leq k$ is the largest integer such that $2^{r'} | (q_0 + 1)$, then the number of Hermitian self-dual 1-generator H-quasi-abelian codes in $\mathbb{F}_q[G]$ is

$$(q_0+1)^{2^{r's}}\left(\prod_{r=r'+1}^{k}(q^{\nu_{2^r}}+1)^{\frac{2^{rs}-2^{(r-1)s}}{2\nu_{2^r}}}\right).$$

ii) If p is odd and $\gcd(p, q) = 1$, then the number of Hermitian self-dual 1-generator H-quasi-abelian codes in $\mathbb{F}_q[G]$ is

$$\begin{cases}\prod_{i=0}^{k}\left(q_0^{\nu_{p^i}}+1\right)^{\frac{p^{is}-p^{(i-1)s}}{\nu_{p^i}}} & \text{if } \nu_p \text{ is odd and } \mu_p \text{ is even,}\\ (q_0+1)\left(\prod_{i=1}^{k}(q^{\nu_{p^i}}+1)^{\frac{p^{is}-p^{(i-1)s}}{2\nu_{p^i}}}\right) & \text{if } \nu_p \text{ is even or } \mu_p \text{ is odd.}\end{cases}$$

Proof. The first statement is derived using (8) and Corollary 4.3 by getting the number of Hermitian self-dual codes C_i over $\mathbb{F}_q$ of length $l = 2$, for $i = 1, 2, \dots, 2^{r's}$, and the number of 1-dimensional linear codes $D_{r,j'}$ of length $l = 2$ over $\mathbb{F}_{q^{\nu_{2^r}}}$ which is equal $q^{\nu_{2^r}}+1$, for $r = r'+1, \dots, k$ and $j' = 1, 2, \dots, (2^{rs} - 2^{(r-1)s})/2\nu_{2^r}$.

Suppose p is odd, $\gcd(p, q) = 1$, ν_p is odd and μ_p is even. This case follows directly from Proposition 3.13 by letting $l = 2$ and noting that $q = q_0^2$. On the other hand, suppose ν_p is even or μ_p is odd. We apply Corollary 4.3 and (9). The first factor is obtained by counting the number of Hermitian self-dual codes C_1 of length 2 over $\mathbb{F}_q$. For the second factor, we count the number of 1-dimensional linear codes $D_{i,j}$ over $\mathbb{F}_{q^{\nu_{p^i}}}$, given by $q^{\nu_{p^i}}+1$, for each $i = 1, 2, \dots, k$, and $j = 1, 2, \dots, (p^{is} - p^{(i-1)s})/2\nu_{p^i}$. □

For the case where H is an elementary p-group, we have the following example.

Example 4.6. *Let $H \leq G$ be abelian groups such that $H \cong (Z_p)^s$, an elementary p-group, $\gcd(|H|, q) = 1$ and $l = [G : H] = 2$ (i.e., $G = \mathbb{Z}_2 \times H$). Then one of the following statements holds.*

i) If $p = 2$ and q is odd, then the number of Hermitian self-dual 1-generator H-quasi-abelian codes in $\mathbb{F}_q[G]$ is

$$(q_0 + 1)^{2^s}.$$

ii) If p is odd and $\gcd(p, q) = 1$, then the number of Hermitian self-dual 1-generator H-quasi-abelian codes in $\mathbb{F}_q[G]$ is

$$\begin{cases} (q_0+1)(q_0^{\nu_p}+1)^{\frac{p^s-1}{\nu_p}} & \text{if } \nu_p \text{ is odd and } \mu_p \text{ is even,} \\ (q_0+1)(q^{\nu_p}+1)^{\frac{p^s-1}{2\nu_p}} & \text{if } \nu_p \text{ is even or } \mu_p \text{ is odd.} \end{cases}$$

5. Summary

Characterization and enumeration of Hermitian self-dual quasi-abelian codes were established based on the well-known decomposition of quasi-abelian codes. Necessary and sufficient conditions for the existence of Hermitian self-dual 1-generator quasi-abelian codes were also given. For special cases where the underlying groups are some p-groups, complete classification of cyclotomic classes has been done. As a result, the actual number of resulting Hermitian self-dual quasi-abelian codes has been determined. It is interesting to note that the results in this work is restricted to $\mathbb{F}_q[H]$ being a semi-simple group algebra, i.e., the characteristic of $\mathbb{F}_q$ and $|H|$ are coprime, where H is a finite abelian group.

