Hermitian Self-Dual Abelian Codes

Somphong Jitman, San Ling, and Patrick Solé, *Member, IEEE*

Abstract

Hermitian self-dual abelian codes in a group ring $\mathbb{F}_{q^2}[G]$, where $\mathbb{F}_{q^2}$ is a finite field of order q^2 and G is a finite abelian group, are studied. Using the well-known discrete Fourier transform decomposition for a semi-simple group ring, a characterization of Hermitian self-dual abelian codes in $\mathbb{F}_{q^2}[G]$ is given, together with an alternative proof of necessary and sufficient conditions for the existence of such a code in $\mathbb{F}_{q^2}[G]$, *i.e.*, there exists a Hermitian self-dual abelian code in $\mathbb{F}_{q^2}[G]$ if and only if the order of G is even and $q = 2^l$ for some positive integer l. Later on, the study is further restricted to the case where $\mathbb{F}_{2^{2l}}[G]$ is a principal ideal group ring, or equivalently, $G \cong A \oplus \mathbb{Z}_{2^k}$ with $2 \nmid |A|$. Based on the characterization obtained, the number of Hermitian self-dual abelian codes in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ can be determined easily. When A is cyclic, this result answers an open problem of Jia *et al*. concerning Hermitian self-dual cyclic codes. In many cases, $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ contains a unique Hermitian self-dual abelian code. The criteria for such cases are determined in terms of l and the order of A. Finally, the distribution of finite abelian groups A such that a unique Hermitian self-dual abelian code exists in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_2]$ is established, together with the distribution of odd integers m such that a unique Hermitian self-dual cyclic code of length $2m$ over $\mathbb{F}_{2^{2l}}$ exists.

Index Terms

Abelian codes, cyclic codes, Hermitian inner product, self-dual codes

I. Introduction

Algebraically structured codes such as cyclic codes and abelian codes are an important class of linear codes that has been extensively studied for both theoretical and practical reasons (see [2], [3], [6], [9], [18], [19] and references therein). Self-dual codes are another interesting class of codes due to their rich structures, their fascinating links to other objects such as lattices, and their wide applications [16]. Self-dual codes are also closely related to quantum stabilizer codes [11]. It is therefore of natural interest to investigate families of algebraically structured codes with self-duality.

Some major results on Euclidean self-dual cyclic codes have been discussed in [10]. In [8], the complete characterization and enumeration of such codes have been established. Extensively, these results have been generalized to abelian codes in principal ideal group rings [9].

In this paper, we study Hermitian self-dual abelian codes in a group ring $\mathbb{F}_{q^2}[G]$, where $\mathbb{F}_{q^2}$ is a finite field of q^2 elements and G is a finite abelian group. Modifying the decomposition of $\mathbb{F}_{q^2}[G]$ in [9, Section 2.C], we arrive at the structure of Hermitian duals of abelian codes in $\mathbb{F}_{q^2}[G]$. We give a characterization of Hermitian self-dual abelian codes in $\mathbb{F}_{q^2}[G]$. In [20, Corollary 1.3 and Remark 4.4], for every finite (not necessarily abelian) group G, it has been shown that $\mathbb{F}_{q^2}[G]$ contains a Hermitian self-dual group code if and only if the order of G is even and $q = 2^l$ for some positive integer l. This is similar to the Euclidean case [9, Proposition 2.10] and [20, Corollary 1.3] in the sense that the characteristic of the field is 2 and G has even order. However, Euclidean self-dual abelian codes make sense not only in $\mathbb{F}_{2^{2l}}[G]$ but also in $\mathbb{F}_{2^l}[G]$. Based on our characterization, we give an alternative proof of the above necessary and sufficient conditions for the existence of a Hermitian self-dual abelian code in the case where G is a finite abelian group.

colorblueSubsequently, we restrict the study to the case where $\mathbb{F}_{2^{2l}}[G]$ is a principal ideal group ring, or equivalently, $G \cong A \oplus \mathbb{Z}_{2^k}$ with $2 \nmid |A|$ (see [7]). In this case, the number of Hermitian self-dual abelian codes in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ can be determined easily via our characterization mentioned above. As a special case, our results cover the study of Hermitian self-dual cyclic codes posed as an open problem in [8]. Next, we move on to the case where $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ contains exactly one Hermitian self-dual abelian code and determine the criterion for this case. Finally, we consider the asymptotic behavior of this unique case.

The paper is organized as follows. In Section II, we recall some basic knowledge concerning abelian codes and prove some properties of the Hermitian duality of such codes, including necessary and sufficient conditions for a group ring to contain a Hermitian self-dual abelian code. From Section III, we restrict the study to the case where the group ring is a principal ideal group ring. A characterization and an enumeration of Hermitian self-dual abelian codes are given in Section III. In Section IV, criteria for a group ring to contain a unique Hermitian self-dual abelian code are determined in many cases. The distribution of finite abelian groups whose group rings contain a unique Hermitian self-dual abelian code is established in Section V. Conclusive remarks and suggestions for further work are provided in Section VI.

S. Jitman is with the Department of Mathematics, Faculty of Science, Silpakorn University, Nakhonpathom 73000, Thailand, (email: sjitman@gmail.com).

S. Ling is with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371, Republic of Singapore (email: lingsan@ntu.edu.sg).

P. Solé is with Telecom ParisTech, 46 rue Barrault, 75634 Paris Cedex 13, France, and, Math Dept of King Abdulaziz University, Jeddah, Saudi Arabia (email:patrick.sole@telecom-paristech.fr).

The work of S. Jitman and S. Ling was supported by the National Research Foundation of Singapore under Research Grant NRF-CRP2-2007-03. The work of S. Jitman and P. Solé was partially supported by the Embassy of France in Singapore under the MERLION Project No. 1.02.10.

II. Abelian Codes in Group Rings

In this section, we recall some definitions and basic properties of abelian codes (see [9] and [18]) and prove some results concerning the Hermitian duality of abelian codes.

A. Notations

For a commutative ring R with identity and a finite abelian group G, written additively, let $R[G]$ denote the *group ring* of G over R. The elements in $R[G]$ will be written as $\sum_{g\in G} \alpha_g Y^g$, where $\alpha_g \in R$. The addition and the multiplication in $R[G]$ are given as in the usual polynomial ring over R with indeterminate Y, where the indices are computed additively in G. By convention, $Y^0 = 1$ is the identity of R, where 0 is the identity of G.

An *abelian code* in $R[G]$ is defined to be an ideal in $R[G]$. If G is cyclic, such a code becomes a cyclic code. In this case, an abelian code will be referred as a *cyclic code*. Over a finite field $\mathbb{F}_q$, it is well known that cyclic codes of length n can be regarded as ideals in the quotient polynomial ring $\mathbb{F}_q[X]/\langle X^n - 1\rangle$ and each cyclic code is uniquely generated by a monic divisor of $X^n - 1$.

Let $\mathbb{F}_{q^2}$ denote a finite field of characteristic p and order q^2. For each $\alpha \in \mathbb{F}_{q^2}$, denote by $\overline{\alpha}$ the conjugate of α, *i.e.*, $\overline{\alpha} := \alpha^q$. In the case where we deal with different finite fields at the same time, all the conjugates will be written using $^-$, however, they are defined in their respective appropriate fields.

Let G be a finite abelian group of order n. Without loss of generality, we write $n = mp^k$, where $0 \le k$ and $1 \le m$ are integers with $p \nmid m$. A subgroup of G of order p^k is called a *Sylow p-subgroup*. Since G is abelian, its Sylow p-subgroup is unique. We denote it by B. The group G can be decomposed as $G = A \oplus B$, where A is a subgroup of G of order m.

The Sylow p-subgroup B of G is crucial for the determination of an algebraic structure of $\mathbb{F}_{q^2}[G]$. From Maschke's Theorem (see [17, Chapter 2: Theorem 4.2]), $\mathbb{F}_{q^2}[G]$ is semi-simple if and only if B is trivial. Consequently, $\mathcal{R} := \mathbb{F}_{q^2}[A]$ is semi-simple. The group ring $\mathbb{F}_{q^2}[G]$ is a principal ideal group ring if and only if B is cyclic (see [7]).

B. Abelian Codes in $\mathbb{F}_{q^2}[G]$ viewed as Abelian Codes in $\mathcal{R}[B]$

Let $\mathcal{R} := \mathbb{F}_{q^2}[A]$. Then the map $\Phi : \mathbb{F}_{q^2}[G] \to \mathcal{R}[B]$ given by

$$\Phi\Big(\sum_{a\in A}\sum_{b\in B} \alpha_{a+b} Y^{a+b}\Big) = \sum_{b\in B} \boldsymbol{\alpha}_b(Y) Y^b, \qquad \text{where } \boldsymbol{\alpha}_b(Y) = \sum_{a\in A} \alpha_{a+b} Y^a \in \mathcal{R},$$

is well known to be a ring isomorphism [9, Lemma 2.1], and hence, Φ induces a one-to-one correspondence between abelian codes in $\mathbb{F}_{q^2}[G]$ and abelian codes in $\mathcal{R}[B]$.

The *Euclidean* (resp., *Hermitian*) *inner product* of $\boldsymbol{u} = \sum_{g\in G} \alpha_g Y^g$ and $\boldsymbol{v} = \sum_{g\in G} \beta_g Y^g$ in $\mathbb{F}_{q^2}[G]$ is defined to be

$$\langle \boldsymbol{u}, \boldsymbol{v}\rangle_{\mathrm{E}} := \sum_{g\in G} \alpha_g \beta_g \quad (\text{resp., } \langle \boldsymbol{u}, \boldsymbol{v}\rangle_{\mathrm{H}} := \sum_{g\in G} \alpha_g \overline{\beta_g}).$$

Define an *involution* $\widetilde{\ }$ on $\mathcal{R}$ to be the $\mathbb{F}_{q^2}$-linear map that sends α to $\overline{\alpha}$ for all $\alpha \in \mathbb{F}_{q^2}$ and sends Y^a to Y^{-a} for all $a \in A$. Let $\langle \cdot, \cdot\rangle_\sim : \mathcal{R}[B] \times \mathcal{R}[B] \to \mathcal{R}$ be defined by

$$\langle \boldsymbol{x}, \boldsymbol{y}\rangle_\sim := \sum_{b\in B} \boldsymbol{x}_b(Y)\widetilde{\boldsymbol{y}_b(Y)},$$

where $\boldsymbol{x} = \sum_{b\in B} \boldsymbol{x}_b(Y) Y^b$ and $\boldsymbol{y} = \sum_{b\in B} \boldsymbol{y}_b(Y) Y^b$.

