J. Algebra Comb. Discrete Appl.
6(2) • 75–94

Received: 2 January 2019
Accepted: 16 April 2019

Journal of Algebra Combinatorics Discrete Structures and Applications

Self-dual and complementary dual abelian codes over Galois rings*

Research Article

Somphong Jitman, San Ling

Abstract: Self-dual and complementary dual cyclic/abelian codes over finite fields form important classes of linear codes that have been extensively studied due to their rich algebraic structures and wide applications. In this paper, abelian codes over Galois rings are studied in terms of the ideals in the group ring $\mathrm{GR}(p^r, s)[G]$, where G is a finite abelian group and $\mathrm{GR}(p^r, s)$ is a Galois ring. Characterizations of self-dual abelian codes have been given together with necessary and sufficient conditions for the existence of a self-dual abelian code in $\mathrm{GR}(p^r, s)[G]$. A general formula for the number of such self-dual codes is established. In the case where $\gcd(|G|, p) = 1$, the number of self-dual abelian codes in $\mathrm{GR}(p^r, s)[G]$ is completely and explicitly determined. Applying known results on cyclic codes of length p^a over $\mathrm{GR}(p^2, s)$, an explicit formula for the number of self-dual abelian codes in $\mathrm{GR}(p^2, s)[G]$ are given, where the Sylow p-subgroup of G is cyclic. Subsequently, the characterization and enumeration of complementary dual abelian codes in $\mathrm{GR}(p^r, s)[G]$ are established. The analogous results for self-dual and complementary dual cyclic codes over Galois rings are therefore obtained as corollaries.

2010 MSC: 94B15, 94B05, 16A26

Keywords: Abelian codes, Galois rings, Self-dual codes, Complementary dual codes, Codes over rings

1. Introduction

Algebraically structured codes over finite fields with self-duality and complementary duality are important families of linear codes that have been extensively studied for both theoretical and practical reasons (see [1], [3], [11], [13], [15], [21], [26], [27], and references therein). Codes over finite rings have been interesting since it was proven that some binary non-linear codes such as the Kerdock, Preparata, and Goethal codes are the Gray images of linear codes over $\mathbb{Z}_4$ [10]. Algebraically structured codes such

* *S. Jitman was supported by the Thailand Research Fund and Silpakorn University under Research Grant RSA6280042. S. Ling was supported by Nanyang Technological University Research Grant M4080456.*
Somphong Jitman(Corresponding Author); Department of Mathematics, Faculty of Science, Silpakorn University, Nakhon Pathom 73000, Thailand (email: sjitman@gmail.com).
San Ling; Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371, Republic of Singapore (email: lingsan@ntu.edu.sg).

as cyclic, constacyclic, and abelian codes have extensively been studied over $\mathbb{Z}_{p^r}$, Galois rings, and finite chain rings in general (see [7],[18], and references therein).

The characterization and enumeration of Euclidean self-dual cyclic codes over finite fields have been established in [11] and generalized to Euclidean and Hermitian self-dual abelian codes over finite fields in [13] and [15], respectively. Over some finite rings, a characterization of self-dual cyclic, constacyclic and abelian codes has been done (see, for example, [1], [7],[16], [17], [24], and [26]). In [1], [5], [4] and [23], characterization and enumeration of Euclidean and Hermitian self-dual cyclic codes over finite chain rings have been discussed. Euclidean complementary dual cyclic codes over finite fields have been studied in [27]. Recently, they have been generalized to Euclidean and Hermitian complementary dual abelian codes over finite fields in [3]. The complete characterization and enumeration of complementary dual abelian codes over finite fields have been established in the said paper.

In this paper, we focus on abelian codes over Galois rings $\mathrm{GR}(p^r, s)$, *i.e.,* ideals in the group ring $\mathrm{GR}(p^r, s)[G]$ of an abelian group G over a Galios ring $\mathrm{GR}(p^r, s)$. Specifically, we study self-dual and complementary dual abelian codes in $\mathrm{GR}(p^r, s)[G]$ with respect to both the Euclidean and Hermitian inner products. We characterize such self-dual abelian codes and determine necessary and sufficient conditions for the existence of a self-dual abelian code in $\mathrm{GR}(p^r, s)[G]$. We give a formula for the number of self-dual abelian codes in $\mathrm{GR}(p^r, s)[G]$. Under the restriction *i)* $\gcd(|G|, p) = 1$; or *ii)* $r = 2$ and the Sylow p-subgroup of G is cyclic, the numbers of self-dual abelian codes in $\mathrm{GR}(p^r, s)[G]$ are explicitly determined. Subsequently, the characterization and enumeration of complementary dual abelian codes in $\mathrm{GR}(p^r, s)[G]$ are given. The number of complementary dual abelian codes in $\mathrm{GR}(p^r, s)[G]$ is shown to be independent of r and the Sylow p-subgroup of G.

We note that the Hermitian duality is meaningful only when s is even. Since we study Euclidean and Hermitian self-dual codes in parallel, the assumption that s is even is included whenever we refer to the Hermitian duality.

The paper is organized as follows. In Section 2, we recall and prove some basic results for group rings, abelian codes, and their duals. In Section 3, we present the characterization and a general set up for the enumeration of self-dual abelian codes in $\mathrm{GR}(p^r, s)[G]$. The complete enumeration of Euclidean and Hermitian self-dual abelian codes in $\mathrm{GR}(p^r, s)[G]$ is given in the special cases where *i)* $\gcd(p, |G|) = 1$; and *ii)* $r = 2$ and the Sylow p-subgroup of G is cyclic. In Section 4, the characterization and enumeration of complementary dual abelian codes in $\mathrm{GR}(p^r, s)[G]$ are given.

2. Preliminaries

In this section, we recall some definitions and basic properties of abelian codes and prove some results on their Euclidean and Hermitian duals.

2.1. Abelian codes

For a finite 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 rings over R with the indeterminate Y, where the indices are computed additively in G. By convention, $Y^0 = 1$ is the identity of R, where 0 is the additive identity of G.

An *abelian code* in $R[G]$ is defined to be an ideal of $R[G]$. If $G = \{g_1, g_2, \ldots, g_n\}$ is an abelian group of order n, it is not dificult to see that the map $\pi : R[G] \to R^n$ defined by $\sum_{i=1}^n \alpha_{g_i} Y^{g_i} \mapsto (\alpha_{g_1}, \alpha_{g_2}, \ldots, \alpha_{g_n})$ is an R-module isomorphism. Hence, an abelian code C in $R[G]$ can be viewed as an R-submodule $\pi(C)$ in R^n. Precisely, $\pi(C)$ is a linear code of length n over R. If G is cyclic of order n, an abelian code in $R[G]$ becomes a classical cyclic code of length n over R. In this case, an abelian code will be referred to as a *cyclic code*. It is well known that a cyclic code of length n over R can also be regarded as an ideal

in the quotient polynomial ring $R[X]/\langle X^n - 1\rangle$.

From now on, we focus on the case where the ring is a Galois ring $\mathrm{GR}(p^r, s)$, a Galois extension of degree s of an integer residue ring $\mathbb{Z}_{p^r}$. Let ξ be an element in $\mathrm{GR}(p^r, s)$ that generates a Teichmüller set $\mathcal{T}_s$ of $\mathrm{GR}(p^r, s)$. In other words, $\mathcal{T}_s = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^s-2}\}$. Then every element in $\mathrm{GR}(p^r, s)$ has a unique p-adic expansion of the form

$$\alpha = \alpha_0 + \alpha_1 p + \cdots + \alpha_{r-1} p^{r-1},$$

where $\alpha_i \in \mathcal{T}_s$ for all $i = 0, 1, \ldots, r-1$. In the case where s is even, the map $\bar{} : \mathrm{GR}(p^r, s) \to \mathrm{GR}(p^r, s)$ defined by

$$\overline{\alpha} = \alpha_0^{p^{s/2}} + \alpha_1^{p^{s/2}} p + \cdots + \alpha_{r-1}^{p^{s/2}} p^{r-1} \tag{1}$$

is a ring automorphism on $\mathrm{GR}(p^r, s)$. For more details on Galois rings, we refer the readers to [25].

Let P be the Sylow p-subgroup of G and let A be a complementary subgroup of P in G. Then $G \cong A \times P$. Let $\mathcal{R} := \mathrm{GR}(p^r, s)[A]$. Then the map $\Phi : \mathrm{GR}(p^r, s)[G] \to \mathcal{R}[P]$ given by

$$\Phi\Big(\sum_{a\in A}\sum_{b\in P} \alpha_{a+b} Y^{a+b}\Big) = \sum_{b\in P} \boldsymbol{\alpha}_b(Y) Y^b,$$

where $\boldsymbol{\alpha}_b(Y) = \sum_{a\in A} \alpha_{a+b} Y^a \in \mathcal{R}$, is a well-known ring isomorphism (see [19, Section 3.2, Exercise 4]). Then Φ induces a one-to-one correspondence between the ideals in $\mathrm{GR}(p^r, s)[G]$ and the ideals in $\mathcal{R}[P]$. Since an abelian code is an ideal in a group ring, the above discussion can be interpreted in terms of abelian codes as follows.

Lemma 2.1. *The map Φ induces a one-to-one correspondence between the abelian codes in $\mathrm{GR}(p^r, s)[G]$ and the abelian codes in $\mathcal{R}[P]$.*

An abelian code $\mathcal{C}$ in $\mathrm{GR}(p^r, s)[G]$ is said to be *Euclidean self-dual* (resp., *Euclidean complementary dual*) if $\mathcal{C} = \mathcal{C}^{\perp_{\mathrm{E}}}$ (resp., $\mathcal{C} \cap \mathcal{C}^{\perp_{\mathrm{E}}} = \{0\}$), where $\mathcal{C}^{\perp_{\mathrm{E}}}$ is the dual of $\mathcal{C}$ with respect to the form

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

where $\boldsymbol{u} = \sum_{g\in G} \alpha_g Y^g$ and $\boldsymbol{v} = \sum_{g\in G} \beta_g Y^g$.

Define an *involution* $\widehat{\ }$ on $\mathcal{R}$ to be the $\mathrm{GR}(p^r, s)$-module homomorphism that fixes $\mathrm{GR}(p^r, s)$ and sends Y^a to Y^{-a} for all $a \in A$. An abelian code D in $\mathcal{R}[P]$ is said to be $\widehat{\ }$*-self-dual* if $D = D^{\perp_{\widehat{\ }}}$, where $D^{\perp_{\widehat{\ }}}$ is the dual of D with respect to the form

$$\langle \boldsymbol{x}, \boldsymbol{y}\rangle_{\widehat{\ }} := \sum_{b\in P} \boldsymbol{x}_b(Y)\widehat{\boldsymbol{y}_b(Y)},$$

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

In addition, if s is even, an abelian code $\mathcal{C}$ in $\mathrm{GR}(p^r, s)[G]$ is said to be *Hermitian self-dual* (resp., *Hermitian complementary dual*) if $\mathcal{C} = \mathcal{C}^{\perp_{\mathrm{H}}}$ (resp., $\mathcal{C} \cap \mathcal{C}^{\perp_{\mathrm{H}}} = \{0\}$), where $\mathcal{C}^{\perp_{\mathrm{H}}}$ is the dual of $\mathcal{C}$ with respect to the form

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

where $\boldsymbol{u} = \sum_{g\in G} \alpha_g Y^g$ and $\boldsymbol{v} = \sum_{g\in G} \beta_g Y^g$.