Acknowledgment: The authors would like to thank the anonymous referees for their helpful comments. H. S. Palines wishes to thank the University of the Philippines Systems for providing the Alternative Study "Sandwich" Grant while doing this research at the Mathematics Department, Faculty of Science, Silpakorn University, Nakhon Pathom, Thailand. Also, to the Department of Science and Technology-Science Education Institute (DOST-SEI) of the Philippines for his Ph.D. scholarship grant. S. Jitman is supported by the Thailand Research Fund under Research Grant TRG5780065.

References

[1] L. M. J. Bazzi, S. K. Mitter, Some randomized code constructions from group actions, IEEE Trans. Inform. Theory 52(7) (2006) 3210–3219.

[2] J. Conan, G. Séguin, Structural properties and enumeration of quasi–cylic codes, Appl. Algebra Engrg. Comm. Comput. 4(1) (1993) 25–39.

[3] B. K. Dey, On existence of good self–dual quasicyclic codes, IEEE Trans. Inform. Theory 50(8) (2004) 1794–1798.

[4] B. K. Dey, B. S. Rajan, Codes closed under arbitrary abelian group of permutations, SIAM J. Discrete Math. 18(1) (2004) 1–18.

[5] C. Ding, D. R. Kohel, S. Ling, Split group codes, IEEE Trans. Inform. Theory 46(2) (2000) 485–495.

[6] S. Jitman, S. Ling, Quasi–abelian codes, Des. Codes Cryptogr. 74(3) (2015) 511–531.

[7] S. Jitman, S. Ling, P. Solé, Hermitian self–dual abelian codes, IEEE Trans. Inform. Theory 60(3) (2014) 1496–1507.

[8] A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli, Nonbinary stabilizer codes over finite fields, IEEE Trans. Inform. Theory 52(11) (2006) 4892–4914.

[9] K. Lally, P. Fitzpatrick, Algebraic structure of quasicyclic codes, Discrete Appl. Math. 111(1–2) (2001) 157–175.

[10] S. Ling, P. Solé, On the algebraic structure of quasi–cyclic codes I: Finite fields, IEEE Trans. Inform. Theory 47(7) (2001) 2751–2760.

[11] S. Ling, P. Solé, Good self–dual quasi–cyclic codes exist, IEEE Trans. Inform. Theory 49(4) (2003) 1052–1053.
[12] S. Ling, P. Solé, On the algebraic structure of quasi–cyclic codes III: Generator theory, IEEE Trans. Inform. Theory 51(7) (2005) 2692–2700.
[13] G. Nebe, E. M. Rains, N. J. A. Sloane, Self–Dual Codes and Invariant Theory, Algorithms and Computation in Mathematics 17, Springer–Verlag, Berlin, Heidelberg, 2006.
[14] J. Pei, X. Zhang, 1−generator quasi–cyclic codes, J. Syst. Sci. Complex. 20(4) (2007) 554–561.
[15] V. Pless, On the uniqueness of the Golay codes, J. Combinatorial Theory 5(3) (1968) 215–228.
[16] B. S. Rajan, M. U. Siddiqi, Transform domain characterization of abelian codes, IEEE Trans. Inform. Theory 38(6) (1992) 1817–1821.
[17] G. Séguin, A class of 1−generator quasi–cyclic codes, IEEE Trans. Inform. Theory 50(8) (2004) 1745–1753.
[18] S. K. Wasan, Quasi abelian codes, Publ. Inst. Math. 21(35) (1977) 201–206.