Remark 2.1: We note that the map $\langle \cdot, \cdot\rangle_\sim$ resembles a Hermitian form, in the sense that it is $\mathcal{R}$-linear in the first component and behaves as a Hermitian form under $\widetilde{\ }$.

The *Euclidean dual* (resp., *Hermitian dual*) of $C \subseteq \mathbb{F}_{q^2}[G]$ is defined to be the set

$$C^{\perp_{\mathrm{E}}} := \{\boldsymbol{u} \in \mathbb{F}_{q^2}[G] \mid \langle \boldsymbol{u}, \boldsymbol{v}\rangle_{\mathrm{E}} = 0 \text{ for all } \boldsymbol{v} \in C\}$$

$$(\text{resp., } C^{\perp_{\mathrm{H}}} := \{\boldsymbol{u} \in \mathbb{F}_{q^2}[G] \mid \langle \boldsymbol{u}, \boldsymbol{v}\rangle_{\mathrm{H}} = 0 \text{ for all } \boldsymbol{v} \in C\}).$$

In the same fashion, the *$\sim$-dual* of $D \subseteq \mathcal{R}[B]$ is defined to be

$$D^{\perp_\sim} := \{\boldsymbol{x} \in \mathcal{R}[B] \mid \langle \boldsymbol{x}, \boldsymbol{y}\rangle_\sim = 0 \text{ for all } \boldsymbol{y} \in D\}.$$

We say that $C \subseteq \mathbb{F}_{q^2}[G]$ is *Euclidean self-dual* (resp., *Hermitian self-dual*) if $C = C^{\perp_{\mathrm{E}}}$ (resp., $C = C^{\perp_{\mathrm{H}}}$). Similarly, $D \subseteq \mathcal{R}[B]$ is *$\sim$-self-dual* if $D = D^{\perp_\sim}$.

Connections between the Euclidean inner product, the Hermitian inner product, and the map $\langle \cdot, \cdot\rangle_\sim$ are given as follows.

Lemma 2.2: Let $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_{q^2}[G]$. Then $\langle Y^a \boldsymbol{u}, \boldsymbol{v}\rangle_{\mathrm{H}} = 0$ for all $a \in A$ if and only if $\langle \Phi(\boldsymbol{u}), \Phi(\boldsymbol{v})\rangle_\sim = 0$.

Proof: Assume that $\boldsymbol{u} = \sum_{g\in G} \alpha_g Y^g$ and $\boldsymbol{v} = \sum_{g\in G} \beta_g Y^g$. By comparing the coefficients,

$$\begin{aligned} 0 &= \langle \Phi(\boldsymbol{u}), \Phi(\boldsymbol{v})\rangle_\sim \\ &= \sum_{b\in B} \left(\sum_{a\in A} \alpha_{a+b} Y^a \right) \left(\sum_{a\in A} \overline{\beta_{a+b}} Y^{-a} \right) \end{aligned} \tag{II.1}$$

is equivalent to

$$\sum_{b\in B} \sum_{a\in A} \alpha_{a+h+b} \overline{\beta_{a+b}} = 0 \text{ for all } h \in A, \tag{II.2}$$

where the subscripts are computed in G. The expression in (II.2) is equivalent to $\langle Y^{-h}\boldsymbol{u}, \boldsymbol{v}\rangle_{\mathrm{H}} = 0$ for all $h \in A$. Since h runs over all the elements in A, (II.1) is equivalent to $\langle Y^a \boldsymbol{u}, \boldsymbol{v}\rangle_{\mathrm{H}} = 0$ for all $a \in A$. ∎

Proposition 2.3: Let $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_{q^2}[G]$. Then $\langle Y^g \boldsymbol{u}, \boldsymbol{v}\rangle_{\mathrm{H}} = 0$ for all $g \in G$ if and only if $\langle Y^b \Phi(\boldsymbol{u}), \Phi(\boldsymbol{v})\rangle_\sim = 0$ for all $b \in B$.

Proof: For each $b \in B$, we have

$$0 = \langle Y^b \Phi(\boldsymbol{u}), \Phi(\boldsymbol{v})\rangle_\sim = \langle \Phi(Y^b \boldsymbol{u}), \Phi(\boldsymbol{v})\rangle_\sim.$$

By Lemma 2.2, this is equivalent to $\langle Y^{a+b}\boldsymbol{u}, \boldsymbol{v}\rangle_{\mathrm{H}} = 0$ for all $a \in A$ and $b \in B$, or equivalently, $\langle Y^g \boldsymbol{u}, \boldsymbol{v}\rangle_{\mathrm{H}} = 0$ for all $g \in G$. ∎

The next corollary follows immediately from Proposition 2.3.

Corollary 2.4: Let C be an abelian code in $\mathbb{F}_{q^2}[G]$. Then $\Phi(C)^{\perp_\sim} = \Phi(C^{\perp_{\mathrm{H}}})$. In particular, C is Hermitian self-dual if and only if $\Phi(C)$ is $\sim$-self-dual.

C. Decomposition

For positive integers i, j with $\gcd(i, j) = 1$, 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 $a \in A$, denote by $\mathrm{ord}(a)$ the *additive order* of a in A.

A q^2*-cyclotomic class* of A containing $a \in A$, denoted by $S_{q^2}(a)$, is defined to be the set

$$\begin{aligned} S_{q^2}(a) :=& \{q^{2i} \cdot a \mid i = 0, 1, \dots\} \\ =& \{q^{2i} \cdot a \mid 0 \le i < \mathrm{ord}_{\mathrm{ord}(a)}(q^2)\}, \end{aligned}$$

where $q^{2i} \cdot a := \sum_{j=1}^{q^{2i}} a$ in A.

Remark 2.5: From the definition of a q^2-cyclotomic class, we have the following observations:

i) Let $a \in A$. Since $\gcd(q^2, \mathrm{ord}(a)) = 1$, we have $\mathrm{ord}(a) = \mathrm{ord}(q^{2i} \cdot a)$ for all $i \ge 0$. It follows that every element in $S_{q^2}(a)$ has the same order.

ii) For each $a, b \in A$, if $\mathrm{ord}(a) = \mathrm{ord}(b)$, then $|S_{q^2}(a)| = \mathrm{ord}_{\mathrm{ord}(a)}(q^2) = \mathrm{ord}_{\mathrm{ord}(b)}(q^2) = |S_{q^2}(b)|$. Since any two distinct q^2-cyclotomic classes are disjoint, the set of elements in A of the same order are partitioned into q^2-cyclotomic classes of the same size.

Let $-q \cdot a$ denote the element $q \cdot (-a)$. A q^2-cyclotomic class $S_{q^2}(a)$ is said to be of *type I* if $S_{q^2}(a) = S_{q^2}(-q \cdot a)$ and it is of *type II* if $S_{q^2}(-q \cdot a) \neq S_{q^2}(a)$.

Remark 2.6: We have some observations for q^2-cyclotomic classes of type I.

1) $S_{q^2}(0)$ is a q^2-cyclotomic class of type I.
2) If $S_{q^2}(a)$ is of type I, then $|S_{q^2}(a)|$ is odd. To see this, assume that $|S_{q^2}(a)| = \nu$. Then $-q \cdot a = q^{2i} \cdot a$ for some $0 < i \le \nu$. It follows that $a = -q^{2i-1} \cdot a = q^{2i-2} \cdot (-q \cdot a) = q^{2(2i-1)} \cdot a$ which implies $\nu | (2i - 1)$. Hence, ν is odd.

An *idempotent* in a ring R is a non-zero element e such that $e^2 = e$, and it is called *primitive* if, for every other idempotent f, either $ef = e$ or $ef = 0$. The primitive idempotents in $\mathcal{R}$ are induced by the q^2-cyclotomic classes of A (see [6, Proposition II.4]). Using properties of group characters and [6, Proposition II.4], it is not difficult to verify that e is induced by $S_{q^2}(a)$ if and only if $\widetilde{e}$ is induced by $S_{q^2}(-q \cdot a)$.

Assume that A contains t q^2-cyclotomic classes. Without loss of generality, let $\{a_1 = 0, a_2, \dots, a_t\}$ be a set of representatives of the q^2-cyclotomic classes of A such that $\{a_i \mid i = 1, 2, \dots, r_I\}$ and $\{a_{r_I+j}, a_{r_I+r_{II}+j} = -q \cdot a_{r_I+j} \mid j = 1, 2, \dots, r_{II}\}$ are sets of representatives of q^2-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 $\{S_{q^2}(a_i) \mid i = 1, 2, \dots, t\}$, respectively. Then $e_i = \widetilde{e_i}$ and $e_{r_I+r_{II}+j} = \widetilde{e}_{r_I+j}$ for all $i = 1, 2, \dots, r_I$ and $j = 1, 2, \dots, r_{II}$.

Rearranging the terms in the decomposition of $\mathcal{R}$ in [18] or in [9] based on the two types of q^2-cyclotomic classes, we have

$$\mathcal{R} = \bigoplus_{i=1}^{t} \mathcal{R} e_i \cong \left(\prod_{i=1}^{r_I} \mathbb{E}_i \right) \times \left(\prod_{j=1}^{r_{II}} (\mathbb{K}_j \times \mathbb{K}'_j) \right), \tag{II.3}$$

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 extension fields of $\mathbb{F}_{q^2}$ for all $i = 1, 2, \ldots, r_I$ and $j = 1, 2, \ldots, r_{II}$.

From (II.3), we have

$$\mathbb{F}_{q^2}[G] = \mathcal{R}[B] \cong \left(\prod_{i=1}^{r_I} \mathbb{E}_i[B]\right) \times \left(\prod_{j=1}^{r_{II}} (\mathbb{K}_j[B] \times \mathbb{K}'_j[B])\right). \tag{II.4}$$

Consequently, every abelian code C in $\mathbb{F}_{q^2}[G]$ can be viewed as

$$C \cong \left(\prod_{i=1}^{r_I} C_i\right) \times \left(\prod_{j=1}^{r_{II}} (D_j \times D'_j)\right), \tag{II.5}$$

where C_i, D_j and D'_j are abelian codes in $\mathbb{E}_i[B]$, $\mathbb{K}_j[B]$, and $\mathbb{K}'_j[B]$, respectively, for all $i = 1, 2, \ldots, r_I$ and $j = 1, 2, \ldots, r_{II}$.

The readers may refer to [9, Proposition 2.7] for an explicit form of the isomorphism in (II.5).

D. Duality

Let ψ denote the isomorphism in (II.3). Then an element $\boldsymbol{x} \in \mathcal{R}$ can be written as

$$\psi(\boldsymbol{x}) = (x_1, \ldots, x_{r_I}, y_1, y'_1, \ldots, y_{r_{II}}, y'_{r_{II}}), \tag{II.6}$$

where $x_i \in \mathbb{E}_i$, $y_j \in \mathbb{K}_j$ and $y'_j \in \mathbb{K}'_j$ for all $i = 1, 2, \ldots, r_I$ and $j = 1, 2, \ldots, r_{II}$.