Define an *involution* $\widetilde{\ }$ on $\mathcal{R}$ to be the $\mathrm{GR}(p^r,s)$-module homomorphism that sends α to $\overline{\alpha}$ for all $\alpha \in \mathrm{GR}(p^r,s)$ and sends Y^a to Y^{-a} for all $a \in A$. An abelian code D in $\mathcal{R}[P]$ is said to be $\sim$*-self-dual* if $D = D^{\perp_\sim}$, where $D^{\perp_\sim}$ is the dual of D with respect to the form

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

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

Similarly to the finite field case, the following relations among the above forms can be verified using arguments similar to those in [13, Proposition 2.4] and [15, Proposition 2.4].

Lemma 2.2. *Let r and s be positive integers and let p be a prime number. Let $G \cong A \times P$ be as above and $\boldsymbol{u}, \boldsymbol{v} \in \mathrm{GR}(p^r,s)[G]$. Then the following statements hold.*

i) $\langle Y^g \boldsymbol{u}, \boldsymbol{v} \rangle_{\mathrm{E}} = 0$ *for all* $g \in G$ *if and only if* $\langle Y^b \Phi(\boldsymbol{u}), \Phi(\boldsymbol{v}) \rangle_{\widehat{\ }} = 0$ *for all* $b \in P$.

ii) If s is even, 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* $b \in P$.

The next corollary follows immediately.

Corollary 2.3. *Let r and s be positive integers and let p be a prime number. Let $\mathcal{C}$ be an abelian code in* $\mathrm{GR}(p^r,s)[G]$. *Then the following statements hold.*

i) $\Phi(\mathcal{C})^{\perp_{\widehat{\ }}} = \Phi(\mathcal{C}^{\perp_{\mathrm{E}}})$. *In particular, $\mathcal{C}$ is Euclidean self-dual if and only if $\Phi(\mathcal{C})$ is $\widehat{\ }$-self-dual.*

ii) If s is even, then $\Phi(\mathcal{C})^{\perp_\sim} = \Phi(\mathcal{C}^{\perp_{\mathrm{H}}})$. *In particular, $\mathcal{C}$ is Hermitian self-dual if and only if $\Phi(\mathcal{C})$ is $\sim$-self-dual.*

Therefore, to study Euclidean and Hermitian self-dual abelian codes in $\mathrm{GR}(p^r,s)[G]$, it is sufficient to consider $\widehat{\ }$-self-dual and $\sim$-self-dual abelian codes in $\mathcal{R}[P]$, respectively.

2.2. Decomposition and dualities

Recall that p represents a prime number, s is a positive integer, and A is a finite abelian group such that $\gcd(p,|A|) = 1$.

For coprime positive integers i, j, let $\mathrm{ord}_i(j)$ denote the multiplicative order of j modulo i. For $a \in A$, denote by $\mathrm{ord}(a)$ the additive order of a in A. For each $a \in A$, a p^s*-cyclotomic class* of A containing a is defined to be the set

$$S_{p^s}(a) := \{p^{si} \cdot a \mid i = 0, 1, \dots\} = \{p^{si} \cdot a \mid 0 \le i < \mathrm{ord}_{\mathrm{ord}(a)}(p^s)\},$$

where $p^{si} \cdot a := \sum_{j=1}^{p^{si}} a$ in A. A p^s-cyclotomic class $S_{p^s}(a)$ is said to be of *type* I if $a = -a$, *type* II if $S_{p^s}(a) = S_{p^s}(-a)$ and $a \ne -a$, or *type* III if $S_{p^s}(-a) \ne S_{p^s}(a)$. If s is even, a p^s-cyclotomic class $S_{p^s}(a)$ is said to be of *type* II′ if $S_{p^s}(a) = S_{p^s}(-p^{s/2} \cdot a)$ or *type* III′ if $S_{p^s}(-p^{s/2} \cdot a) \ne S_q(a)$, where $-p^{s/2} \cdot a$ denotes $p^{s/2} \cdot (-a)$.

Remark 2.4. *We have the following facts for the p^s-cyclotomic classes of A (see [13, Remark 2.5] and [15, Remark 2.6]).*

1. *A p^s-cyclotomic class of type* I *has cardinality one.*
2. *$S_{p^s}(0)$ is a p^s-cyclotomic class of both types* I *and* II′.
3. *If a p^s-cyclotomic class of type* II *exists, then its cardinality is even. Moreover, if $S_{p^s}(a)$ is a p^s-cyclotomic class of type* II *of cardinality 2ν, then $-a = p^{s\nu} \cdot a$.*

4. A p^s-cyclotomic class of A of type $\mathbb{II}'$ has odd cardinality. Moreover, if $S_{p^s}(a)$ is a p^s-cyclotomic class of type $\mathbb{II}'$ of cardinality ν, then $-a = p^{s\nu/2} \cdot a$ and $-p^{s/2} \cdot a = p^{s(\nu+1)/2} \cdot a$.

Assume that A has cardinality m and exponent M. By the Fundamental Theorem of finite abelian groups, A can be written as a direct product of finite cyclic groups $A = \prod_{i=1}^{N} \mathbb{Z}_{m_i}$, where $\mathbb{Z}_{m_i} = \{0, 1, \ldots, m_i - 1\}$ denotes the additive cyclic group of order $m_i \geq 2$ for all $1 \leq i \leq N$. Then an element $b \in A$ can be written as $b = (b_1, b_2, \ldots, b_N)$, where $b_i \in \mathbb{Z}_{m_i}$. For each $h \in A$, let $\gamma_h : A \to \mathbb{Z}$ be defined by

$$\gamma_h(b) = \sum_{i=1}^{N} b_i h_i (M/m_i), \tag{2}$$

where the sum is a rational sum.

Let μ be the order of p^s modulo M. Denote by ζ a primitive Mth root of unity in $\mathrm{GR}(p^r, s\mu)$. For a given $\boldsymbol{c} = \sum_{a \in A} c_a Y^a \in \mathcal{R} := \mathrm{GR}(p^r, s)[A]$, its Discrete Fourier Transform (DFT) is $\breve{\boldsymbol{c}} = \sum_{h \in A} \breve{c}_h Y^h$, where

$$\breve{c}_h = \sum_{a \in A} c_a \zeta^{\gamma_h(a)} \in \mathrm{GR}(p^r, s\mu). \tag{3}$$

Moreover, if $S_{p^s}(h)$ has cardinality ν, then it is not difficult to verify that $\breve{c}_h$ is contained in a subring of $\mathrm{GR}(p^r, s\mu)$ which is isomorphic to $\mathrm{GR}(p^r, s\nu)$.

Using this DFT, the decomposition of $\mathcal{R} := \mathrm{GR}(p^r, s)[A]$, where $\gcd(p, |A|) = 1$, has been given in [18] in terms of the mix-radix representation of the elements in A. In order to utilize the decomposition in [18] for characterizing self-dual codes, we need to consider a suitable rearrangement of the terms in the decomposition.

2.2.1. Euclidean case

For the Euclidean self-duality, we consider the rearrangement based on the p^s-cyclotomic classes of types $\mathrm{I} - \mathbb{III}$ as follows. Assume that A contains L p^s-cyclotomic classes. Without loss of generality, let $\{a_1, a_2, \ldots, a_L\}$ be a set of representatives of the p^s-cyclotomic classes such that $\{a_i \mid i = 1, 2, \ldots, t_{\mathrm{I}}\}$, $\{a_{t_{\mathrm{I}}+j} \mid j = 1, 2, \ldots, t_{\mathrm{II}}\}$ and $\{a_{t_{\mathrm{I}}+t_{\mathrm{II}}+k}, a_{t_{\mathrm{I}}+t_{\mathrm{II}}+t_{\mathrm{III}}+k} = -a_{t_{\mathrm{I}}+t_{\mathrm{II}}+k} \mid k = 1, 2, \ldots, t_{\mathrm{III}}\}$ are sets of representatives of p^s-cyclotomic classes of types $\mathrm{I}, \mathbb{II}$, and $\mathbb{III}$, respectively, where $L = t_{\mathrm{I}} + t_{\mathrm{II}} + 2t_{\mathrm{III}}$. From the definition, $|S_{p^s}(a_i)| = 1$ for all $i = 1, 2, \ldots, t_{\mathrm{I}}$. From Remark 2.4, the order of the p^s-cyclotomic classes of type $\mathbb{II}$ is even order. For $j = 1, 2, \ldots, t_{\mathrm{II}}$, let $2e_j$ denote the cardinality of $S_{p^s}(a_{t_{\mathrm{I}}+j})$. For $k = 1, 2, \ldots, t_{\mathrm{III}}$, $S_{p^s}(a_{t_{\mathrm{I}}+t_{\mathrm{II}}+k})$ and $S_{p^s}(a_{t_{\mathrm{I}}+t_{\mathrm{II}}+t_{\mathrm{III}}+k})$ have the same cardinality and denote it by f_k.

Rearranging the terms in the decomposition in [18] based on the p^s-cyclotomic classes of A of types $\mathrm{I} - \mathbb{III}$, we have

$$\mathcal{R} \cong \left(\prod_{i=1}^{t_{\mathrm{I}}} \mathrm{GR}(p^r, s) \right) \times \left(\prod_{j=1}^{t_{\mathrm{II}}} \mathrm{GR}(p^r, 2se_j) \right) \times \left(\prod_{k=1}^{t_{\mathrm{III}}} (\mathrm{GR}(p^r, sf_k) \times \mathrm{GR}(p^r, sf_k)) \right), \tag{E1}$$

where $\mathrm{GR}(p^r, 2se_j)$ is induced by $S_{p^s}(a_{t_{\mathrm{I}}+j})$ for all $j = 1, 2, \ldots, t_{\mathrm{II}}$ and $\mathrm{GR}(p^r, sf_k) \times \mathrm{GR}(p^r, sf_k)$ is induced by $(S_{p^s}(a_{t_{\mathrm{I}}+t_{\mathrm{II}}+k}), S_{p^s}(-a_{t_{\mathrm{I}}+t_{\mathrm{II}}+k}))$ for all $k = 1, 2, \ldots, t_{\mathrm{III}}$. For more details and the explicit isomorphism, the readers may refer to [18, Section II].

It follows that

$$\mathcal{R}[P] \cong \left(\prod_{i=1}^{t_{\mathrm{I}}} \mathrm{GR}(p^r, s)[P] \right) \times \left(\prod_{j=1}^{t_{\mathrm{II}}} \mathrm{GR}(p^r, 2se_j)[P] \right) \times \left(\prod_{k=1}^{t_{\mathrm{III}}} (\mathrm{GR}(p^r, sf_k)[P] \times \mathrm{GR}(p^r, sf_k)[P]) \right). \tag{E2}$$

Therefore, by Lemma 2.1, every abelian code in $\mathrm{GR}(p^r,s)[G] \cong \mathcal{R}[P]$ can be written in the form

$$\mathcal{C} \cong \left(\prod_{i=1}^{t_{\mathrm{I}}} U_i\right) \times \left(\prod_{j=1}^{t_{\mathrm{II}}} V_j\right) \times \left(\prod_{k=1}^{t_{\mathrm{III}}} (W_k \times W_k')\right), \tag{E3}$$

where U_i is an abelian code in $\mathrm{GR}(p^r,s)[P]$, V_j is an abelian code in $\mathrm{GR}(p^r,2se_j)[P]$, and W_k, W_k' are abelian codes in $\mathrm{GR}(p^r,sf_k)[P]$ for all $i=1,2,\ldots,t_{\mathrm{I}}$, $j=1,2,\ldots,t_{\mathrm{II}}$, and $k=1,2,\ldots,t_{\mathrm{III}}$.