To view $\widetilde{\boldsymbol{x}}$ defined in Section II in terms of (II.6), we begin with the following discussion.

If e is induced by a q^2-cyclotomic class of type I of size ν, then ν is odd by Remark 2.6, and hence, for each element $r = \left(\sum_{a\in A} r_a Y^a\right) e \in \mathcal{R}e$, we have $\widetilde{r} = \left(\sum_{a\in A} r_a^q Y^{-a}\right) \widetilde{e} = \left(\sum_{a\in A} r_a^{q^\nu} Y^{q^\nu \cdot a}\right) e = r^{q^\nu}$. Hence, the map $\widetilde{\ }$ induces the field automorphism $\bar{\ }$ on $\psi(\mathcal{R}e)$ of the form $\alpha \mapsto \alpha^{q^\nu}$ for all $\alpha \in \psi(\mathcal{R}e)$.

If e is induced by a q^2-cyclotomic class of type II, then $\widetilde{\ }$ induces a field isomorphism between $\psi(\mathcal{R}e)$ and $\psi(\mathcal{R}\widetilde{e})$.

Therefore, $\widetilde{\boldsymbol{x}}$ can be viewed in terms of (II.6) as

$$\psi(\widetilde{\boldsymbol{x}}) = (\overline{x_1}, \ldots, \overline{x_{r_I}}, y'_1, y_1, \ldots, y'_{r_{II}}, y_{r_{II}}),$$

where $\bar{\ }$ is induced as above in an appropriate field.

Proposition 2.7: Let $\boldsymbol{x} = \sum_{b\in B} \boldsymbol{x}_b Y^b$ and $\boldsymbol{u} = \sum_{b\in B} \boldsymbol{u}_b Y^b$ be elements in $\mathcal{R}[B]$. Decomposing $\boldsymbol{x}_b, \boldsymbol{u}_b$ using (II.6), we have

$$\psi(\boldsymbol{x}_b) = (x_{b,1}, \ldots, x_{b,r_I}, y_{b,1}, y'_{b,1}, \ldots, y_{b,r_{II}}, y'_{b,r_{II}})$$

and

$$\psi(\boldsymbol{u}_b) = (u_{b,1}, \ldots, u_{b,r_I}, v_{b,1}, v'_{b,1}, \ldots, v_{b,r_{II}}, v'_{b,r_{II}}).$$

Then

$$\begin{aligned}\psi(\langle \boldsymbol{x}, \boldsymbol{u}\rangle_\sim) = \psi(\sum_{b\in B} \boldsymbol{x}_b \widetilde{\boldsymbol{u}_b}) &= \sum_{b\in B} \psi(\boldsymbol{x}_b)\psi(\widetilde{\boldsymbol{u}_b}) \\ &= \Bigg(\sum_{b\in B} x_{b,1}\overline{u_{b,1}}, \ldots, \sum_{b\in B} x_{b,r_I}\overline{u_{b,r_I}}, \sum_{b\in B} y_{b,1}v'_{b,1}, \\ &\qquad \sum_{b\in B} y'_{b,1}v_{b,1}, \ldots, \sum_{b\in B} y_{b,r_{II}}v'_{b,r_{II}}, \sum_{b\in B} y'_{b,r_{II}}v_{b,r_{II}}\Bigg).\end{aligned}$$

In particular, $\langle \boldsymbol{x}, \boldsymbol{u}\rangle_\sim = 0$ if and only if $\psi(\langle \boldsymbol{x}, \boldsymbol{u}\rangle_\sim) = \mathbf{0}$, or equivalently,

$$\sum_{b\in B} x_{b,j}\overline{u_{b,j}} = 0 \text{ for all } j = 1, 2, \ldots, r_I,$$

and

$$\sum_{b\in B} y_{b,j}v'_{b,j} = 0 = \sum_{b\in B} y'_{b,j}v_{b,j} \text{ for all } j = 1, 2, \ldots, r_{II}.$$

For a code C of the form (II.5), the Hermitian dual of C has the form

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

The next corollary follows from the orthogonality given in Proposition 2.7.

Corollary 2.8: An abelian code C in $\mathcal{R}[B]$ is $\sim$-self-dual, or equivalently, an abelian code in $\mathbb{F}_{q^2}[G]$ is Hermitian self-dual, if and only if, in the decomposition (II.5),

i) C_i is Hermitian self-dual for all $i = 1, 2, \ldots, r_I$, and
ii) $D'_j = D_j^{\perp_{\mathrm{E}}}$ for all $j = 1, 2, \ldots, r_{II}$.

From [20, Corollary 1.3 and Remark 4.4], necessary and sufficient conditions for the existence of a Hermitian self-dual group code in $\mathbb{F}_{q^2}[G]$, where G is a finite (not necessarily abelian) group, have been determined. We give an alternative proof of these conditions in the case where G is a finite abelian group, using the characterization given in Corollary 2.8.

Proposition 2.9: Let $\mathbb{F}_{q^2}$ denote a finite field of order q^2 and characteristic p, and let G be a finite abelian group of order mp^k, where $p \nmid m$. Then there exists a Hermitian self-dual abelian code in $\mathbb{F}_{q^2}[G]$ if and only if $p = 2$ and $k \geq 1$.

Proof: Assume that $G = A \oplus B$, where $|A| = m$ and $|B| = p^k$. According to (II.5), we assume that

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

is Hermitian self-dual with $C_1 \subseteq \mathbb{F}_{q^2}[B] = \mathbb{E}_1[B]$. Then, by Corollary 2.8, C_1 is Hermitian self-dual of length $|B| = p^k$, which implies that p^k must be even. Hence, $p = 2$ and $k \geq 1$.

Conversely, assume that $p = 2$ and $k \geq 1$. Then $|B| = p^k$ and B contains an element x of order 2. We claim that

$$C \cong \left(\prod_{i=1}^{r_I} \mathbb{E}_i[B](Y^x + 1) \right) \times \left(\prod_{j=1}^{r_{II}} \left(\mathbb{K}_j[B] \times \{0\} \right) \right). \tag{II.7}$$

is Hermitian self-dual in $\mathbb{F}_{q^2}[G]$. By Corollary 2.8, it suffices to show that $\mathbb{E}_i[B](Y^x + 1)$ is Hermitian self-dual for all $i = 1, 2, \ldots, r_I$. For each $i \in \{1, 2, \ldots, r_I\}$, let $\boldsymbol{u} = (Y^x + 1) \sum_{b \in B} u_b Y^b$ and $\boldsymbol{v} = (Y^x + 1) \sum_{b \in B} v_b Y^b$ be elements in $\mathbb{E}_i[B](Y^x + 1)$, where $u_b, v_b \in \mathbb{E}_i$ for all $b \in B$. Since x has order 2, we have $x = -x$, and hence,

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle_{\mathrm{H}} = \sum_{b \in B} (u_{b-x} + u_b)\overline{(v_{b-x} + v_b)} = \sum_{b \in B} u_{b-x}\overline{v_{b-x}} + \sum_{b \in B} u_{b-x}\overline{v_b} + \sum_{b \in B} u_b \overline{v_{b+x}} + \sum_{b \in B} u_b \overline{v_b} = 0$$

since $\sum_{b \in B} u_{b-x}\overline{v_{b-x}} = \sum_{b \in B} u_b \overline{v_b}$, $\sum_{b \in B} u_{b-x}\overline{v_b} = \sum_{b \in B} u_b \overline{v_{b+x}}$ and $\mathbb{E}_i$ has characteristic 2. Since $x = -x$, it is not difficult to verify that $\{Y^b(Y^x + 1) \mid b \in B\}$ has size $\frac{|B|}{2}$ and it is an $\mathbb{E}_i$-basis of $\mathbb{E}_i[B](Y^x + 1)$. Therefore, $\mathbb{E}_i[B](Y^x + 1)$ is Hermitian self-dual. ∎

We note that the conditions for the existence of a Hermitian self-dual cyclic code are the same as those in the abelian case since a cyclic codes is abelian and the code C constructed in (II.7) is still Hermitian self-dual when G is a cyclic group.

By Proposition 2.9, it is impossible to have any Hermitian self-dual abelian code in a semi-simple group algebra $\mathbb{F}_{q^2}[G]$ because either the cardinality of G or the characteristic of $\mathbb{F}_{q^2}$ is odd since they are co-prime.

To study Hermitian self-dual abelian codes, by Proposition 2.9, it suffices to consider only abelian codes in the group ring $\mathbb{F}_{2^{2l}}[A \oplus B]$, where A is a finite abelian group of odd order and B is a non-trivial finite 2-group.

III. Hermitian Self-Dual Abelian Codes in Principal Ideal Group Rings

From now on, we restrict the study to the case where $\mathbb{F}_{2^{2l}}[A \oplus B]$ is a principal ideal group ring. In this section, we give the characterization and enumeration of Hermitian self-dual abelian codes in such group rings. In [7], $\mathbb{F}_{2^{2l}}[A \oplus B]$ is shown to be a principal ideal group ring if and only if the Sylow 2-subgroup B of G is cyclic. Hence, to address our goal, it suffices to study Hermitian self-dual abelian codes in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$, where A is an abelian group of odd order and $l, k \geq 1$.

The decomposition in (II.4) can be specifically viewed as

$$\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}] \cong \left(\prod_{i=1}^{r_I} \mathbb{E}_i[\mathbb{Z}_{2^k}] \right) \times \left(\prod_{j=1}^{r_{II}} \left(\mathbb{K}_j[\mathbb{Z}_{2^k}] \times \mathbb{K}'_j[\mathbb{Z}_{2^k}] \right) \right). \tag{III.1}$$

For simplicity, we set $\mathbb{Z}_{2^k} = \{0, 1, \ldots, 2^k - 1\}$. For each $i = 1, 2, \ldots, r_I$, it is well known that $\mathbb{E}_i[\mathbb{Z}_{2^k}]$ and $\mathbb{E}_i[X]/\langle X^{2^k} - 1 \rangle$ are isomorphic as rings via the isomorphism $Y^a \mapsto X^a + \langle X^{2^k} - 1 \rangle$ for all $a \in \mathbb{Z}_{2^k}$, and the ideals in $\mathbb{E}_i[X]/\langle X^{2^k} - 1 \rangle$ are generated by $(X - 1)^i$ for some $0 \leq i \leq 2^k$. Using the convention $1 = Y^0$ and $Y = Y^1$ in $\mathbb{E}_i[\mathbb{Z}_{2^k}]$, every ideal in $\mathbb{E}_i[\mathbb{Z}_{2^k}]$ can be viewed in the form of $\mathbb{E}_i[\mathbb{Z}_{2^k}](Y - 1)^b$, where $b \in \mathbb{Z}_{2^k}$, or $\mathbb{E}_i[\mathbb{Z}_{2^k}](Y - 1)^{2^k} := \{0\}$. We have similar results for $\mathbb{K}_j[\mathbb{Z}_{2^k}]$'s and $\mathbb{K}'_j[\mathbb{Z}_{2^k}]$'s. Then every abelian code C in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ is cyclic in $\mathcal{R}[B]$, where $\mathcal{R} = \mathbb{F}_{2^{2l}}[A]$, and C can be viewed as

$$C \cong \left(\prod_{i=1}^{r_I} C_i \right) \times \left(\prod_{j=1}^{r_{II}} \left(D_j \times D'_j \right) \right), \tag{III.2}$$

where C_i, D_j, and D'_j are cyclic codes in $\mathbb{E}_i[\mathbb{Z}_{2^k}]$, $\mathbb{K}_j[\mathbb{Z}_{2^k}]$, and $\mathbb{K}'_j[\mathbb{Z}_{2^k}]$, respectively, for all $i = 1, 2, \ldots, r_I$ and $j = 1, 2, \ldots, r_{II}$.

Based on the discussion above, a characterization of Hermitian self-dual abelian codes is given as follows.

Proposition 3.1: An abelian code C in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ is Hermitian self-dual if and only if, in the decomposition (III.2),

i) C_i is a Euclidean self-dual cyclic code for all $i = 1, 2, \ldots, r_I$, and

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

Proof: By (III.2) and Corollary 2.8, it suffices to show that, for each $i = 1, 2, \ldots, r_I$, C_i is Euclidean self-dual if and only if it is Hermitian self-dual.

From (III.2), we recall that C_i is a cyclic code in $\mathbb{E}_i[\mathbb{Z}_{2^k}]$, where $\mathbb{E}_i$ is an extension field of $\mathbb{F}_{2^{2l}}$ with odd degree. If C_i is either Euclidean or Hermitian self-dual, then $C_i = \mathbb{E}_i[\mathbb{Z}_{2^k}](Y-1)^{2^{k-1}}$ is the only ideal in $\mathbb{E}_i[\mathbb{Z}_{2^k}]$ of dimension 2^{k-1}. By the uniqueness, we have $C_i = C_i^{\perp_{\mathrm{E}}} = C_i^{\perp_{\mathrm{H}}}$. Therefore, the statement is proved. ∎

A. Enumeration of Hermitian self-dual abelian codes

Let $\mathcal{HSD}_{2^{2l}}(A \oplus \mathbb{Z}_{2^k})$ denote the number of Hermitian self-dual abelian codes in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$. Denote by $r_{II}(A, 2^{2l})$ the number of 2^{2l}-cyclotomic classes of A of type II, *i.e.*, $r_{II}(A, 2^{2l}) = 2r_{II}$, where r_{II} is obtained from the decomposition (II.3). The enumeration of Hermitian self-dual abelian codes is given as follows.

Proposition 3.2: Let l and k be positive integers and let A be an abelian group of odd order. Then

$$\mathcal{HSD}_{2^{2l}}(A \oplus \mathbb{Z}_{2^k}) = (2^k+1)^{\frac{1}{2}r_{II}(A,2^{2l})}.$$

Proof: As mentioned in the proof of Proposition 3.1, there exists a unique Euclidean self-dual cyclic code in $\mathbb{L}[\mathbb{Z}_{2^k}]$ for any extension field $\mathbb{L}$ of $\mathbb{F}_{2^{2l}}$. Hence, by (III.2) and Proposition 3.1, $\mathcal{HSD}_{2^{2l}}(A \oplus \mathbb{Z}_{2^k})$ equals the number of choices of cyclic codes D_j in (III.2), which is $(2^k+1)^{\frac{1}{2}r_{II}(A,2^{2l})}$. ∎

We note that, for fixed positive integers l and k, $\mathcal{HSD}_{2^{2l}}(A \oplus \mathbb{Z}_{2^k})$ depends only on the number of 2^{2l}-cyclotomic classes of A of type II. Hence, it suffices to account for the number $r_{II}(A, 2^{2l})$.

In order to determine $r_{II}(A, 2^{2l})$, we need the following results.

For $i \geq 0$ and $j \geq 1$, we say that 2^i exactly divides j, denoted by $2^i || j$, if 2^i divides j but 2^{i+1} does not divide j.

Let j be an odd positive integer and let l be positive integer. The pair (j, l) is said to be *oddly good* if j divides $(2^l)^s + 1$ for some odd integer $s \geq 1$, and *evenly good* if j divides $(2^l)^s + 1$ for some even integer $s \geq 2$. It is said to be *good* if it is oddly good or evenly good, and *bad* otherwise.

We note that $(1, l)$ is always good. We recall the following result for the goodness of (j, l), where $j > 1$.

Lemma 3.3 ([14, Theorem 1]): Let $j > 1$ be an odd integer and let l be a positive integer. Then (j, l) is good if and only if there exists $s \geq 1$ such that $2^s || \mathrm{ord}_p(2^l)$ for every prime p dividing j.

Since $1 \mid \left(2^l + 1\right)$ and $1 \mid \left(\left(2^l\right)^2 + 1\right)$, we have that $(1, l)$ is both oddly good and evenly good. However, for an odd integer $j > 1$, we have that (j, l) can be either oddly good or evenly good, but not both.

Lemma 3.4: Let $j > 1$ be an odd integer and let l be positive integer. If the pair (j, l) is good, then it is either oddly good or evenly good, but not both.

Proof: Assume that s and t are positive integers such that $s \geq t$, $j \mid ((2^l)^s + 1)$, and $j \mid ((2^l)^t + 1)$. To prove the lemma, it is sufficient to show that s and t have the same parity. Let p be a prime divisor of j. Then $p \mid ((2^l)^s - (2^l)^t)$. It follows that $p \mid (2^l)^t((2^l)^{s-t} - 1)$ which implies $\mathrm{ord}_p(2^l) \mid (s - t)$. Since (j, l) is good, by Lemma 3.3, $\mathrm{ord}_p(2^l)$ is even which implies $s - t$ is even. Hence, s and t have the same parity. ∎

Let χ and λ be functions defined on the pair (j, l), where j is odd, as follows:

$$\chi(j,l) = \begin{cases} 0 & \text{if } (j,l) \text{ is good,} \\ 1 & \text{otherwise,} \end{cases} \tag{III.3}$$

and

$$\lambda(j,l) = \begin{cases} 0 & \text{if } (j,l) \text{ is oddly good,} \\ 1 & \text{otherwise.} \end{cases} \tag{III.4}$$

The function χ is key to studying the number of Euclidean self-dual abelian and cyclic codes (see [8] and [9]). In this paper, we use λ for determining the number of Hermitian self-dual abelian and cyclic codes.

Next, we determine the type of a 2^{2l}-cyclotomic class in A via the order of elements in A.

Lemma 3.5: Let A be a finite abelian group of odd order and let $a \in A \setminus \{0\}$. Then $S_{2^{2l}}(a)$ is of type II if and only if $(\mathrm{ord}(a), l)$ is evenly good or bad.

Proof: Since $a \neq 0$, the order $\mathrm{ord}(a) > 1$ and it is odd. Then, by Lemma 3.4, proving Lemma 3.5 is equivalent to showing that $S_{2^{2l}}(a)$ is of type I if and only if $(\mathrm{ord}(a), l)$ is oddly good.

We observe that $S_{2^{2l}}(a)$ is of type I if and only if $2^l \cdot (-a) \in S_{2^{2l}}(a)$, which is equivalent to $(2^{2l})^s \equiv -2^l \pmod{\mathrm{ord}(a)}$ for some integer $s \geq 0$. This holds true if and only if

$$\begin{aligned} &\mathrm{ord}(a) \mid (2^l+1) && \text{if } s = 0, \text{ or} \\ &\mathrm{ord}(a) \mid 2^l((2^l)^{2s-1}+1) && \text{if } s \geq 1, \end{aligned}$$

or equivalently, $\mathrm{ord}(a) \mid ((2^l)^s+1)$ for some odd positive integer s. Therefore, $S_{2^{2l}}(a)$ is of type I if and only if $(\mathrm{ord}(a), l)$ is oddly good. ∎

Using the discussion above, we conclude the following main result.

Theorem 3.6: Let A be a finite abelian group of odd order with exponent M. Then

$$r_{II}(A, 2^{2l}) = \sum_{d \mid M} \lambda(d,l) \frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(2^{2l})}, \tag{III.5}$$

and hence,

$$\mathcal{HSD}_{2^{2l}}(A \oplus \mathbb{Z}_{2^k}) = (2^k+1)^{\frac{1}{2}\sum_{d \mid M} \lambda(d,l) \frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(2^{2l})}}, \tag{III.6}$$

where $\mathcal{N}_A(d)$ denotes the number of elements in A of order d (see [1]).

In particular, (M, l) is oddly good if and only if $r_{II}(A, 2^{2l}) = 0$. In this case, there is exactly one Hermitian self-dual abelian code in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$.

Proof: From Remark 2.5, the elements in A of the same order are partitioned into 2^{2l}-cyclotomic classes of the same size. Therefore, (III.5) follows from Lemma 3.5. Then (III.6) can be concluded from (III.5) and Proposition 3.2.

Next, we assume that (M, l) is oddly good. Then M divides $(2^l)^s + 1$ for some odd integer $s \geq 1$. It follows that d divides $(2^l)^s + 1$ for all divisors d of M. Hence, (d, l) is oddly good and $\lambda(d, l) = 0$ for all $d \mid M$. By (III.5), we have $r_{II}(A, 2^l) = 0$.

Conversely, assume that $r_{II}(A, 2^{2l}) = 0$. Then $\lambda(d, l) = 0$ for all divisors d of M, which implies that $\lambda(M, l) = 0$ and (M, l) is oddly good. ∎

Note that, if A is a cyclic group, the exponent M of A is just the cardinality of A and $\mathcal{N}_A(d)$ is just $\phi(d)$, where ϕ is the Euler phi function. Then the following corollary follows.

Corollary 3.7: Let $n = m2^k$ be positive integer such that $m \geq 1$ is odd and $k \geq 1$. Then the number of Hermitian self-dual cyclic codes of length n over $\mathbb{F}_{2^{2l}}$ is

$$(2^k+1)^{\frac{1}{2}\sum_{d \mid m} \lambda(d,l) \frac{\phi(d)}{\mathrm{ord}_d(2^{2l})}}. \tag{III.7}$$

In particular, (m, l) is oddly good if and only if the exponent of $2^k + 1$ in (III.7) is 0. In this case, there exists exactly one Hermitian self-dual cyclic code of length n over $\mathbb{F}_{2^{2l}}$.