The Euclidean dual of $\mathcal{C}$ in (E3) can be viewed to be of the form

$$\mathcal{C}^{\perp_{\mathrm{E}}} \cong \left(\prod_{i=1}^{t_{\mathrm{I}}} U_i^{\perp_{\mathrm{E}}}\right) \times \left(\prod_{j=1}^{t_{\mathrm{II}}} V_j^{\perp_{\mathrm{H}}}\right) \times \left(\prod_{k=1}^{t_{\mathrm{III}}} \left((W_k')^{\perp_{\mathrm{E}}} \times W_k^{\perp_{\mathrm{E}}}\right)\right). \tag{E4}$$

The detailed justification for (E4) is provided in Appendix A.1.

2.2.2. Hermitian case

In the case where s is even, we consider the other rearrangement of the decomposition of $\mathcal{R}$ in terms of the p^s-cyclotomic classes of A of types $\mathbb{I}'$ and $\mathbb{III}'$. Let $\{b_1=0, b_2, \ldots, b_L\}$ denote a set of representatives of the p^s-cyclotomic classes such that $\{b_j \mid j=1,2,\ldots,t_{\mathbb{II}'}\}$ and $\{b_{t_{\mathbb{II}'}+k}, b_{t_{\mathbb{II}'}+t_{\mathbb{III}'}+k} = -p^{s/2}\cdot b_{t_{\mathbb{II}'}+k} \mid k=1,2,\ldots,t_{\mathbb{III}'}\}$ represent p^s-cyclotomic classes of types $\mathbb{I}'$ and $\mathbb{III}'$, respectively, where $L = t_{\mathbb{II}'} + 2t_{\mathbb{III}'}$. For $j=1,2,\ldots,t_{\mathbb{II}'}$, let $\acute{e}_j$ denote the cardinality of $S_{p^s}(b_j)$. For $k=1,2,\ldots,t_{\mathbb{III}'}$, $S_{p^s}(b_{t_{\mathbb{II}'}+k})$ and $S_{p^s}(b_{t_{\mathbb{II}'}+t_{\mathbb{III}'}+k})$ have the same cardinality and denote it by $\acute{f}_k$.

Rearranging the terms in the decomposition in [18] based on the p^s-cyclotomic classes of A of types $\mathbb{I}'$ and $\mathbb{III}'$, we have

$$\mathcal{R} \cong \left(\prod_{j=1}^{t_{\mathbb{II}'}} \mathrm{GR}(p^r, s\acute{e}_j)\right) \times \left(\prod_{k=1}^{t_{\mathbb{III}'}} \left(\mathrm{GR}(p^r, s\acute{f}_k) \times \mathrm{GR}(p^r, s\acute{f}_k)\right)\right), \tag{H1}$$

where $\mathrm{GR}(p^r, s\acute{e}_j)$ is induced by $S_{p^s}(b_j)$ for all $j=1,2,\ldots,t_{\mathbb{II}'}$ and $\mathrm{GR}(p^r, s\acute{f}_k) \times \mathrm{GR}(p^r, s\acute{f}_k)$ is induced by $\left(S_{p^s}(b_{t_{\mathbb{II}'}+k}), S_{p^s}(-p^{s/2}\cdot b_{t_{\mathbb{II}'}+k})\right)$ for all $k=1,2,\ldots,t_{\mathbb{III}'}$.

Consequently,

$$\mathcal{R}[P] \cong \left(\prod_{j=1}^{t_{\mathbb{II}'}} \mathrm{GR}(p^r, s\acute{e}_j)[P]\right) \times \left(\prod_{k=1}^{t_{\mathbb{III}'}} \left(\mathrm{GR}(p^r, s\acute{f}_k)[P] \times \mathrm{GR}(p^r, s\acute{f}_k)[P]\right)\right), \tag{H2}$$

and, by Lemma 2.1, every abelian code in $\mathrm{GR}(p^r,s)[G] \cong \mathcal{R}[P]$ can be viewed as

$$\mathcal{C} \cong \left(\prod_{j=1}^{t_{\mathbb{II}'}} E_j\right) \times \left(\prod_{k=1}^{t_{\mathbb{III}'}} (F_k \times F_k')\right), \tag{H3}$$

where E_j is an abelian code in $\mathrm{GR}(p^r, s\acute{e}_j)[P]$ and F_k, F_k' are abelian codes in $\mathrm{GR}(p^r, s\acute{f}_k)[P]$ for all $j=1,2,\ldots,t_{\mathbb{II}'}$ and $k=1,2,\ldots,t_{\mathbb{III}'}$.

Then the Hermitian dual of $\mathcal{C}$ in (H3) has the form

$$\mathcal{C}^{\perp_{\mathrm{H}}} \cong \left(\prod_{j=1}^{t_{\mathbb{II}'}} E_j^{\perp_{\mathrm{H}}}\right) \times \left(\prod_{k=1}^{t_{\mathbb{III}'}} \left((F_k')^{\perp_{\mathrm{E}}} \times F_k^{\perp_{\mathrm{E}}}\right)\right). \tag{H4}$$

The detailed discussion for (H4) is provided in Appendix A.2.

3. Self-dual abelian codes in $\mathrm{GR}(p^r, s)[G]$

In this section, we characterize and enumerate Euclidean and Hermitian self-dual abelian codes in $\mathrm{GR}(p^r, s)[G]$. We determine necessary and sufficient conditions for the existence of self-dual abelian codes in $\mathrm{GR}(p^r, s)[G]$ in Subsection 3.1 and followed by general results for the enumeration of such self-dual codes in Subsection 3.2. Some special cases will be discussed in Subsections 3.3 and 3.4.

3.1. The existence of self-dual abelian codes

The characterizations of Euclidean and Hermitian self-dual abelian codes in $\mathrm{GR}(p^r, s)[G]$ are given as follows.

From (E3) and (E4), the characterization of Euclidean self-dual abelian codes in $\mathrm{GR}(p^r, s)[G]$ is given in the next proposition.

Proposition 3.1. *Let r and s be positive integers and let p be a prime number. An abelian code $\mathcal{C}$ in $\mathrm{GR}(p^r, s)[G]$ is Euclidean self-dual if and only if, in the decomposition (E3),*

i) U_i is Euclidean self-dual for all $i = 1, 2, \ldots, t_{\mathrm{I}}$,

ii) V_j is Hermitian self-dual for all $j = 1, 2, \ldots, t_{\mathrm{II}}$, and

iii) $W'_k = W_k^{\perp_{\mathrm{E}}}$ for all $k = 1, 2, \ldots, t_{\mathrm{III}}$.

The characterization of Hermitian self-dual abelian codes in $\mathrm{GR}(p^r, s)[G]$ follows immediately from (H3) and (H4).

Proposition 3.2. *Let r and s be positive integers such that s is even and let p be a prime number. Then an abelian code $\mathcal{C}$ in $\mathrm{GR}(p^r, s)[G]$ is Hermitian self-dual if and only if, in the decomposition (H3),*

i) E_j is Hermitian self-dual for all $j = 1, 2, \ldots, t_{\mathrm{II}'}$, and

ii) $F'_k = F_k^{\perp_{\mathrm{E}}}$ for all $k = 1, 2, \ldots, t_{\mathrm{III}'}$.

Necessary and sufficient conditions for the existence of Euclidean and Hermitian self-dual abelian codes in $\mathrm{GR}(p^r, s)[G]$ are given as follows. The conditions for the Euclidean case have been proven in [26, Theorem 1.1]. Here, we provide an alternative constructive proof.

Proposition 3.3. *Let r and s be positive integers and let p be a prime number. Let G be a finite abelian group. Then there exists a Euclidean self-dual abelian code in $\mathrm{GR}(p^r, s)[G]$ if and only if one of the following statements holds,*

i) r is even, or

ii) $p = 2$ and $|G|$ is even.

In addition, if s is even, then the conditions are equivalent to the existence of a Hermitian self-dual abelian code in $\mathrm{GR}(p^r, s)[G]$.

Proof. Assume that G is decomposed as $G = A \oplus P$, where $p \nmid |A|$ and P is the Sylow p-subgroup of G of order p^a, where $a \geq 0$.

From (E3), assume that the code

$$\mathcal{C} \cong \left(\prod_{i=1}^{t_{\mathrm{I}}} U_i\right) \times \left(\prod_{j=1}^{t_{\mathrm{II}}} V_j\right) \times \left(\prod_{k=1}^{t_{\mathrm{III}}} (W_k \times W'_k)\right)$$

is Euclidean self-dual in $\mathrm{GR}(p^r,s)[G]$. Then, by Proposition 3.1, U_1 is Euclidean self-dual in $\mathrm{GR}(p^r,s)[P]$. It follows that $|U_1|=(p^s)^{rp^a/2}$ and $rp^a/2$ is an integer. Hence, r is even, or $p=2$ and $a\geq 1$.

For the converse, if r is even, then $p^{r/2}\mathrm{GR}(p^r,s)[G]$ is Euclidean self-dual. Assume that r is odd, $p=2$ and $|G|$ is even. Let $r'=\lceil\frac{r}{2}\rceil$. Then $|P|=2^a$ with $a\geq 1$ and $r=2r'-1$. Since the order of P is even, P contains an element x of order 2. Define

$$\begin{aligned}\mathcal{C}\cong&\left(\prod_{i=1}^{t_{\mathrm{I}}}\left(2^{r'}\mathrm{GR}(2^r,s)[P]+2^{r'-1}\mathrm{GR}(2^r,s)[P](Y^x+1)\right)\right)\\&\times\left(\prod_{j=1}^{r_{\mathrm{II}}}\left(2^{r'}\mathrm{GR}(2^r,2se_j)[P]+2^{r'-1}\mathrm{GR}(2^r,2se_j)[P](Y^x+1)\right)\right)\\&\times\left(\prod_{k=1}^{t_{\mathrm{III}}}(\mathrm{GR}(2^r,sf_k)[P]\times\{0\})\right).\end{aligned}$$

We prove that $\mathcal{C}$ is Euclidean self-dual. By Proposition 3.1, it is sufficient to show that

$$U:=2^{r'}\mathrm{GR}(2^r,s)[P]+2^{r'-1}\mathrm{GR}(2^r,s)[P](Y^x+1)$$

is Euclidean self-dual and

$$V_j:=2^{r'}\mathrm{GR}(2^r,2se_j)[P]+2^{r'-1}\mathrm{GR}(2^r,2se_j)[P](Y^x+1)$$

is Hermitian self-dual for all $j=1,2\ldots,t_{\mathrm{II}}$.