Some remarks on Hermitian self-dual cyclic codes will be discussed in the next subsection.

Tables III.1 present the numbers of Hermitian self-dual abelian codes in $\mathbb{F}_4[G]$ for all abelian groups $G = A \oplus \mathbb{Z}_{2^k}$ of order less than or equal to 200.

B. Some Remarks on Hermitian Self-Dual Cyclic Codes

In this subsection, we establish some remarks on the structure of Hermitian self-dual cyclic codes using polynomials. To investigate the structure of Hermitian self-dual cyclic codes, it suffices to consider only cyclic codes of length $m2^k$ over $\mathbb{F}_{2^{2l}}$, where $k, m \geq 1$ and m is odd,

It is well known that every cyclic code of length $m2^k$ over $\mathbb{F}_{2^{2l}}$ can be viewed as an ideal in the principal ideal ring $\mathbb{F}_{2^{2l}}[X]/\langle X^{m2^k} - 1\rangle$. In particular, for a non-zero cyclic code C, it is generated by a monic divisor $g(X)$ of $X^{m2^k} - 1$. Moreover, $g(X)$ is unique and called the *generator polynomial* of C. The polynomial

$$h(X) := \frac{X^{m2^k} - 1}{g(X)}$$

is called the *parity-check polynomial* of C.

For a polynomial $f(X) = f_0 + f_1 X + \cdots + f_a X^a$ in $\mathbb{F}_{2^{2l}}[X]$ with $f_0 \neq 0$, let $f^*(X) = X^a f_0^{-1} f\left(\frac{1}{X}\right)$ be the *reciprocal polynomial* of $f(X)$ and let $\overline{f(X)} = \overline{f_0} + \overline{f_1} X + \cdots + \overline{f_a} X^a$ be the *conjugate polynomial* of $f(X)$, where $\bar{}$ denotes the conjugation $a \mapsto a^{2^l}$ for all $a \in \mathbb{F}_{2^{2l}}$. The *conjugate-reciprocal polynomial* of $f(X)$, denoted by $f^\dagger(X)$, is defined by $f^\dagger(X) = \overline{f^*(X)}$. The polynomial $f(X)$ is said to be *self-conjugate-reciprocal* if $f(X) = f^\dagger(X)$. Otherwise, $f(X)$ and $f^\dagger(X)$ are called a *conjugate-reciprocal polynomial pair*.

It is not difficult to verify that $h^\dagger(X)$ is a monic divisor of $X^{m2^k} - 1$ and it is the generator polynomial of $C^{\perp_{\mathrm{H}}}$. Hence, the next proposition follows from the discussion above.

Proposition 3.8: Let C be a cyclic code of length $m2^k$ over $\mathbb{F}_{2^{2l}}$ with generator polynomial $g(X)$ and parity check polynomial $h(X)$. Then C is Hermitian self-dual if and only if $g(X) = h^\dagger(X)$.

TABLE III.1
NUMBER OF HERMITIAN SELF-DUAL ABELIAN CODES IN $\mathbb{F}_4[G]$

Order of G	G	$\mathcal{HSD}_4(G)$
2	$\mathbb{Z}_2$	1
4	$\mathbb{Z}_{2^2}$	1
6	$\mathbb{Z}_3 \oplus \mathbb{Z}_2$	1
8	$\mathbb{Z}_{2^3}$	1
10	$\mathbb{Z}_5 \oplus \mathbb{Z}_2$	3
12	$\mathbb{Z}_3 \oplus \mathbb{Z}_{2^2}$	1
14	$\mathbb{Z}_7 \oplus \mathbb{Z}_2$	3
16	$\mathbb{Z}_{2^4}$	1
18	$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	1
	$\mathbb{Z}_{3^2} \oplus \mathbb{Z}_2$	1
20	$\mathbb{Z}_5 \oplus \mathbb{Z}_{2^2}$	5
22	$\mathbb{Z}_{11} \oplus \mathbb{Z}_2$	1
24	$\mathbb{Z}_3 \oplus \mathbb{Z}_{2^3}$	1
26	$\mathbb{Z}_{13} \oplus \mathbb{Z}_2$	3
28	$\mathbb{Z}_7 \oplus \mathbb{Z}_{2^2}$	5
30	$\mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	27
32	$\mathbb{Z}_{2^5}$	1
34	$\mathbb{Z}_{17} \oplus \mathbb{Z}_2$	9
36	$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{2^2}$	1
	$\mathbb{Z}_{3^2} \oplus \mathbb{Z}_{2^2}$	1
38	$\mathbb{Z}_{19} \oplus \mathbb{Z}_2$	1
40	$\mathbb{Z}_5 \oplus \mathbb{Z}_{2^3}$	9
42	$\mathbb{Z}_7 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	3
44	$\mathbb{Z}_{11} \oplus \mathbb{Z}_{2^2}$	1
46	$\mathbb{Z}_{23} \oplus \mathbb{Z}_2$	3
48	$\mathbb{Z}_3 \oplus \mathbb{Z}_{2^4}$	1
50	$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2$	729
	$\mathbb{Z}_{5^2} \oplus \mathbb{Z}_2$	9
52	$\mathbb{Z}_{13} \oplus \mathbb{Z}_{2^2}$	5
54	$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	1
	$\mathbb{Z}_{3^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	1
	$\mathbb{Z}_{3^3} \oplus \mathbb{Z}_2$	1
56	$\mathbb{Z}_7 \oplus \mathbb{Z}_{2^3}$	9
58	$\mathbb{Z}_{29} \oplus \mathbb{Z}_2$	3
60	$\mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{2^2}$	125
62	$\mathbb{Z}_{31} \oplus \mathbb{Z}_2$	27
64	$\mathbb{Z}_{2^6}$	1
66	$\mathbb{Z}_{11} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	1
68	$\mathbb{Z}_{17} \oplus \mathbb{Z}_{2^2}$	25
70	$\mathbb{Z}_7 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2$	81
72	$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{2^3}$	1
	$\mathbb{Z}_{3^2} \oplus \mathbb{Z}_{2^2}$	1
74	$\mathbb{Z}_{37} \oplus \mathbb{Z}_2$	3
76	$\mathbb{Z}_{19} \oplus \mathbb{Z}_{2^2}$	1
78	$\mathbb{Z}_{13} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	27
80	$\mathbb{Z}_5 \oplus \mathbb{Z}_{2^4}$	17
82	$\mathbb{Z}_{41} \oplus \mathbb{Z}_2$	9
84	$\mathbb{Z}_7 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{2^2}$	5
86	$\mathbb{Z}_{43} \oplus \mathbb{Z}_2$	1
88	$\mathbb{Z}_{11} \oplus \mathbb{Z}_{2^3}$	1
90	$\mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	19683
	$\mathbb{Z}_5 \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_2$	243
92	$\mathbb{Z}_{23} \oplus \mathbb{Z}_{2^2}$	5
94	$\mathbb{Z}_{47} \oplus \mathbb{Z}_2$	3
96	$\mathbb{Z}_3 \oplus \mathbb{Z}_{2^5}$	1
98	$\mathbb{Z}_7 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_2$	6561
	$\mathbb{Z}_{7^2} \oplus \mathbb{Z}_2$	9
100	$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{2^2}$	15625
	$\mathbb{Z}_{5^2} \oplus \mathbb{Z}_{2^2}$	25
102	$\mathbb{Z}_{17} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	729
104	$\mathbb{Z}_{13} \oplus \mathbb{Z}_{2^3}$	9
106	$\mathbb{Z}_{53} \oplus \mathbb{Z}_2$	3
108	$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{2^2}$	1
	$\mathbb{Z}_3 \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_{2^2}$	1
	$\mathbb{Z}_{3^3} \oplus \mathbb{Z}_{2^2}$	1
110	$\mathbb{Z}_{11} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2$	27
112	$\mathbb{Z}_7 \oplus \mathbb{Z}_{2^4}$	17
114	$\mathbb{Z}_{19} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	1
116	$\mathbb{Z}_{29} \oplus \mathbb{Z}_{2^2}$	5
118	$\mathbb{Z}_{59} \oplus \mathbb{Z}_2$	1
120	$\mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{2^3}$	729
122	$\mathbb{Z}_{61} \oplus \mathbb{Z}_2$	3
124	$\mathbb{Z}_{31} \oplus \mathbb{Z}_{2^2}$	125
126	$\mathbb{Z}_7 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	3
	$\mathbb{Z}_7 \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_2$	3
128	$\mathbb{Z}_{2^7}$	1
130	$\mathbb{Z}_{13} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2$	729
132	$\mathbb{Z}_{11} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{2^2}$	1
134	$\mathbb{Z}_{67} \oplus \mathbb{Z}_2$	1
136	$\mathbb{Z}_{17} \oplus \mathbb{Z}_{2^3}$	81
138	$\mathbb{Z}_{23} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	3
140	$\mathbb{Z}_7 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{2^2}$	625
142	$\mathbb{Z}_{71} \oplus \mathbb{Z}_2$	3
144	$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{2^4}$	1
	$\mathbb{Z}_{3^2} \oplus \mathbb{Z}_{2^4}$	1
146	$\mathbb{Z}_{73} \oplus \mathbb{Z}_2$	81
148	$\mathbb{Z}_{37} \oplus \mathbb{Z}_{2^2}$	5
150	$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	387420489
	$\mathbb{Z}_{5^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	729
152	$\mathbb{Z}_{19} \oplus \mathbb{Z}_{2^3}$	1
154	$\mathbb{Z}_{11} \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_2$	3
156	$\mathbb{Z}_{13} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{2^2}$	125
158	$\mathbb{Z}_{79} \oplus \mathbb{Z}_2$	3
160	$\mathbb{Z}_5 \oplus \mathbb{Z}_{2^5}$	33
162	$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	1
	$\mathbb{Z}_{3^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	1
	$\mathbb{Z}_{3^3} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	1
	$\mathbb{Z}_{3^2} \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_2$	1
	$\mathbb{Z}_{3^4} \oplus \mathbb{Z}_2$	1
164	$\mathbb{Z}_{41} \oplus \mathbb{Z}_{2^2}$	25
166	$\mathbb{Z}_{83} \oplus \mathbb{Z}_2$	1
168	$\mathbb{Z}_7 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{2^3}$	9
170	$\mathbb{Z}_{17} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2$	177147
172	$\mathbb{Z}_{43} \oplus \mathbb{Z}_{2^2}$	1
174	$\mathbb{Z}_{29} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	27
176	$\mathbb{Z}_{11} \oplus \mathbb{Z}_{2^4}$	1
178	$\mathbb{Z}_{89} \oplus \mathbb{Z}_2$	81
180	$\mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{2^2}$	1953125
	$\mathbb{Z}_5 \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_{2^2}$	3125
182	$\mathbb{Z}_{13} \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_2$	6561
184	$\mathbb{Z}_{23} \oplus \mathbb{Z}_{2^3}$	9
186	$\mathbb{Z}_{31} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	27
188	$\mathbb{Z}_{47} \oplus \mathbb{Z}_{2^2}$	5
190	$\mathbb{Z}_{19} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2$	27
192	$\mathbb{Z}_3 \oplus \mathbb{Z}_{2^6}$	1
194	$\mathbb{Z}_{97} \oplus \mathbb{Z}_2$	9
196	$\mathbb{Z}_7 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_{2^2}$	309625
	$\mathbb{Z}_{7^2} \oplus \mathbb{Z}_{2^2}$	25
198	$\mathbb{Z}_{11} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	1
	$\mathbb{Z}_{11} \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_2$	1
200	$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{2^3}$	531441
	$\mathbb{Z}_{5^2} \oplus \mathbb{Z}_{2^3}$	81

Note that a cyclic code of length $m2^k$ over $\mathbb{F}_{2^{2l}}$ generated by $g(X) = (X^m - 1)^{2^{k-1}}$ is always Hermitian self-dual (and Euclidean self-dual) since $g(X) = h(X) = h^*(X) = h^\dagger(X)$.

Without loss of generality, we assume that $X^m - 1$ is factorized into a product of distinct monic irreducible polynomials

$$X^m - 1 = f_1(X) \dots f_s(X) \ell_1(X) \ell_1^\dagger(X) \dots \ell_t(X) \ell_t^\dagger(X), \tag{III.8}$$

where $f_i(X)$ is a self-conjugate-reciprocal polynomial for all $1 \leq i \leq s$, and $\ell_j(X)$ and $\ell_j^\dagger(X)$ are a conjugate-reciprocal polynomial pair for all $1 \leq j \leq t$.

The generators of all Hermitian self-dual cyclic codes of length $m2^k$ over $\mathbb{F}_{2^{2l}}$ can be obtained in the next theorem.

Theorem 3.9: Let l, k be positive integers and let m be an odd integer. Assume that $X^m - 1$ is factorized as in (III.8). Then a cyclic code C of length $m2^k$ over $\mathbb{F}_{2^{2l}}$ is Hermitian self-dual if and only if its generator polynomial is of the form

$$f_1(X)^{2^{k-1}} \dots f_s(X)^{2^{k-1}} \ell_1(X)^{j_1} \ell_1^\dagger(X)^{2^k - j_1} \dots \ell_t(X)^{j_t} \ell_t^\dagger(X)^{2^k - j_t},$$

where $0 \leq j_i \leq 2^k$ for all $1 \leq i \leq t$.

Proof: The theorem can be obtained using statements similar to those in [8, Theorem 2] while Proposition 3.8 is applied instead of [8, Proposition 1]. ■

IV. Abelian Groups with a Unique Hermitian Self-Dual Abelian Code

In this section, we discuss the case where $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ contains a unique Hermitian self-dual abelian code. We begin with some number-theoretic tools, followed by criteria for this situation to occur, and end with some relationship between the Euclidean and Hermitian cases.

A. Number-Theoretic Results

We first prove some number-theoretic properties of oddly and evenly good pairs.

Theorem 4.1: Let $j > 1$ be an odd integer and let l be a positive integer. Then the following statements hold.

i) The pair (j, l) is oddly good if and only if $2||\mathrm{ord}_p(2^l)$ for every prime p dividing j.

ii) The pair (j, l) is evenly good if and only if there exists $s \geq 2$ such that $2^s||\mathrm{ord}_p(2^l)$ for every prime p dividing j.

Proof: Let $p_1, p_2, \dots, p_t$ be the distinct prime divisors of j. For each $1 \leq i \leq t$, let r_i be the positive integer such that $p_i^{r_i}||j$. To prove the necessity in $i)$, assume that (j, l) is oddly good. There exists an odd positive integer c such that $(2^l)^c \equiv -1 \pmod{j}$ and, hence, $(2^l)^c \equiv -1 \pmod{p_i^{r_i}}$ for all $i = 1, 2, \dots, t$. By [14, Proposition 2], we have that $\mathrm{ord}_{p_i^{r_i}}(2^l)$ is even and

$$c \equiv \frac{\mathrm{ord}_{p_i^{r_i}}(2^l)}{2} \pmod{\mathrm{ord}_{p_i^{r_i}}(2^l)}$$

for all $i = 1, 2, \dots, t$. Since c is an odd integer, $\frac{\mathrm{ord}_{p_i^{r_i}}(2^l)}{2}$ is odd for all $i = 1, 2, \dots, t$. Therefore, by [14, Proposition 4], $2||\mathrm{ord}_p(2^l)$ for every prime p dividing j.

Conversely, assume that $2||\mathrm{ord}_p(2^l)$ for every prime p dividing j. Then, by [14, Proposition 4] and the assumption, we have $2||\mathrm{ord}_{p_i^{r_i}}(2^l)$ for all $i = 1, 2, \dots, t$. By [14, Lemma 1], there exists an integer c such that

$$c \equiv \frac{\mathrm{ord}_{p_i^{r_i}}(2^l)}{2} \pmod{\mathrm{ord}_{p_i^{r_i}}(2^l)}$$

for all $i = 1, 2, \dots, t$. Since $\frac{\mathrm{ord}_{p_i^{r_i}}(2^l)}{2}$ is odd, c is an odd integer. Thus $(2^l)^c \equiv -1 \pmod{p_i^{r_i}}$ for all $i = 1, 2, \dots, t$, and hence, $(2^l)^c \equiv -1 \pmod{j}$. Therefore, (j, l) is oddly good as desired.

The statement $ii)$ follows immediately from $i)$ and Lemmas 3.3 and 3.4. ■

Corollary 4.2: Let j be an odd positive integer and let l be a positive integer. Then the following statements hold.

i) The following statements are equivalent.
- *a)* (j, l) is oddly good.
- *b)* (d, l) is oddly good for all divisors d of j.
- *c)* (p, l) is oddly good for all prime divisors p of j.

ii) If (j, l) is (evenly) good, then (d, l) is (evenly) good for all divisors d of j.

Proof: Part $i)$ follows immediately from Theorem 4.1 $i)$.

For $ii)$, the case of good pair follows from Lemma 3.3 and the case of evenly good pair follows form part $ii)$ of Theorem 4.1. ■

B. The Existence of Abelian Groups with a Unique Hermitian Self-Dual Abelian Code

For a finite abelian group A of order m and exponent M, M and m share the same prime divisors. Hence, by Corollary 4.2, (M, l) is oddly good if and only if (m, l) is oddly good. Therefore, the next corollary follows from Corollary 4.2 and Theorem 3.6.

Corollary 4.3: Let A be a finite abelian group of odd order m and exponent M. Let l, k be positive integers. Then the following statements are equivalent.

i) There exists a unique Hermitian self-dual code in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$.

ii) (M, l) is oddly good.

iii) (m, l) is oddly good.

iv) (p, l) is oddly good for all prime divisors p of m.

To determine the existence of a unique Hermitian self-dual code in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$, we prove some results concerning the oddly goodness of the pair (p, l) and the value of $\lambda(p, l)$, where p is an odd prime and l is a positive integer.

Proposition 4.4: Let p be an odd prime and let l be a positive integer.

1. If $p \equiv 3 \pmod 8$, then one of the following statements holds.
   i) If l is odd, then $2^1 || \mathrm{ord}_p(2^l)$ and $\lambda(p, l) = 0$.
   ii) If l is even, then $2^0 || \mathrm{ord}_p(2^l)$ and $\lambda(p, l) = 1$.
2. If $p \equiv 5 \pmod 8$, then one of the following statements holds.
   i) If l is odd, then $2^2 || \mathrm{ord}_p(2^l)$ and $\lambda(p, l) = 1$.
   ii) If $l \equiv 2 \pmod 4$, then $2^1 || \mathrm{ord}_p(2^l)$ and $\lambda(p, l) = 0$.
   iii) If $l \equiv 0 \pmod 4$, then $2^0 || \mathrm{ord}_p(2^l)$ and $\lambda(p, l) = 1$.
3. If $p \equiv 7 \pmod 8$, then $2^0 || \mathrm{ord}_p(2^l)$ and $\lambda(p, l) = 1$.

Proof: In each case, the integer i such that $2^i || \mathrm{ord}_p(2^l)$ is obtained in [8, Proposition 2]. From Theorem 4.1 and the definition of λ, we have that (p, l) is bad and $\lambda(p, l) = 1$ if $i = 0$, (p, l) is oddly good and $\lambda(p, l) = 0$ if $i = 1$, and (p, l) is evenly good and $\lambda(p, l) = 1$ if $i > 1$. ■

Proposition 4.5: Let p be a prime such that $p \equiv 1 \pmod 8$ and $2^r || (p - 1)$. Let l be a positive integer.

P1-1. If $r = 3$ and p is represented by the quadratic form $U^2 + 64(U + 2V)^2$, then $2^0 || \mathrm{ord}_p(2^l)$ and $\lambda(p, l) = 1$.

P1-2. If $r = 3$ and p is represented by the quadratic form $U^2 + 256V^2$, then one of the following statements holds.
   i) If l is odd, then $2^1 || \mathrm{ord}_p(2^l)$ and $\lambda(p, l) = 0$.
   ii) If l is even, then $2^0 || \mathrm{ord}_p(2^l)$ and $\lambda(p, l) = 1$.

P1-3. If $r \geq 4$ and p is represented by the quadratic form $U^2 + 64(U + 2V)^2$, then one of the following statements holds.
   i) If $2^s || l$ for some $0 \leq s \leq r - 4$, then $2^{r-2-s} || \mathrm{ord}_p(2^l)$ and $\lambda(p, l) = 1$.
   ii) If $2^{r-3} || l$, then $2^1 || \mathrm{ord}_p(2^l)$ and $\lambda(p, l) = 0$.
   iii) If $2^{r-2} \mid l$, then $2^0 || \mathrm{ord}_p(2^l)$ and $\lambda(p, l) = 1$.

P1-4. If p is represented by the quadratic form $U^2 + 16(U + 2V)^2$, then one of the following statements holds.
   i) If $2^s || l$ for some $0 \leq s \leq r - 3$, then $2^{r-1-s} || \mathrm{ord}_p(2^l)$ and $\lambda(p, l) = 1$.
   ii) If $2^{r-2} || l$, then $2^1 || \mathrm{ord}_p(2^l)$ and $\lambda(p, l) = 0$.
   iii) If $2^{r-1} \mid l$, then $2^0 || \mathrm{ord}_p(2^l)$ and $\lambda(p, l) = 1$.