Let $\boldsymbol{u}=2^{r'}\boldsymbol{e}+2^{r'-1}\boldsymbol{e}'(Y^x+1)$ and $\boldsymbol{v}=2^{r'}\boldsymbol{f}+2^{r'-1}\boldsymbol{f}'(Y^x+1)$ be elements in U, where $\boldsymbol{e}$, $\boldsymbol{e}'$, $\boldsymbol{f}$, and $\boldsymbol{f}'$ are in $\mathrm{GR}(2^r,s)[P]$. Since $r=2r'-1$ and $x=-x$, we have

$$\begin{aligned}\langle\boldsymbol{u},\boldsymbol{v}\rangle_{\mathrm{E}}&=\langle 2^{r'}\boldsymbol{e},2^{r'}\boldsymbol{f}\rangle_{\mathrm{E}}+\langle 2^{r'}\boldsymbol{e},2^{r'-1}\boldsymbol{f}'(Y^x+1)\rangle_{\mathrm{E}}\\&\quad+\langle 2^{r'-1}\boldsymbol{e}'(Y^x+1),2^{r'}\boldsymbol{f}\rangle_{\mathrm{E}}+\langle 2^{r'-1}\boldsymbol{e}'(Y^x+1),2^{r'-1}\boldsymbol{f}'(Y^x+1)\rangle_{\mathrm{E}}\\&=2^{r-1}\langle\boldsymbol{e}'(Y^x+1),\boldsymbol{f}'(Y^x+1)\rangle_{\mathrm{E}}\\&=2^{r-1}\left(\langle\boldsymbol{e}'Y^x,\boldsymbol{f}'Y^x\rangle_{\mathrm{E}}+\langle\boldsymbol{e}'Y^x,\boldsymbol{f}'\rangle_{\mathrm{E}}+\langle\boldsymbol{e}',\boldsymbol{f}'Y^x\rangle_{\mathrm{E}}+\langle\boldsymbol{e}',\boldsymbol{f}'\rangle_{\mathrm{E}}\right)\\&=2^{r-1}\left(2\langle\boldsymbol{e}',\boldsymbol{f}'\rangle_{\mathrm{E}}+2\langle\boldsymbol{e}'Y^x,\boldsymbol{f}'\rangle_{\mathrm{E}}\right)\\&=0.\end{aligned}$$

It is not difficult to verify that

$$|U|=\frac{|2^{r'}\mathrm{GR}(2^r,s)[P]||2^{r'-1}\mathrm{GR}(2^r,s)[P](Y^x+1)|}{|(2^{r'}\mathrm{GR}(2^r,s)[P])\cap(2^{r'-1}\mathrm{GR}(2^r,s)[P](Y^x+1))|}=\frac{(2^s)^{(r'-1)2^a}(2^s)^{r'2^a/2}}{(2^s)^{(r'-1)2^a/2}}=(2^s)^{r2^{a-1}}.$$

Therefore, U is Euclidean self-dual.

Using arguments similar to the above, we can see that V_j is Hermitian self-dual for all $j=1,2\ldots,t_{\mathrm{II}}$.

For the Hermitian case, we assume that s is even. The proof of the sufficiency is similar to the Euclidean case, except that (H3) and Proposition 3.2 are applied instead of (E3) and Proposition 3.1 .

For the converse, if r is even, then $p^{r/2}\mathrm{GR}(p^r,s)[G]$ is Hermitian self-dual. Assume that r is odd, $p=2$ and $|G|$ is even. Then P contains an element x of order 2. Let $r'=\lceil\frac{r}{2}\rceil$ and define

$$\mathcal{C}\cong\left(\prod_{j=1}^{r_{\mathrm{II}'}}\left(2^{r'}\mathrm{GR}(2^r,s\acute{e}_j)[P]+2^{r'-1}\mathrm{GR}(2^r,s\acute{e}_j)[P](Y^x+1)\right)\right)\times\left(\prod_{k=1}^{t_{\mathrm{III}'}}\left(\mathrm{GR}(2^r,s\acute{f}_k)[P]\times\{0\}\right)\right).$$

By arguments similar to those in the proof of the Euclidean case, we can verity that $2^{r'}\mathrm{GR}(2^r,s\acute{e}_j)[P]+2^{r'-1}\mathrm{GR}(2^r,s\acute{e}_j)[P](Y^x+1)$ is Hermitian self-dual for all $j=1,2,\ldots,t_{\mathrm{II}'}$. Therefore, $\mathcal{C}$ is Hermitian self-dual by Proposition 3.2. □

3.2. Enumeration of self-dual abelian codes

We aim to characterize and enumerate Euclidean and Hermitian self-dual cyclic and abelian codes over Galois rings. For convenience, we fix the following notations.

- $NC(\mathrm{GR}(p^r,s),n)$ – the number of cyclic codes of length n over $\mathrm{GR}(p^r,s)$,
- $NEC(\mathrm{GR}(p^r,s),n)$ – the number of Euclidean self-dual cyclic codes of length n over $\mathrm{GR}(p^r,s)$,
- $NHC(\mathrm{GR}(p^r,s),n)$ – the number of Hermitian self-dual cyclic codes of length n over $\mathrm{GR}(p^r,s)$,
- $NA(\mathrm{GR}(p^r,s)[G])$ – the number of abelian codes in $\mathrm{GR}(p^r,s)[G]$,
- $NEA(\mathrm{GR}(p^r,s)[G])$ – the number of Euclidean self-dual abelian codes in $\mathrm{GR}(p^r,s)[G]$,
- $NHA(\mathrm{GR}(p^r,s)[G])$ – the number of Hermitian self-dual abelian codes in $\mathrm{GR}(p^r,s)[G]$,

where s is assumed to be even in cases of $NHC(\mathrm{GR}(p^r,s),n)$ and $NHA(\mathrm{GR}(p^r,s)[G])$.

To determine the numbers of Euclidean and Hermitian self-dual abelian codes, we need some group-theoretic and number-theoretic results. For completeness, we recall the following results.

For a finite group A and a positive integer d, let $\mathcal{N}_A(d)$ denote the number of elements in A of order d. The explicit expression of $\mathcal{N}_A(d)$ is completely determined in [2].

Let q be a prime power and let j be a positive integer. The pair (j,q) is said to be *oddly good* if j divides q^t+1 for some odd integer $t\geq 1$, and *evenly good* if j divides q^t+1 for some even integer $t\geq 2$. It is said to be *good* if it is oddly good or evenly good, and *bad* otherwise. The characterization of good and oddly-good pairs of integers can be found in [12], [11], [13], [15], and [20].

Let χ and λ be functions defined on the pair (j,q), where j is a positive integer, as follows.

$$\chi(j,q)=\begin{cases}0 & \text{if } (j,q) \text{ is good,}\\ 1 & \text{otherwise,}\end{cases} \tag{4}$$

and

$$\lambda(j,q)=\begin{cases}0 & \text{if } (j,q) \text{ is oddly good,}\\ 1 & \text{otherwise.}\end{cases} \tag{5}$$

The following two lemmas are extended from the case where q is a power of 2 in [13] and [15] and the proof is omitted. The readers may refer to [13, Lemma 4.5] and [15, Lemma 7] for the idea of the proofs.

Lemma 3.4. *Let s be a positive integer and let p be a prime number. Let A be a finite abelian group such that $\gcd(|A|,p)=1$ and let $h\in A$. Then $S_{p^s}(h)$ is of type $\mathbb{III}$ if and only if $(\mathrm{ord}(h),p^s)$ is bad.*

Lemma 3.5. *Let s be an even positive integer and let p be a prime number. Let A be a finite abelian group such that $\gcd(|A|,p)=1$ and let $h\in A\setminus\{0\}$. Then $S_{p^s}(h)$ is of type $\mathbb{III}'$ if and only if $(\mathrm{ord}(h),p^{s/2})$ is evenly good or bad.*

Utilizing the decomposition in Section 2 and the discussion above, we obtain the following formulas for the numbers of Euclidean and Hermitian self-dual abelian codes in $\mathrm{GR}(p^r,s)[G]$, where G is an arbitrary finite abelian group. Without loss of generality, we assume that $G=A\oplus P$, where P is a finite abelian p-group and A is a finite abelian group such that $p\nmid|A|$.

Theorem 3.6. *Let p be a prime and let s,r be integers such that $1\leq s$ and $1\leq r$. Let A be a finite abelian group of exponent M such that $p\nmid M$ and let P be a finite abelian p-group. Then*

$$\begin{aligned}NEA(\mathrm{GR}(p^r,s)[A\oplus P]) &= (NEA(\mathrm{GR}(p^r,s)[P]))^{\sum_{d|M,\mathrm{ord}_d(p^s)=1}(1-\chi(d,p^s))\mathcal{N}_A(d)}\\ &\times\prod_{\substack{d|M\\ \mathrm{ord}_d(p^s)\neq 1}}(NHA(\mathrm{GR}(p^r,s\cdot\mathrm{ord}_d(p^s))[P]))^{(1-\chi(d,p^s))\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^s)}}\\ &\times\prod_{d|M}(NA(\mathrm{GR}(p^r,s\cdot\mathrm{ord}_d(p^s))[P]))^{\chi(d,p^s)\frac{\mathcal{N}_A(d)}{2\mathrm{ord}_d(p^s)}}.\end{aligned}$$

In addition, if s is even, then

$$NHA(\mathrm{GR}(p^r,s)[A\oplus P]) = \prod_{d|M} (NHA(\mathrm{GR}(p^r,s\cdot \mathrm{ord}_d(p^s))[P]))^{(1-\lambda(d,p^{\frac{s}{2}}))\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^s)}} \times \prod_{d|M} (NA(\mathrm{GR}(p^r,s\cdot \mathrm{ord}_d(p^s))[P]))^{\lambda(d,p^{\frac{s}{2}})\frac{\mathcal{N}_A(d)}{2\mathrm{ord}_d(p^s)}}.$$

Proof. First, we consider the Euclidean case. From (E3) and Proposition 3.1, it is sufficient to count the numbers of Euclidean self-dual abelian codes U_i's, the numbers of Hermitian self-dual abelian codes V_i's, and the numbers of abelian codes W_i's which correspond to the p^s-cyclotomic classes of types I, II, and III, respectively.

From [14, Remark 2.5], we note that the elements in A of the same order are partitioned into p^s-cyclotomic classes of the same type. For each divisor d of M, a p^s-cyclotomic class containing an element of order d has cardinality $\mathrm{ord}_d(p^s)$, and hence, the number of such p^s-cyclotomic classes is $\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^s)}$.

For each divisor d of M, we consider the following 3 cases.

Case 1. $\chi(d,p^s)=0$ and $\mathrm{ord}_d(p^s)=1$. By Lemma 3.4, every p^s-cyclotomic class of A containing an element of order d is of type I. Since there are $\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^s)}$ such p^s-cyclotomic classes, the number of Euclidean self-dual abelian codes U_i's corresponding to d is

$$(NEA(\mathrm{GR}(p^r,s\cdot \mathrm{ord}_d(p^s))[P]))^{\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^s)}} = (NEA(\mathrm{GR}(p^r,s)[P]))^{(1-\chi(d,p^s))\mathcal{N}_A(d)}.$$

Case 2. $\chi(d,p^s)=0$ and $\mathrm{ord}_d(p^s)\neq 1$. By Lemma 3.4, every p^s-cyclotomic class of A containing an element of order d is of type II. Since there are $\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^s)}$ such p^s-cyclotomic classes, the number of Hermitian self-dual abelian codes V_i's corresponding to d is

$$(NHA(\mathrm{GR}(p^r,s\cdot \mathrm{ord}_d(p^s))[P]))^{\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^s)}} = (NHA(\mathrm{GR}(p^r,s\cdot \mathrm{ord}_d(p^s))[P]))^{(1-\chi(d,p^s))\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^s)}}.$$

Case 3. $\chi(d,p^s)=1$. By Lemma 3.4, every p^s-cyclotomic class of A containing an element of order d is of type III. Since there are $\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^s)}$ such p^s-cyclotomic classes, the number of abelian codes W_i's corresponding to d is

$$(NA(\mathrm{GR}(p^r,s\cdot \mathrm{ord}_d(p^s))[P]))^{\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^s)}} (NA(\mathrm{GR}(p^r,s\cdot \mathrm{ord}_d(p^s))[P]))^{\chi(d,p^s)\frac{\mathcal{N}_A(d)}{2\mathrm{ord}_d(p^s)}}.$$

Since d runs over all divisors of M, we conclude the desired result.

For the Hermitian case, by Proposition 3.2, it suffices to count the numbers of Hermitian self-dual abelian codes E_i's and the numbers of abelian codes F_i's in (H3) which correspond to the p^s-cyclotomic classes of types II′ and III′, respectively. Considering the cases where $\lambda(d,p^{\frac{s}{2}})=1$ and where $\lambda(d,p^{\frac{s}{2}})=0$, the desired result can be obtained similarly to the Euclidean case, where Lemma 3.5 is applied instead of Lemma 3.4. □

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

In Theorem 3.6, if P is cyclic of order p^a, then the values NA, NEA and NHA may be replaced by NC, NEC, and NHC, respectively. In general, these values are not known in the literature. Some special cases where *i)* $\gcd(p,|G|)=1$; and *ii)* $r=2$ and the Sylow p-subgroup of G is cyclic are discussed in the following subsections.

3.3. Self-dual abelian codes in $\mathrm{GR}(p^r, s)[A]$, $\gcd(p, |A|) = 1$

In this subsection, we complete the enumeration of Euclidean and Hermitian self-dual abelian codes in $\mathrm{GR}(p^r, s)[A]$, where $\gcd(p, |A|) = 1$, or equivalently, $\mathrm{GR}(p^r, s)[A]$ is a principal ideal group ring (see Proposition 3.7). If A is cyclic, this case is identical with that of simple root cyclic codes.

Proposition 3.7. *Let p be a prime number and let r, s be positive integers. Let G be a finite abelian group. Then one of the following statements holds.*

i) If $r = 1$, then $\mathrm{GR}(p^r, s)[G] \cong \mathbb{F}_{p^s}[G]$ is a principal ideal ring if and only if the Sylow p-subgroup of G is cyclic.

ii) If $r \geq 2$, then $\mathrm{GR}(p^r, s)[G]$ is a principal ideal ring if and only if $\gcd(p, |G|) = 1$.

For $r = 1$, the statement has been proven in [9]. For $r \geq 2$, using notion of morphic rings (see the definition in [6]), it has been shown that $\mathbb{Z}_{p^r}[G]$ is principal ideal if and only if $\gcd(p, |G|) = 1$ (see [8, Theorem 1.2] and [6, Theorem 3.12 and Corollary 3.13]). The statements can be extended naturally to the case of $\mathrm{GR}(p^r, s)[G]$.

The enumerations of Euclidean and Hermitian self-dual abelian codes in a principal ideal group ring $\mathrm{GR}(p^r, s)[A]$ is given as follows.

Theorem 3.8. *Let p be a prime and let s, r be positive integers. Let A be a finite abelian group of exponent M such that $\gcd(p, |A|) = 1$. Then*

$$NEA(\mathrm{GR}(p^r, s)[A]) = \begin{cases} (1+r)^{\sum_{d|M} \chi(d, p^s) \frac{\mathcal{N}_A(d)}{2\mathrm{ord}_d(p^s)}} & \text{if } r \text{ is even,} \\ 0 & \text{if } r \text{ is odd.} \end{cases}$$

In addition, if s is even, then

$$NHA(\mathrm{GR}(p^r, s)[A]) = \begin{cases} (1+r)^{\sum_{d|M} \lambda(d, p^{s/2}) \frac{\mathcal{N}_A(d)}{2\mathrm{ord}_d(p^s)}} & \text{if } r \text{ is even,} \\ 0 & \text{if } r \text{ is odd.} \end{cases}$$

Proof. In $\mathrm{GR}(p^r, s)$, every ideal can be regarded as an abelian code in $\mathrm{GR}(p^r, s)[G]$ with $G = \{0\}$, and we have the following facts.

i) The number of abelian codes in $\mathrm{GR}(p^r, s)$ is $r + 1$.

ii) If r is odd, then there are neither Euclidean self-dual abelian codes nor Hermitian self-dual abelian codes in $\mathrm{GR}(p^r, s)$.

iii) If r is even, then $r^{r/2}\mathrm{GR}(p^r, s)$ is the only Euclidean self-dual abelian code and it is the only Hermitian self-dual abelian code if s is even.

The above results hold true for any Galois extension of $\mathrm{GR}(p^r, s)$.

By considering $P = \{0\}$ in Theorem 3.6, the result follows immediately. □

Note that, if A is cyclic, M and $\mathcal{N}_A(d)$ can be replaced by the cardinality of A and $\phi(d)$, respectively, where ϕ is the Euler's totient function.

If A is cyclic of order n with $\gcd(n, p) = 1$, then the number of Euclidean self-dual cyclic codes of length n over $\mathrm{GR}(p^r, s)$ obtained in Theorem 3.8 is a special case of [1, Theorem 5.7] by viewing $\mathrm{GR}(p^r, s)$ as a finite chain ring of depth r.

3.4. Self-dual abelian codes in $\mathrm{GR}(p^2,s)[A\oplus C_{p^a}]$

In this section, we restrict our study to the case where $r=2$ and $P=C_{p^a}$, a cyclic group of order p^a. The enumerations of Euclidean and Hermitian self-dual abelian codes in $\mathrm{GR}(p^2,s)[A\oplus C_{p^a}]$ can be obtained as an application of Theorem 3.6 and some known results on cyclic codes of length p^a over $\mathrm{GR}(p^2,s)$.

We recall some results on cyclic codes of length p^a over $\mathrm{GR}(p^2,s)$. The next lemma follows immediately from [16, Corollary 3.9] and [16, Theorem 3.6].

Lemma 3.9. *The number of cyclic codes of length p^a over $\mathrm{GR}(p^2,s)$ is*

$$NC(\mathrm{GR}(p^2,s),p^a)=2\sum_{d=0}^{p^a-1}\frac{p^{s(\min\{\lfloor\frac{d}{2}\rfloor,p^{a-1}\}+1)}-1}{p^s-1}+\frac{p^{s(p^{a-1}+1)}-1}{p^s-1}. \tag{6}$$

Proposition 3.10 ([17, Corollary 3.5])**.** *The number of Euclidean self-dual cyclic codes of length 2^a over $\mathrm{GR}(2^2,s)$ is*

$$NEC(\mathrm{GR}(2^2,s),2^a)=\begin{cases}1 & \text{if } a=1,\\ 1+2^s & \text{if } a=2,\\ 1+2^s+2^{2s+1}\left(\frac{(2^s)^{(2^{a-2}-1)}-1}{2^s-1}\right) & \text{if } a\geq 3.\end{cases}$$

If p is an odd prime, then the number of Euclidean self-dual cyclic codes of length p^a over $\mathrm{GR}(p^2,s)$ is

$$NEC(\mathrm{GR}(p^2,s),p^a)=2\left(\frac{(p^s)^{(p^{a-1}+1)}/2-1}{p^s-1}\right).$$

Proposition 3.11 ([14, Theorem 3.5])**.** *Let p be a prime and let s,a be positive integers such that s is even. Then the number of Hermitian self-dual cyclic codes of length p^a over $\mathrm{GR}(p^2,s)$ is*

$$NHC(\mathrm{GR}(p^2,s),p^a)=\sum_{i_1=0}^{p^{a-1}}p^{si_1/2}=\frac{p^{s(p^{a-1}+1)/2}-1}{p^{s/2}-1}.$$

Remark 3.12. *For cyclic codes of length p^a over $\mathrm{GR}(p^2,s)$, the numbers NC, NEC, and NHC have already been determined in Lemma 3.9, Proposition 3.10, and Proposition 3.11, respectively. Combining these results and Theorem 3.6, the numbers $NEA(\mathrm{GR}(p^2,s)[A\oplus C_{p^a}])$ and $NHA(\mathrm{GR}(p^2,s)[A\oplus C_{p^a}])$ are explicitly determined.*

The numbers of Euclidean and Hermitian self-dual cyclic codes of arbitrary length n over $\mathrm{GR}(p^2,s)$ can be obtained as a corollary of Remark 3.12. Some parts of the formulas can be simplified as in the next corollary.

Corollary 3.13. *Let p be a prime and let s,n be positive integers. Write $n=mp^a$, where $a\geq 0$ and $p\nmid m$. Then*

$$\begin{aligned}NEC(\mathrm{GR}(p^2,s),n)=&\left(NEC(\mathrm{GR}(p^2,s),p^a)\right)^{\eta(m)}\\ &\times\prod_{\substack{d\mid m\\ d\notin\{1,2\}}}\left(NHC(\mathrm{GR}(p^2,s\cdot\mathrm{ord}_d(p^s)),p^a)\right)^{(1-\chi(d,p^s))\frac{\phi(d)}{\mathrm{ord}_d(p^s)}}\\ &\times\prod_{d\mid m}\left(NC(\mathrm{GR}(p^2,s\cdot\mathrm{ord}_d(p^s)),p^a)\right)^{\chi(d,p^s)\frac{\phi(d)}{2\mathrm{ord}_d(p^s)}},\end{aligned}$$

where

$$\eta(m) = \begin{cases} 1 & \text{if } m \text{ is odd,} \\ 2 & \text{if } m \text{ is even.} \end{cases}$$

In addition, if s is even, then

$$NHC(\mathrm{GR}(p^2,s),n) = \prod_{d|m} \left(NHC(\mathrm{GR}(p^2, s\cdot \mathrm{ord}_d(p^s)), p^a)\right)^{(1-\lambda(d,p^{\frac{s}{2}}))\frac{\phi(d)}{\mathrm{ord}_d(p^s)}} \times \prod_{d|m} \left(NC(\mathrm{GR}(p^2, s\cdot \mathrm{ord}_d(p^s)), p^a)\right)^{\lambda(d,p^{\frac{s}{2}})\frac{\phi(d)}{2\mathrm{ord}_d(p^s)}}.$$

Proof. Setting $r = 2$ and A a cyclic group of order m in Theorem 3.6, the exponent of A is m and $\mathcal{N}_A(d)$ is just $\phi(d)$, where ϕ is the Euler's function.

Note that $S_{p^s}(0)$ is the only p^s-cyclotomic class of A of type I if m is odd, and $S_{p^s}(0)$ and $S_{p^s}(\frac{m}{2})$ are the only p^s-cyclotomic classes of A of type I if m is even. Therefore, the values of $\eta(m)$ follows. □

4. Complementary dual abelian codes in $\mathrm{GR}(p^r,s)[G]$

In this section, the characterization and enumeration of complementary dual abelian codes in the group ring $\mathrm{GR}(p^r,s)[G]$ are given based on the decomposition in Section 2 and the theory of local group rings.