Proof: From [14, Theorem 6], the following statements hold.

1) If $r = 3$ and p is represented by the quadratic form $U^2 + 64(U + 2V)^2$, then $2^0 || \mathrm{ord}_p(2)$.
2) If $r = 3$ and p is represented by the quadratic form $U^2 + 256V^2$, then $2^1 || \mathrm{ord}_p(2)$.
3) If $r \geq 4$ and p is represented by the quadratic form $U^2 + 64(U + 2V)^2$, then $2^{r-2} || \mathrm{ord}_p(2)$.
4) If p is represented by the quadratic form $U^2 + 16(U + 2V)^2$, then $2^{r-1} || \mathrm{ord}_p(2)$.

Since $\mathrm{ord}_p(2^l) = \frac{\mathrm{ord}_p(2)}{\gcd(\mathrm{ord}_p(2^l), l)}$, in each case, we can determine the integer i such that $2^i || \mathrm{ord}_p(2^l)$. The desired results follow from Theorem 4.1 and the definition of λ, *i.e.*, (p, l) is bad and $\lambda(p, l) = 1$ if $i = 0$, (p, l) is oddly good and $\lambda(p, l) = 0$ if $i = 1$, and (p, l) is evenly good and $\lambda(p, l) = 1$ if $i > 1$. ■

In Proposition 4.5, a prime p in each case is called a prime of type P1-ν where $\nu \in \{1, 2, 3, 4\}$.

From Corollary 4.3, there is a unique Hermitian self-dual abelian code in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ if and only if (p, l) is oddly good for all prime divisors p of the order of A. Hence, by Propositions 4.4 and 4.5, we obtain the following corollaries.

Corollary 4.6: Let A be a finite abelian group of odd order m and let k, l be positive integers. Suppose that m has no prime factor congruent to 1 modulo 8.

1) If l is odd, then there exists a unique Hermitian self-dual abelian code in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ if and only if all prime factors of m are congruent to 3 modulo 8.
2) If $l \equiv 2 \pmod 4$, then there exists a unique Hermitian self-dual abelian code in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ if and only if all prime factors of m are congruent to 5 modulo 8.
3) If $l \equiv 0 \pmod 4$, then there are at least two Hermitian self-dual abelian codes in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$.

Corollary 4.7: Let A be a finite abelian group of odd order m and let k, l be positive integers. Suppose that m has no prime factor congruent to 1 modulo 8 which is not of types P1-1, P1-2, P1-3, and P1-4.

1) If l is odd, then there exists a unique Hermitian self-dual abelian code in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ if and only if each prime factor of m is congruent to 3 modulo 8 or of type P1-2.
2) If $l \equiv 2 \pmod 4$, then there exists a unique Hermitian self-dual abelian code in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ if and only if each prime factor of m is congruent to 5 modulo 8, of type P1-3 with $r = 4$, or of type P1-4 with $r = 3$.
3) If $2^s || l$ where $s \geq 2$, then there exists a unique Hermitian self-dual abelian code in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ if and only if each prime factor of m is of type P1-3 with $r = s + 3$, or of type P1-4 with $r = s + 2$.

Note that one may apply Proposition 4.5 and [8, Theorem 4] to obtain more results on the unique case of Euclidean self-dual cyclic codes in [8] but we do not go into this discussion in this paper.

C. Euclidean Versus Hermitian Self-Dual Abelian Codes

Both Euclidean self-dual abelian codes (see [9]) and Hermitian self-dual abelian codes can exist in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$. In this subsection, we discuss some relationship between them in the case where $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ contains either a unique Euclidean self-dual abelian code or a unique Hermitian self-dual abelian code.

The enumeration of Euclidean self-dual abelian codes in $\mathbb{F}_{2^l}[A \oplus \mathbb{Z}_{2^k}]$ is given in [9]. For our purpose, we recall this result for $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$.

Theorem 4.8 ([9, Theorem 4.6]): Let A be a finite abelian group of odd order with exponent M. Then the number of Euclidean self-dual abelian codes in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ is

$$\mathcal{ESD}_{2^{2l}}(A \oplus \mathbb{Z}_{2^k}) := (2^k+1)^{\frac{1}{2}\sum_{d|M}\chi(d,2l)\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(2^{2l})}}. \tag{IV.1}$$

In particular, $(M, 2l)$ is good if and only if there is exactly one Euclidean self-dual abelian code in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$.
In [9, Theorem 4.6], the latter statement states only the sufficient part. The necessary part follows since $\chi(M, 2l) = 0$ if the exponent of $(2^k + 1)$ in (IV.1) is 0.

Using an observation similar to that before Corollary 4.3, we obtain the next corollary.

Corollary 4.9: Let A be a finite abelian group of odd order m and let l, k be positive integers. Then there exists a unique Euclidean self-dual code in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ if and only if $(m, 2l)$ is good.

The next lemma is key to studying the relationship between the two families of self-dual codes.

Lemma 4.10: Let $d > 1$ be an odd integer and let l be positive integer. Then the following statements hold.

i) (d, l) is evenly good if and only if $(d, 2l)$ is good.
ii) (d, l) is oddly good or bad if and only if $(d, 2l)$ is bad.

Proof: We observe that (d, l) is evenly good if and only if d divides $(2^l)^{2s} + 1 = (2^{2l})^s + 1$ for some positive integer s, or equivalently, $(d, 2l)$ is good. Hence, $i)$ is proved.

The statement $ii)$ follows immediately from $i)$. ∎

Table IV.1 can be concluded from Lemma 4.10, the definitions of χ in (III.3) and λ in (III.4).

TABLE IV.1
$\lambda(d, l)$ AND $\chi(d, 2l)$

(d, l)	$\lambda(d, l)$	$\chi(d, 2l)$
$d = 1$	0	0
bad	1	1
oddly good, $d > 1$	0	1
evenly good, $d > 1$	1	0

In general, the values of $\lambda(d, l)$ and $\chi(d, 2l)$ in Table IV.1 may be helpful for comparing the numbers of self-dual abelian codes from the two families. For the case where $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ contains either a unique Euclidean self-dual abelian code or a unique Hermitian self-dual abelian code, we have the following result.

Corollary 4.11: Let A be a finite abelian group of odd order $m > 1$ and let l, k be positive integers. Then the following statements hold.

i) If $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ contains a unique Euclidean self-dual abelian code, then there exist at least $2^k + 1$ Hermitian self-dual abelian codes in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$.
ii) If $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ contain a unique Hermitian self-dual abelian code, then there exist at least $2^k + 1$ Euclidean self-dual abelian codes in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$.

Proof: To prove $i)$, assume that $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ contains a unique Euclidean self-dual abelian code. By Corollary 4.9, $(m, 2l)$ is good. Then (m, l) is evenly good by Lemma 4.10. Hence, by Theorem 3.6 and Corollary 4.3, there exist at least $2^k + 1$ Hermitian self-dual abelian codes in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$.

To prove $ii)$, assume that $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ contains a unique Hermitian self-dual abelian code. Then (m, l) is oddly good by Corollary 4.3. By Lemma 4.10, $(m, 2l)$ is bad. Therefore, by Theorem 4.8 and Corollary 4.9, $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ contains at least $2^k + 1$ Euclidean self-dual abelian codes. ∎

We note that $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ never contains both a unique Euclidean self-dual abelian code and a unique Hermitian self-dual abelian code simultaneously, except for $|A| = 1$.

V. Distribution of Abelian Groups with a Unique Hermitian Self-Dual Abelian Code

Unlike determining the number of Hermitian self-dual abelian codes, which requires the knowledge of k, the existence of a unique Hermitian self-dual abelian code in $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ is independent of k and it depends only on a positive integer l and the order of A (see Corollary 4.3). Precisely, $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ contains a unique Hermitian self-dual code if and only if $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_2]$ does. Because of this, we begin with the distribution of abelian groups A for which $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_2]$ contains a

unique Hermitian self-dual abelian code and then deduce the asymptotic behavior of the unique case for finite abelian groups whose Sylow 2-subgroup is non-trivial cyclic.

For a finite abelian group A of odd order m, by Corollary 4.3, $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_2]$ contains a unique Hermitian self-dual abelian code if and only if (m, l) is oddly good, or equivalently, $2||\mathrm{ord}_p(2^l)$ for all prime divisors p of m, by Theorem 4.1. Hence, we need to estimate the number of odd positive integers that are the products of primes p such that $2||\mathrm{ord}_p(2^l)$ and estimate the number of non-isomorphic abelian groups A of odd order m.

Let $HA_{2l}(x)$ be the number of non-isomorphic abelian groups A of odd order $m \leq x$ for which $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_2]$ contains a unique Hermitian self-dual abelian code. Let $HC_{2l}(x)$ be the number of odd integers $m \leq x$ for which there exists a unique Hermitian self-dual cyclic code of length $2m$ over $\mathbb{F}_{2^{2l}}$.

Let $\mathcal{P}$ be the set of primes p such that $2||\mathrm{ord}_p(2^l)$ and let $\mathcal{G}$ be the multiplicative subsemigroup of the natural numbers generated by $\mathcal{P}$. Denote by $\mathcal{P}(x)$ the number of primes $p \in \mathcal{P}$ such that $p \leq x$.

Then, by Corollary 4.3 and Theorem 4.1, we have

$$HA_{2l}(x) = \sum_{m \leq x, m \in \mathcal{G}} a(m) = \sum_{m \leq x} \mathrm{char}_{\mathcal{G}}(m) a(m) \tag{V.1}$$

and

$$HC_{2l}(x) = \sum_{m \leq x, m \in \mathcal{G}} 1 = \sum_{m \leq x} \mathrm{char}_{\mathcal{G}}(m), \tag{V.2}$$

where $\mathrm{char}_{\mathcal{G}}(m)$ is the characteristic function on $\mathcal{G}$ defined by

$$\mathrm{char}_{\mathcal{G}}(m) = \begin{cases} 1 & \text{if } m \in \mathcal{G}, \\ 0 & \text{if } m \notin \mathcal{G}, \end{cases}$$

and $a(m)$ is the number of non-isomorphic abelian groups of odd order m.

In [5], some useful results have been discussed in a more general set up. Let $\mathcal{S}$ be a multiplicative subsemigroup of the natural numbers generated by a set $\mathcal{Q}$ of primes and let $\mathcal{Q}(x)$ be the number of primes $p \in \mathcal{Q}$ such that $p \leq x$. Denote by $\mathrm{Li}(x)$ the logarithmic integral $\int_2^x \frac{1}{\log t} dt$. Assuming the Generalized Riemann Hypothesis, we have the following result.