4.1. Characterization and enumeration of complementary dual abelian codes in $\mathrm{GR}(p^r,s)[P]$

In this subsection, we focus on complementary dual abelian codes and direct summand ideals in each component of $\mathrm{GR}(p^r,s)[P]$ in the decompositions (E1) and (H1), where P is a finite abelian p-group.

First, we recall some useful definitions and properties in ring theory. For a finite commutative ring R with identity, the *Jacobson radical* of R, denoted by $Jac(R)$, is defined to be the intersection of all maximal ideals of R. The ring R is said to be *local* if it has a unique maximal ideal.

A local group ring has been characterized in the following lemma.

Lemma 4.1 ([22, Theorem]). *Let R be a commutative ring with identity and let G be a finite abelian group. Then $R[G]$ is local if and only if R is local, G is a p-group and $p \in Jac(R)$.*

Proposition 4.2. *Let p be a prime number and let r,s be positive integers. Let P be a finite abelian p-group. Then $\mathrm{GR}(p^r,s)[P]$ is a local group ring.*

Proof. Since the ideal $\langle p\rangle$ is the unique maximal ideal of $\mathrm{GR}(p^r,s)$, the ring $\mathrm{GR}(p^r,s)$ is local. Moreover, $p \in \langle p\rangle = Jac(\mathrm{GR}(p^r,s)$. By Lemma 4.1, $\mathrm{GR}(p^r,s)[P]$ is a local group ring. □

By Proposition 4.2, $\mathrm{GR}(p^r,s)[P]$ is local. Denote by M the maximal ideal of $\mathrm{GR}(p^r,s)[P]$. The characterizations of the Euclidean and Hermitian complementary dual abelian codes and the direct summands in a local group ring $\mathrm{GR}(p^r,s)[P]$ are given in the following theorems.

Theorem 4.3. *Let p be a prime number and let r,s be positive integers. Let P be a finite abelian p-group. Then $\{0\}$ and $\mathrm{GR}(p^r,s)[P]$ are the only Euclidean complementary dual abelian codes in $\mathrm{GR}(p^r,s)[P]$.*

Proof. Clearly, $\{0\}$ and $\mathrm{GR}(p^r,s)[P]$ are Euclidean complementary dual abelian codes in $\mathrm{GR}(p^r,s)[P]$. Let $\mathcal{C}$ be an abelian code in $\mathrm{GR}(p^r,s)[P]$ such that $\{0\}\subsetneq\mathcal{C}\subsetneq\mathrm{GR}(p^r,s)[P]$. Then $\mathcal{C}\subseteq M$. It follows that $M^{\perp_{\mathrm{E}}}\subseteq\mathcal{C}^{\perp_{\mathrm{E}}}\subseteq M$ which implies $M^{\perp_{\mathrm{E}}}\subseteq\mathcal{C}\subseteq M$. Hence, $\{0\}\neq M^{\perp_{\mathrm{E}}}\subseteq\mathcal{C}\cap\mathcal{C}^{\perp_{\mathrm{E}}}\subseteq M$. Consequently, $\mathcal{C}$ is not Euclidean complementary dual. Therefore, the ideals $\{0\}$ and $\mathrm{GR}(p^r,s)[P]$ are the only Euclidean complementary dual abelian codes in $\mathrm{GR}(p^r,s)[P]$. □

It is not difficult to see that the proof of Theorem 4.3 is independent of the inner product. Hence, we have the following corollary.

Corollary 4.4. *Let p be a prime number and let r,s be positive integers such that s is even. Let P be a finite abelian p-group. Then $\{0\}$ and $\mathrm{GR}(p^r,s)[P]$ are the only Hermitian complementary dual abelian codes in $\mathrm{GR}(p^r,s)[P]$.*

Theorem 4.5. *Let p be a prime number and let r,s be positive integers. Let P be a finite abelian p-group. Then ideals $\{0\}$ and $\mathrm{GR}(p^r,s)[P]$ are the only direct summands in $\mathrm{GR}(p^r,s)[P]$.*

Proof. Clearly, $\{0\}$ and $\mathrm{GR}(p^r,s)[P]$ are direct summands in $\mathrm{GR}(p^r,s)[P]$. Let $\{0\}\subsetneq\mathcal{C}\subsetneq\mathrm{GR}(p^r,s)[P]$ be an ideal in $\mathrm{GR}(p^r,s)[P]$. Suppose that $\mathcal{C}$ is a direct summand. Then there exists an ideal $\mathcal{C}'$ in $\mathrm{GR}(p^r,s)[P]$ such that $\mathcal{C}\cap\mathcal{C}'=\{0\}$ and $\mathcal{C}+\mathcal{C}'=\mathrm{GR}(p^r,s)[P]$. Since M is the maximal ideal in $\mathrm{GR}(p^r,s)[P]$, we have $\mathcal{C}\subseteq M$ and $\mathcal{C}'\subseteq M$. Hence, $\mathcal{C}+\mathcal{C}'\subseteq M\subsetneq\mathrm{GR}(p^r,s)[P]$, a contradiction. Therefore, the ideals $\{0\}$ and $\mathrm{GR}(p^r,s)[P]$ are the only direct summands in $\mathrm{GR}(p^r,s)[P]$. □

The above results can be summarized as follows.

Corollary 4.6. *Let p be a prime number and let r,s be positive integers. Let P be a finite abelian p-group. Then the following statements hold.*

1. *The number of Euclidean complementary dual abelian codes in $\mathrm{GR}(p^r,s)[P]$ is 2.*
2. *If s is even, the number of Hermitian complementary dual abelian codes in $\mathrm{GR}(p^r,s)[P]$ is 2.*
3. *The number of direct summand ideals in $\mathrm{GR}(p^r,s)[P]$ is 2.*

4.2. Characterization and enumeration of complementary dual abelian codes in $\mathrm{GR}(p^r,s)[G]$

In this subsection, we focus on the characterization and enumeration of complementary dual abelian codes in $\mathrm{GR}(p^r,s)[G]$, where G is an arbitrary finite abelian group. Using the decompositions in Section 2 and results in the previous subsection, the characterization and enumeration of such complementary dual codes are given independent of r and the Sylow p-subgroup of G.

Recall that $G\cong A\times P$, where P is the Sylow p-subgroup of G and A is its complement subgroup. The group ring $\mathrm{GR}(p^r,s)[G]$ is viewed as $\mathrm{GR}(p^r,s)[G]\cong\mathcal{R}[P]$, where $\mathcal{R}=\mathrm{GR}(p^r,s)[A]$. Using the decomposition of $\mathrm{GR}(p^r,s)[G]$ in (E2), the characterization of a Euclidean complementary dual abelian code in $\mathrm{GR}(p^r,s)[G]$ can be concluded via (E3) and (E4) as follows.

Proposition 4.7. *Let p be a prime number and let r,s be positive integers. Let A be finite abelian group such that $p\nmid|A|$ and let P be a finite abelian p-group. Then an abelian code $\mathcal{C}$ in $\mathrm{GR}(p^r,s)[A\times P]$ decomposed as in (E3) is Euclidean complementary dual if and only if the following statements hold.*

1. *U_i is Euclidean complementary dual for all $i=1,2,\ldots,r_{\mathrm{I}}$.*
2. *V_j is Hermitian complementary dual for all $j=1,2,\ldots,r_{\mathrm{II}}$.*
3. *$W_k\cap(W_k')^{\perp_{\mathrm{E}}}=\{0\}$ and $W_k'\cap W_k^{\perp_{\mathrm{E}}}=\{0\}$ for all $k=1,2,\ldots,r_{\mathrm{III}}$.*

The next corollary follows immediately from Theorem 4.3, Proposition 4.7, and Corollary 4.4.

Corollary 4.8. *Let p be a prime number and let r, s be positive integers. Let A be finite abelian group such that $p \nmid |A|$ and let P be a finite abelian p-group. Then an abelian code C in $\mathrm{GR}(p^r, s)[A \times P]$ decomposed as in (E3) is Euclidean complementary dual if and only if the following statements hold.*

1. $U_i \in \{\{0\}, \mathrm{GR}(p^r, s)[P]\}$ *for all* $i = 1, 2, \ldots, r_{\mathrm{I}}$.
2. $V_j \in \{\{0\}, \mathrm{GR}(p^r, 2se_j)[P]\}$ *for all* $j = 1, 2, \ldots, r_{\mathrm{II}}$.
3. $(W_k, W_k') \in \{(\{0\}, \{0\}), (\mathrm{GR}(p^r, sf_k)[P], \mathrm{GR}(p^r, sf_k)[P])\}$ *for all* $k = 1, 2, \ldots, r_{\mathrm{III}}$.

From Corollary 4.8, it is not difficult to see that the number of Euclidean complementary dual abelian codes in $\mathrm{GR}(p^r, s)[A \times P]$ is independent of r and the group P and it can be determined in the following corollary.

Corollary 4.9. *Let p be a prime number and let r, s be positive integers. Let A be finite abelian group such that $p \nmid |A|$ and let P be a finite abelian p-group. If the exponent of A is M and $\mathrm{GR}(p^r, s)[A \times P]$ is decomposed as in (E2), then the number of Euclidean complementary dual abelian codes in $\mathrm{GR}(p^r, s)[A \times P]$ is*

$$2^{r_{\mathrm{I}}+r_{\mathrm{II}}+r_{\mathrm{III}}} = 2^{\sum_{d|M}(1-\chi(d,p^s))\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^s)}+\sum_{d|M}\chi(d,p^s)\frac{\mathcal{N}_A(d)}{2\mathrm{ord}_d(p^s)}},$$

where $\mathcal{N}_A(d)$ denote the number of elements in A of order d.

Proof. The first part follows from Corollary 4.8. The equality can be derived similar to the proof of Theorem 3.6. □

Using the decomposition of $\mathrm{GR}(p^r, s)[G]$ in (H2), the characterization of a Hermitian complementary dual abelian code in $\mathrm{GR}(p^r, s)[G]$ can be concluded via (H3) and (H4) in the following proposition.

Proposition 4.10. *Let p be a prime number and let r, s be positive integers such that s is even. Let A be finite abelian group such that $p \nmid |A|$ and let P be a finite abelian p-group. Then an abelian code $\mathcal{C}$ in $\mathrm{GR}(p^r, s)[A \times P]$ decomposed as in (H3) is Hermitian complementary dual if and only if the following statements hold.*

1. E_j *is Hermitian complementary dual for all* $j = 1, 2, \ldots, r'_{\mathrm{II}}$.
2. $F_k \cap (F_k')^{\perp_{\mathrm{E}}} = \{0\}$ *and* $F_k' \cap F_k^{\perp_{\mathrm{E}}} = \{0\}$ *for all* $j = 1, 2, \ldots, r_{\mathrm{III}'}$.

The following result follows directly from Proposition 4.10 and Corollary 4.4.

Corollary 4.11. *Let p be a prime number and let r, s be positive integers such that s is even. Let A be finite abelian group such that $p \nmid |A|$ and let P be a finite abelian p-group. Then an abelian code $\mathcal{C}$ in $\mathrm{GR}(p^r, s)[A \times P]$ decomposed as in (H3) is Hermitian complementary dual if and only if the following statements hold.*

1. $E_j \in \{\{0\}, \mathrm{GR}(p^r, s\acute{e}_j)[P]\}$ *for all* $j = 1, 2, \ldots, r'_{\mathrm{II}}$.
2. $(F_k, F_k') \in \{(\{0\}, \{0\}), (\mathrm{GR}(p^r, s\acute{f}_k)[P], \mathrm{GR}(p^r, s\acute{f}_k)[P])\}$ *for all* $k = 1, 2, \ldots, r_{\mathrm{III}'}$.

From Corollary 4.11, the number of Hermitian complementary dual abelian codes in $\mathrm{GR}(p^r, s)[A \times P]$ is independent of r and the group P and it is given in the following corollary.

Corollary 4.12. *Let p be a prime number and let r, s be positive integers such that s is even. Let A be finite abelian group such that $p \nmid |A|$ and let P be a finite abelian p-group. If the exponent of A is M and $\mathrm{GR}(p^r, s)[A \times P]$ is decomposed as in (H2), then the number of Hermitian complementary dual abelian codes in $\mathrm{GR}(p^r, s)[A \times P]$ is*

$$2^{r_{\mathrm{I}'}+r_{\mathrm{II}'}} = 2^{\sum_{d|M} (1-\lambda(d,p^{\frac{s}{2}}))\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^s)} + \sum_{d|M} \lambda(d,p^{\frac{s}{2}})\frac{\mathcal{N}_A(d)}{2\mathrm{ord}_d(p^s)}},$$

where $\mathcal{N}_A(d)$ denote the number of elements in A of order d.

Proof. The first part follows from Corollary 4.11. The equality can be derived similar to the proof of Theorem 3.6. □

5. Conclusion

Self-dual and complementary dual abelian codes in $\mathrm{GR}(p^r, s)[G]$, a group ring of a finite abelian group G over a Galois ring $\mathrm{GR}(p^r, s)$, have been studied with respect to the Euclidean and Hermitian inner products. We have characterized such self-dual codes as well as determined necessary and sufficient conditions for $\mathrm{GR}(p^r, s)[G]$ to contain a Euclidean (resp, Hermitian) self-dual abelian code. For any finite abelian group G and Galois ring $\mathrm{GR}(p^r, s)$, the enumerations of such self-dual codes have been given. In the case where $\gcd(|G|, p) = 1$, the enumeration has been completed by restricting the Sylow p-subgroup to be $\{0\}$. Applying some known results on cyclic codes of length p^a over $\mathrm{GR}(p^2, s)$, we have determined explicitly the numbers of Euclidean and Hermitian self-dual abelian codes in $\mathrm{GR}(p^2, s)[G]$ if the Sylow p-subgroup of G is cyclic. As corollaries, analogous results on Euclidean and Hermitian self-dual cyclic codes over $\mathrm{GR}(p^r, s)$ have been concluded. Subsequently, the characterization and enumeration of complementary dual abelian codes in $\mathrm{GR}(p^r, s)[G]$ have been given. The number of complementary dual abelian codes in $\mathrm{GR}(p^r, s)[G]$ has been shown to be independent of r and the Sylow p-subgroup of G.

It would be interesting to study the unknown terms in Theorem 3.6 and extend the results to abelian codes over finite chain rings or the case where the Sylow p-subgroup of the group is not cyclic.

Appendix A

In this appendix, we discuss the Euclidean and Hermitian duals of abelian codes in $\mathrm{GR}(p^r, s)[G]$. First, we recall that $G \cong A \times P$, where P is the Sylow p-subgroup of G and A is a complementary subgroup of P in G. The group ring $\mathcal{R} := \mathrm{GR}(p^r, s)[A]$ is decomposed as in (E1) or (H1), and $\mathrm{GR}(p^r, s)[G] \cong \mathcal{R}[P]$.

A.1. Euclidean duality

Let ψ denote the isomorphism in (E1). For each element $\boldsymbol{x} \in \mathcal{R}$, we can write

$$\psi(\boldsymbol{x}) = (x_1, \ldots, x_{r_{\mathrm{I}}}, y_1, \ldots, y_{r_{\mathrm{II}}}, z_1, z'_1, \ldots, z_{r_{\mathrm{III}}}, z'_{r_{\mathrm{III}}}), \tag{7}$$

where $x_i \in \mathrm{GR}(p^r, s)$, $y_j \in \mathrm{GR}(p^r, 2se_j)$, and $z_k, z'_k \in \mathrm{GR}(p^r, sf_k)$ for all $i = 1, 2, \ldots, r_{\mathrm{I}}$, $j = 1, 2, \ldots, r_{\mathrm{II}}$, and $k = 1, 2, \ldots, r_{\mathrm{III}}$.

We are going to view $\widehat{\boldsymbol{x}}$ defined in Section 2 in terms of (7). We note that, for $\boldsymbol{c} = \sum_{a\in A} c_a Y^a \in \mathrm{GR}(p^2, s)[A]$, we have

$$\widehat{\boldsymbol{c}} = \sum_{a\in A} c_a Y^{-a} = \sum_{a\in A} c_{-a} Y^a.$$

Then $\breve{\widehat{\boldsymbol{c}}} = \sum_{a\in A} \breve{d}_a Y^a$, where

$$\breve{d}_a = \sum_{h\in A} c_{-h}\zeta^{\gamma_a(h)}.$$

From (3), we can see that, if $S_{p^s}(h)$ is of type I, then

$$\breve{d}_h = \breve{c}_h, \tag{8}$$

and if $S_{p^s}(h)$ is of type $\mathbb{I}\!\mathbb{I}$ with cardinality 2ν, then $-h = p^{s\nu}\cdot h$ by Remark 2.4. It follows that

$$\breve{d}_h = \sum_{a\in A} c_{-a}\zeta^{\gamma_h(a)} = \sum_{a\in A} c_a\zeta^{\gamma_{-h}(a)} = \sum_{a\in A} c_a\zeta^{\gamma_{p^{s\nu}\cdot h}(a)} = \sum_{a\in A} c_a\left(\zeta^{\gamma_h(a)}\right)^{p^{s\nu}} = \theta(\breve{c}_h), \tag{9}$$

where $\theta(\alpha) = \alpha_0^{p^{s\nu}} + \alpha_1^{p^{s\nu}}p + \cdots + \alpha_{r-1}^{p^{s\nu}}p^{r-1}$ for all $\alpha = \alpha_0 + \alpha_1 p + \cdots + \alpha_{r-1}p^{r-1}$.

Therefore, by the isomorphism ψ (see also [18]), the following properties are obtained.

1. From (8), the involution $\breve{\ }\,\widehat{\ }$ induces the identity automorphism on $\mathrm{GR}(p^r, s)$.
2. From (9), the involution $\breve{\ }\,\widehat{\ }$ induces the ring automorphism $\bar{\ }$ on $\mathrm{GR}(p^r, 2se_j)$ as defined in (1), *i.e.*,

$$\overline{\alpha} = \alpha_0^{p^{se_j}} + \alpha_1^{p^{se_j}}p + \cdots + \alpha_{r-1}^{p^{se_j}}p^{r-1}$$

for all $\alpha = \alpha_0 + \alpha_1 p + \cdots + \alpha_{r-1}p^{r-1}$ in $\mathrm{GR}(p^r, 2se_j)$, where $\alpha_i \in \mathcal{T}_{2se_j}$ for all $i = 0, 1, \ldots, r-1$.

3. For each pair $(z, z') \in \mathrm{GR}(p^r, sf_k)\times \mathrm{GR}(p^r, sf_k)$, we have

$$\widehat{\psi^{-1}(z, z')} = \psi^{-1}(z', z).$$

From the discussion, we have

$$\psi(\widehat{\boldsymbol{x}}) = (x_1, \ldots, x_{r_{\mathrm{I}}}, \overline{y_1}, \ldots, \overline{y_{r_{\mathrm{II}}}}, z'_1, z_1, \ldots, z'_{r_{\mathrm{III}}}, z_{r_{\mathrm{III}}}),$$

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

Proposition A.1. *Let $\boldsymbol{x} = \sum_{b\in P}\boldsymbol{x}_b Y^b$ and $\boldsymbol{u} = \sum_{b\in P}\boldsymbol{u}_b Y^b$ be elements in $\mathcal{R}[P]$. Decomposing $\boldsymbol{x}_b, \boldsymbol{u}_b$ using (7), we have*

$$\psi(\boldsymbol{x}_b) = (x_{b,1}, \ldots, x_{b,r_{\mathrm{I}}}, y_{b,1}, \ldots, y_{b,r_{\mathrm{II}}}, z_{b,1}, z'_{b,1}, \ldots, z_{b,r_{\mathrm{III}}}, z'_{b,r_{\mathrm{III}}})$$

and

$$\psi(\boldsymbol{u}_b) = (u_{b,1}, \ldots, u_{b,r_{\mathrm{I}}}, v_{b,1}, \ldots, v_{b,r_{\mathrm{II}}}, w_{b,1}, w'_{b,1}, \ldots, w_{b,r_{\mathrm{III}}}, w'_{b,r_{\mathrm{III}}}).$$

Then

$$\begin{aligned}\psi(\langle \boldsymbol{x}, \boldsymbol{u}\rangle_{\prec}) &= \psi\left(\sum_{b\in P}\boldsymbol{x}_b\widehat{\boldsymbol{u}_b}\right) = \sum_{b\in P}\psi(\boldsymbol{x}_b)\psi(\widehat{\boldsymbol{u}_b})\\ &= \left(\sum_{b\in P}x_{b,1}u_{b,1}, \ldots, \sum_{b\in P}x_{b,r_{\mathrm{I}}}u_{b,r_{\mathrm{I}}}, \sum_{b\in P}y_{b,1}\overline{v_{b,1}}, \ldots, \sum_{b\in P}y_{b,r_{\mathrm{II}}}\overline{v_{b,r_{\mathrm{II}}}},\right.\\ &\quad \left.\sum_{b\in P}z_{b,1}w'_{b,1}, \sum_{b\in P}z'_{b,1}w_{b,1}, \ldots, \sum_{b\in P}z_{b,r_{\mathrm{III}}}w'_{b,r_{\mathrm{III}}}, \sum_{b\in P}z'_{b,r_{\mathrm{III}}}w_{b,r_{\mathrm{III}}}\right).\end{aligned}$$

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

$$\sum_{b\in P} x_{b,j}u_{b,j} = 0 \text{ for all } j = 1, 2, \ldots, r_{\mathrm{I}}, \quad \sum_{b\in P} y_{b,j}\widetilde{v_{b,j}} = 0 \text{ for all } j = 1, 2, \ldots, r_{\mathrm{II}},$$

and

$$\sum_{b\in P} z_{b,j}w'_{b,j} = 0 = \sum_{b\in P} z'_{b,j}w_{b,j} \text{ for all } j = 1, 2, \ldots, r_{\mathrm{III}}.$$

Using the orthogonality in Proposition A.1, the Euclidean dual of $\mathcal{C}$ in (E3) can be viewed to be of the form

$$\mathcal{C}^{\perp_{\mathrm{E}}} \cong \left(\prod_{i=1}^{t_{\mathrm{I}}} U_i^{\perp_{\mathrm{E}}}\right) \times \left(\prod_{j=1}^{t_{\mathrm{II}}} V_j^{\perp_{\mathrm{H}}}\right) \times \left(\prod_{k=1}^{t_{\mathrm{III}}} \left((W'_k)^{\perp_{\mathrm{E}}} \times W_k^{\perp_{\mathrm{E}}}\right)\right). \tag{10}$$

A.2. Hermitian duality

Let ψ denote the isomorphism in (H1). Then each element $\boldsymbol{x} \in \mathcal{R}$, we can write

$$\psi(\boldsymbol{x}) = (x_1, \ldots, x_{t_{\mathrm{II}'}}, y_1, y'_1, \ldots, y_{t_{\mathrm{III}'}}, y'_{t_{\mathrm{III}'}}), \tag{11}$$

where $x_j \in \mathrm{GR}(p^r, s\acute{e}_j)$ and $y_k, y'_k \in \mathrm{GR}(p^r, s\acute{f}_k)$ for all $j = 1, 2, \ldots, t_{\mathrm{II}'}$ and $k = 1, 2, \ldots, t_{\mathrm{III}'}$.