Lemma 5.1 ([5, Theorem 4.1]): If $\mathcal{Q}(x) = \tau \mathrm{Li}(x) + O(x \log^{-\gamma-2} x)$ with $\gamma > 0$ and $0 < \tau < 1$, then, for all $\epsilon > 0$, we have

$$\sum_{t \in \mathcal{S}, t \leq x} a(t) = x \sum_{0 \leq i < \gamma} b_i \log^{\tau-i-1} x + O(x \log^{\tau-\gamma-1+\epsilon} x)$$

where the b_i's are constants possibly dependent on $\mathcal{S}$ such that

$$b_0 = \frac{1}{\Gamma(\tau)} \lim_{s \downarrow 1} (s-1)^\tau \sum_{t \in \mathcal{S}} \frac{a(t)}{t^s}$$

and Γ denotes the Gamma function.

Now, we are ready to estimate $HA_{2l}(x)$.

Theorem 5.2: Let l be a positive integer and let ν be a non-negative integer such that $2^\nu || l$. Then, for all $\epsilon > 0$, we have

$$HA_{2l}(x) = b_0 x \log^{\delta-1} x + O(x \log^{\delta-2+\epsilon} x), \tag{V.3}$$

where

$$b_0 = \frac{1}{\Gamma(\delta)} \lim_{s \downarrow 1} (s-1)^\delta \sum_{m \in \mathcal{G}} \frac{a(m)}{m^s}$$

and

$$\delta = \begin{cases} \frac{7}{24} & \text{if } \nu = 0, \\ \frac{1}{3} & \text{if } \nu = 1, \\ \frac{1}{3 \cdot 2^{1+\nu}} & \text{if } \nu \geq 2. \end{cases} \tag{V.4}$$

Proof: Let $\mathcal{P}'$ be the set of odd primes which are not in $\mathcal{P}$ and let $\mathcal{P}'(x)$ be the number of primes $p \in \mathcal{P}'$ such that $p \leq x$. Then the elements in $\mathcal{P}'$ are primes p such that $2 \nmid \mathrm{ord}_p(2^l)$ or $2^2 \mid \mathrm{ord}_p(2^l)$. It has been proved in [4, Lemma A.2] that

$$\mathcal{P}'(x) = (1-\delta)\mathrm{Li}(x) + O(\sqrt{x} \log^2 x), \tag{V.5}$$

where δ is defined in (V.4).

Assuming the Generalized Riemann Hypothesis, it is well known that the number of primes which are less than or equal to x is

$$\pi(x) := \mathrm{Li}(x) + O(\sqrt{x}\log x). \tag{V.6}$$

Combining (V.5) and (V.6), we have

$$\begin{aligned}\mathcal{P}(x) = \pi(x) - \mathcal{P}'(x) &= \delta\mathrm{Li}(x) + O(\sqrt{x}\log^2 x)\\ &= \delta\mathrm{Li}(x) + O(x\log^{-3} x).\end{aligned} \tag{V.7}$$

Since (V.7) satisfies the assumption in Lemma 5.1 with $\gamma = 1$, the result follows from Lemma 5.1 and (V.1). ∎

For a fixed l, Theorem 5.2 implies that $\frac{HA_{2l}(x)}{x} \to 0$ as $x \to \infty$. Therefore, the case where $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_2]$ contains a unique Hermitian self-dual abelian code occurs less frequently as the order of A grows, where A runs over all finite abelian groups of odd order. Since $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_2]$ contains a unique Hermitian self-dual abelian code if and only if $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ does, the case where $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_{2^k}]$ contains a unique Hermitian self-dual abelian code occurs less frequently as A runs over all finite abelian groups of odd order and k runs over all positive integers.

Remark 5.3: It has been shown in [5] that the set of integers multiplicatively generated by $\mathcal{P}'$ in the proof of Theorem 5.2 is the set of all odd integers m such that, for all abelian groups A of order m, $\mathbb{F}_{2^{2l}}[A]$ contains an abelian code for which an extended code is Hermitian self-dual (see [5] for the definition of an extended abelian code). Hence, for an abelian group A of odd order m, $\mathbb{F}_{2^{2l}}[A \oplus \mathbb{Z}_2]$ contains a unique Hermitian self-dual abelian code if and only if $\mathbb{F}_{2^{2l}}[A]$ does not contain any abelian code for which an extended code is Hermitian self-dual.

In the light of [15, Theorem 6] (see also [5, Lemma 4.2]), if $f : \mathbb{N} \cup \{0\} \to \mathbb{R}^+ \cup \{0\}$ is a multiplicative function such that

$$0 \le f(p^r) \le c_1 c_2^r, 1 \le c_1, 1 \le c_2 < 2, \tag{V.8}$$

and

$$\sum_{p \le x} f(p) = \tau\mathrm{Li}(x) + O(x\log^{-3} x) \text{ with } \tau > 0, \tag{V.9}$$

then, for all $\epsilon > 0$, we have

$$\sum_{t \le x} f(t) = c_0 x\log^{\tau-1} x + O(x\log^{\tau-2+\epsilon} x), \tag{V.10}$$

where

$$c_0 = \frac{1}{\Gamma(\tau)} \lim_{s \downarrow 1}(s-1)^\tau \sum_{t=1}^{\infty} \frac{f(t)}{t^s}.$$

From (V.7),

$$\sum_{p \le x} \mathrm{char}_{\mathcal{G}}(p) = \mathcal{P}(x) = \delta\mathrm{Li}(x) + O(x\log^{-3} x),$$

where $\delta > 0$ is defined in (V.4). Then $\mathrm{char}_{\mathcal{G}}$ satisfies (V.8) and (V.9). Therefore, the following corollary follows from (V.2).

Corollary 5.4: Let l be a positive integer and let ν be a non-negative integer such that $2^\nu || l$. Then, for all $\epsilon > 0$, we have that

$$HC_{2l}(x) = c_0 x\log^{\delta-1} x + O(x\log^{\tau-2+\epsilon} x), \tag{V.11}$$

where

$$c_0 = \frac{1}{\Gamma(\delta)} \lim_{s \downarrow 1}(s-1)^\delta \sum_{m \in \mathcal{G}} \frac{1}{m^s}$$

and δ is defined in (V.4).

Corollary 5.4 implies that, for any fixed l, as x grows, $\frac{HC_{2l}(x)}{x}$ tends to 0. Hence, the case where there exists a unique Hermitian self-dual cyclic code over $\mathbb{F}_{2^{2l}}$ occurs less frequently as the length runs over all even integers.

VI. Conclusion

We have characterized Hermitian self-dual abelian codes in $\mathbb{F}_{q^2}[G]$, where G is a finite abelian group. This characterization allows us to express the enumeration of such codes easily in the case where $\mathbb{F}_{q^2}[G]$ is a principal ideal group ring. The criterion for and the distribution of finite abelian groups whose group rings contain a unique Hermitian self-dual abelian code have been established. As a special case, this work has answered an open question in [8] concerning Hermitian self-dual cyclic codes.

Most of the results have been focused on Hermitian self-dual abelian codes in the case of principal ideal group rings. It would be interesting to study the enumeration of Hermitian self-dual abelian codes in a non-principal ideal group ring or study the enumeration of Hermitian self-dual (non-abelian) group codes.

ACKNOWLEDGEMENTS

Part of this work was done when S. Jitman was a research fellow at the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore.

The authors thank the anonymous referees for helpful comments.

REFERENCES

[1] S. Benson, "Students ask the darnedest things: A result in elementary group theory," *Math. Mag.,* vol. 70, pp. 207–211, 1997.
[2] J. J. Bernal and J. J. Simón, "Information sets from defining sets in abelian codes," *IEEE Trans. Inform. Theory,* vol. 57, pp. 7990–7999, 2011.
[3] H. Chabanne, "Permutation decoding of abelian codes," *IEEE Trans. Inform. Theory,* vol. 38, pp. 1826–1829, 1992.
[4] L. Dicuangco, P. Moree, and P. Solé, *The Lengths of Hermitian Self-dual Extended Duadic Codes.* MPI // Max-Planck-Institut für Mathematik, Bonn, 2005.
[5] L. Dicuangco, P. Moree, and P. Solé, *On the Existence of Hermitian Self-dual Extended Abelian Group Codes.* MPI // Max-Planck-Institut für Mathematik, Bonn, 2006.
[6] C. Ding, D. R. Kohel, and S. Ling, "Split group codes," *IEEE Trans. Inform. Theory,* vol. 46, pp. 485–495, 2000.
[7] J. L. Fisher and S. K. Sehgal, "Principal ideal group rings," *Comm. Algebra,* vol. 4, pp. 319–325, 1976.
[8] Y. Jia, S. Ling, and C. Xing, "On self-dual cyclic codes over finite fields," *IEEE Trans. Inform. Theory,* vol. 57, pp. 2243–2251, 2011.
[9] S, Jitman, S. Ling, H. Liu, and X. Xie, "Abelian codes in principal ideal group algebras," *IEEE Trans. Info. Theory,* vol. 59, pp. 3046–3058, 2013.
[10] X. Kai and S. Zhu, "On cyclic self-dual codes," *AAECC*, vol. 19, pp. 509–525, 2008.
[11] A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Trans. Info. Theory,* vol. 52, pp. 4892–4914, 2006.
[12] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes I: Finite fields," *IEEE Trans. Inform. Theory,* vol.47, pp. 2751–2760, 2001.
[13] S. Ling and C. Xing, "Polyadic codes revisited," *IEEE Trans. Inform. Theory,* vol. 50, pp. 200–207, 2004.
[14] P. Moree, On the divisors of $a^k + b^k$, *Acta Arithmetica*, vol.LXXX, no. 3, pp. 197–212, 1997.
[15] P. Moree and J. Cazaran, "On a claim of Ramanujan in his first letter to Hardy," *Exposition. Math.,* vol. 17, no. 4, pp. 289–311, 1999.
[16] G. Nebe, E. M. Rains, and N. J. A. Sloane, *Self-Dual Codes and Invariant Theory,* Algorithms and Computation in Mathematics vol. 17. Berlin, Heidelberg: Springer-Verlag, 2006.
[17] D. S. Passman, *The Algebraic Structure of Group Rings.* Wiley, New York, 1977.
[18] B. S. Rajan and M. U. Siddiqi, "Transform domain characterization of abelian codes," *IEEE Trans. Inform. Theory,* vol. 38, pp. 1817–1821, 1992.
[19] R. E. Sabin, "On determining all codes in semi-simple group rings," *Lecture Notes in Comput. Sci.,* vol. 673, pp. 279–290, 1993.
[20] W. Willems, "A note on self-dual group codes," *IEEE Trans. Inform. Theory,* vol. 48, pp. 3107–3109, 2002.