We note that, for $\boldsymbol{c} = \sum_{a\in A} c_a Y^a \in \mathrm{GR}(p^r, s)[A]$, we have

$$\widetilde{\boldsymbol{c}} = \sum_{a\in A} \overline{c_a} Y^{-a} = \sum_{a\in A} \overline{c_{-a}} Y^a,$$

where $\overline{\alpha_0 + p\alpha_1 + \cdots + p^{r-1}\alpha_{r-1}} = \alpha_0^{p^{s/2}} + p\alpha_1^{p^{s/2}} + \cdots + p^{r-1}\alpha_{r-1}^{p^{s/2}}$. Then $\breve{\boldsymbol{c}} = \sum_{a\in A} \breve{w}_a Y^a$, where $\breve{w}_a = \sum_{h\in A} \overline{c_{-h}}\zeta^{\gamma_a(h)}$.

From (3), if $S_{p^s}(h)$ is of type II' with cardinality ν, then $-a = p^{s\nu/2} \cdot a$ by Remark 2.4. Since ν is odd, we have

$$\breve{w}_h = \sum_{a\in A} \overline{c_{-a}}\zeta^{\gamma_h(a)} = \sum_{a\in A} \overline{c_a}\zeta^{\gamma_{-h}(a)} = \sum_{a\in A} \overline{c_a}\zeta^{\gamma_{p^{s\nu/2}\cdot h}(a)} = \sum_{a\in A} \overline{c_a}\left(\zeta^{\gamma_h(a)}\right)^{p^{s\nu/2}} = \theta(\check{c}_h), \tag{12}$$

where $\theta(\alpha) = \alpha_0^{p^{s\nu/2}} + \alpha_1^{p^{s\nu/2}} p + \cdots + \alpha_{r-1}^{p^{s\nu/2}} p^{r-1}$ for all $\alpha = \alpha_0 + \alpha_1 p + \cdots + \alpha_{r-1}p^{r-1}$.

By the isomorphism ψ (see also [18]), we have the following properties.

1. By (12), the involution $\widetilde{\ }$ induces the ring automorphism $\bar{\ }$ on $\mathrm{GR}(p^r, s\acute{e}_j)$ as defined in (1), *i.e.*,

$$\overline{\alpha} = \alpha_0^{p^{s\acute{e}_j/2}} + \alpha_1^{p^{s\acute{e}_j/2}} p + \cdots + \alpha_{r-1}^{p^{s\acute{e}_j/2}} p^{r-1}$$

for all $\alpha = \alpha_0 + \alpha_1 p + \cdots + \alpha_{r-1}p^{r-1}$ in $\mathrm{GR}(p^r, s\acute{e}_j)$, where $a_i \in \mathcal{T}_{s\acute{e}_j}$ for all $i = 0, 1, \ldots, r-1$.

2. For each pair $(z, z') \in \mathrm{GR}(p^r, s\acute{f}_k) \times \mathrm{GR}(p^r, s\acute{f}_k)$, we have

$$\widetilde{\psi^{-1}(z, z')} = \psi^{-1}(z', z).$$

Hence, $\widetilde{\boldsymbol{x}}$ defined in Section 2 can be viewed in terms of (11) as

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

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

Proposition A.2. *Let* $\boldsymbol{x} = \sum_{b\in P} \boldsymbol{x}_b Y^b$ *and* $\boldsymbol{u} = \sum_{b\in P} \boldsymbol{u}_b Y^b$ *be elements in* $\mathcal{R}[P]$. *Decomposing* $\boldsymbol{x}_b, \boldsymbol{u}_b$ *using (11), we have*

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

and

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

Then

$$\begin{aligned}\psi(\langle \boldsymbol{x}, \boldsymbol{u}\rangle_\sim) &= \psi\left(\sum_{b\in P} \boldsymbol{x}_b \widetilde{\boldsymbol{u}_b}\right) = \sum_{b\in P} \psi(\boldsymbol{x}_b)\psi(\widetilde{\boldsymbol{u}_b}) \\ &= \left(\sum_{b\in P} x_{b,1}\overline{u_{b,1}}, \ldots, \sum_{b\in P} x_{b,t_{\mathrm{II}'}}\overline{u_{b,t_{\mathrm{II}'}}}, \sum_{b\in P} y_{b,1}v'_{b,1}, \sum_{b\in P} y'_{b,1}v_{b,1}, \ldots, \sum_{b\in P} y_{b,t_{\mathrm{III}'}}v'_{b,t_{\mathrm{III}'}}, \sum_{b\in P} y'_{b,t_{\mathrm{III}'}}v_{b,t_{\mathrm{III}'}}\right).\end{aligned}$$

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

$$\sum_{b\in P} x_{b,j}\overline{u_{b,j}} = 0 \text{ for all } j = 1, 2, \ldots, t_{\mathrm{II}'} \quad \text{and} \quad \sum_{b\in P} y_{b,k}v'_{b,k} = 0 = \sum_{b\in P} y'_{b,k}v_{b,k} \text{ for all } k = 1, 2, \ldots, t_{\mathrm{III}'}.$$

Using the orthogonality in Proposition A.2, the Hermitian dual of $\mathcal{C}$ in (H3) can be viewed of the form

$$\mathcal{C}^{\perp_{\mathrm{H}}} \cong \left(\prod_{j=1}^{t_{\mathrm{II}'}} E_j^{\perp_{\mathrm{H}}}\right) \times \left(\prod_{k=1}^{t_{\mathrm{III}'}} \left((F'_k)^{\perp_{\mathrm{E}}} \times F_k^{\perp_{\mathrm{E}}}\right)\right). \tag{13}$$

Acknowledgment: The authors would like to thank anonymous referees for useful comments.

References

[1] A. Batoul, K. Guenda, T. A. Gulliver, On self-dual cyclic codes over finite chain rings, Des. Codes Cryptogr. 70(3) (2014) 347–358.
[2] S. Benson, Students ask the darnedest things: A result in elementary group theory, Math. Mag. 70(3) (1997) 207–211.
[3] A. Boripan, S. Jitman, P. Udomkavanich, Characterization and enumeration of complementary dual abelian codes, J. Appl. Math. Comput. 58(1–2) (2018) 527–544.
[4] A. Boripan, S. Jitman, P. Udomkavanich, Self-conjugate-reciprocal irreducible monic factors of $x^n - 1$ over finite fields and their applications, Finite Fields Appl. 55 (2019) 78–96.
[5] B. Chen, S. Ling, G. Zhang, Enumeration formulas for self-dual cyclic codes, Finite Fields Appl. 42 (2016) 1–22.
[6] J. Chen, Y. Li, Y. Zhou, Morphic group rings, J. Pure Appl. Algebra 205(3) (2006) 621–639.
[7] H.Q. Dinh, S. R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inform. Theory 50(8) (2004) 1728–1744.
[8] T. J. Dorsey, Morphic and principal-ideal group rings, J. Algebra 318(1) (2007) 393–411.
[9] J. L. Fisher, S. K. Sehgal, Principal ideal group rings, Comm. Algebra 4(4) (1976) 319–325.
[10] A. R. Hammons, P.V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. Inform. Theory 40(2) (1994) 301–319.

[11] Y. Jia, S. Ling, C. Xing, On self-dual cyclic codes over finite fields, IEEE Trans. Inform. Theory 57(4) (2011) 2243–2251.
[12] S. Jitman, Good integers and some applications in coding theory, Cryptogr. Commun. 10(4) (2018) 685–704 and S. Jitman, Correction to: Good integers and some applications in coding theory, Cryptogr. Commun. 10(6) (2018) 1203–1203.
[13] S. Jitman, S. Ling, H. Liu, X. Xie, Abelian codes in principal ideal group algebras, IEEE Trans. Inform. Theory 59(5) (2013) 3046–3058.
[14] S. Jitman, S. Ling, E. Sangwisut, On self-dual cyclic codes of length p^a over $\mathrm{GR}(p^2, s)$, Adv. Math. Commun 10(2) (2016) 255–273.
[15] S. Jitman, S. Ling, P. Solé, Hermitian self-dual abelian codes, IEEE Trans. Inform. Theory 60(3) (2014) 1496–1507.
[16] H. M. Kiah, K. H. Leung, S. Ling, Cyclic codes over $\mathrm{GR}(p^2, m)$ of length p^k, Finite Fields Appl. 14(3) (2008) 834–846.
[17] H. M. Kiah, K. H. Leung, S. Ling, A note on cyclic codes over $\mathrm{GR}(p^2, m)$ of length p^k, Des. Codes Cryptogr. 63(1) (2012) 105–112.
[18] T. Kiran, B. S. Rajan, Abelian codes over Galois rings closed under certain permutations, IEEE Trans. Inform. Theory 49(9) (2003) 2242–2253.
[19] C. P. Milies, S. K. Sehgal, An Introduction to Group Rings, Lecture Notes in Mathematics vol. 1. Kluwer Academic Publishes, London, 2002.
[20] P. Moree, On the divisors of $a^k + b^k$, Acta Arithm. 80 (1997) 197–212.
[21] G. Nebe, E. M. Rains, N. J. A. Sloane, Self-Dual Codes and Invariant Theory, Algorithms and Computation in Mathematics vol. 17, Springer-Verlag, Berlin 2006.
[22] W. K. Nicholson, Local group rings, Canad. Math. Bull. 15(1) (1972) 137–138.
[23] A. Sălăgean, Repeated-root cyclic and negacyclic codes over a finite chain ring, Discrete Appl. Math. 154(2) (2006) 413–419.
[24] R. Sobhani, M. Esmaeili, A note on cyclic codes over $\mathrm{GR}(p^2, m)$ of length p^k, Finite Fields Appl. 15(3) (2009) 387–391.
[25] Z. X. Wan, Lectures on Finite Fields and Galois Rings, World Scientific, New Jersey, 2003.
[26] W. Willems, A note on self-dual group codes, IEEE Trans. Inform. Theory 48(12) (2002) 3107–3109.
[27] X. Yang, J. L. Massey, The condition for a cyclic code to have a complementary dual, Discrete Math. 126(1–3) (1994) 391–393.