


---

This is the **submitted version** of the article:

Dougherty, Steven T.; Fernández-Córdoba, Cristina; Ten-Valls, Roger; [et al.].  
«Quaternary group ring codes : ranks, kernels and self-dual codes». Advances in  
Mathematics of Communications, Vol. 14, issue 2 (May 2020), p. 319-332. 14  
pàg. DOI 10.3934/amc.2020023

---

This version is available at <https://ddd.uab.cat/record/239907>

under the terms of the  <sup>IN</sup> COPYRIGHT license

## QUATERNARY GROUP RING CODES: RANKS, KERNELS AND SELF-DUAL CODES

STEVEN T. DOUGHERTY

Department of Mathematics  
University of Scranton  
Scranton, PA 18510, USA

CRISTINA FERNÁNDEZ-CÓRDOBA

Department of Information and Communications Engineering  
Universitat Autònoma de Barcelona  
08193-Bellaterra, Spain

ROGER TEN-VALLS

Department of Information and Communications Engineering  
Universitat Autònoma de Barcelona  
08193-Bellaterra, Spain

BAHATTIN YILDIZ

Department of Department of Mathematics and Statistics  
Northern Arizona University  
Flagstaff, AZ 86001, USA

(Communicated by Aim Sciences)

**ABSTRACT.** We study  $G$ -codes over the ring  $\mathbb{Z}_4$ , which are codes that are held invariant by the action of an arbitrary group  $G$ . We view these codes as ideals in a group ring and we study the rank and kernel of these codes. We use the rank and kernel to study the image of these codes under the Gray map. We study the specific case when the group is the dihedral group and the dicyclic group. Finally, we study quaternary self-dual dihedral and dicyclic codes, tabulating the many good self-dual quaternary codes obtained via these constructions, including the octacode.

Codes over  $\mathbb{Z}_4$  have received an enormous amount of attention ever since the landmark paper [13]. The major importance of these codes is that they are equipped with a Gray map to the binary Hamming space. This Gray map allows for many interesting non-linear binary codes to be viewed as images of linear quaternary codes under this map. This connection makes it important to understand families of quaternary codes and what their images are in the binary Hamming space.

Two of the most important and useful tools to study quaternary codes are the rank and kernel of the code. In this paper, we shall examine both the rank and kernel of a large family of quaternary codes and use these to examine their image under the Gray map.

Cyclic codes are one of the most important families of codes. They are characterized by the fact that the code is held invariant by the action of the cyclic group.

---

2000 *Mathematics Subject Classification*: Primary: 16S34; Secondary: 94B15.

*Key words and phrases*: Group Ring Codes, Quaternary Codes, Dicyclic, Dihedral, Rank, Kernel, self-dual Codes.

This work has been partially supported by the Spanish MINECO under Grant TIN2016-77918-P (AEI/FEDER, UE).

Moreover, cyclic codes have a canonical characterization as ideals in a polynomial ring which enables a classification of cyclic codes. We generalize this definition to  $G$ -codes, which are codes that are held invariant by the action of an arbitrary finite group  $G$ . When the group is specified we use the name of the group. For example, we can talk about cyclic codes, dihedral codes, or dicyclic codes. We then show how these codes can be described in terms of certain skew polynomial rings.

Codes as ideals in group algebras were first studied by Jesse MacWilliams in [15] and [16]. In these early works the alphabet was always the binary alphabet. Our goal is to study the alphabet  $\mathbb{Z}_4$  and use non-abelian groups as well. We begin with the standard definitions. For a complete description of codes over rings and for any undefined terms see [4].

A code over the ring  $\mathbb{Z}_4$  of length  $n$  is a subset of  $\mathbb{Z}_4^n$  and a binary code of length  $n$  is a subset of  $\mathbb{F}_2^n$ . For the ring  $\mathbb{Z}_4$  we say the code is linear if it is a submodule of  $\mathbb{Z}_4^n$  and for  $\mathbb{F}_2$  we say it is linear if it is a sub-vector space of  $\mathbb{F}_2^n$ .

We attach the usual inner-product to  $\mathbb{Z}_4^n$ , namely  $[\mathbf{v}, \mathbf{w}] = \sum v_i w_i$  and we define the orthogonal to a code  $\mathcal{C}$  in  $\mathbb{Z}_4^n$  as  $\mathcal{C}^\perp = \{\mathbf{v} \mid \mathbf{v} \in \mathbb{Z}_4^n, [\mathbf{v}, \mathbf{w}] = 0 \ \forall \mathbf{w} \in \mathcal{C}\}$ . If  $\mathcal{C} \subseteq \mathcal{C}^\perp$ , we say that  $\mathcal{C}$  is self-orthogonal and if  $\mathcal{C} = \mathcal{C}^\perp$  we say that  $\mathcal{C}$  is self-dual.

Denote by  $\phi$  the standard Gray map  $\phi : \mathbb{Z}_4 \rightarrow \mathbb{F}_2^2$  that is defined by  $0 \rightarrow 00, 1 \rightarrow 01, 2 \rightarrow 11, 3 \rightarrow 10$ , see [13] for a complete description of this map. We extend this map to  $\mathbb{Z}_4^n \rightarrow \mathbb{F}_2^{2n}$  by applying it coordinatewise. If  $\mathcal{C}$  is a quaternary code, then  $\phi(\mathcal{C})$  is a binary code that is not linear in general. This map has been generalized to numerous rings. For the widest generalization see [7].

We now give the standard definition of the kernel and the rank of a binary code and relate this code to its quaternary preimage. Let  $C$  be a binary, not necessarily linear code. First, we say that a linear subcode  $C_i$  of  $C$  is a maximal linear code in  $C$  if for any linear code  $D_i$  satisfying  $C_i \subseteq D_i \subseteq C$  we have  $C_i = D_i$ .

Define the kernel of  $C$  to be

$$(1) \quad \ker(C) = \{\mathbf{v} \in \mathbb{F}_2^n \mid \mathbf{v} + C = C\}.$$

If  $\mathcal{C}$  is a quaternary code then its kernel is defined to be

$$(2) \quad \mathcal{K}(\mathcal{C}) = \{\mathbf{v} \in \mathcal{C} \mid \phi(\mathbf{v}) \in \ker(\phi(\mathcal{C}))\}.$$

Note that  $\ker(C)$  must be a linear code and, in fact, it can be characterized as the intersection of all maximal linear codes in  $C$ . Moreover, the code  $C$  can be seen as the union of the cosets of  $\ker(C)$  in  $C$ . See [9] for a complete description of these results.

Denote by  $\langle C \rangle$  the linear binary code generated by the vectors in  $C$ . We say that the rank of  $C$  is

$$(3) \quad \text{rank}(C) = \dim(\langle C \rangle).$$

For a quaternary code  $\mathcal{C}$  we shall also say that  $\text{rank}(\mathcal{C}) = \text{rank}(\phi(\mathcal{C}))$ . Then define the quaternary preimage of  $\langle \phi(\mathcal{C}) \rangle$  as  $\mathcal{R}(\mathcal{C})$ , that is,

$$(4) \quad \phi(\mathcal{R}(\mathcal{C})) = \langle \phi(\mathcal{C}) \rangle.$$

We have the following lemma which appears in [9].

**Lemma 1.** *Let  $\mathcal{C}$  be quaternary linear code. Then,  $\mathcal{R}(\mathcal{C})$  and  $\mathcal{K}(\mathcal{C})$  are quaternary linear codes satisfying*

$$\mathcal{K}(\mathcal{C}) \subseteq \mathcal{C} \subseteq \mathcal{R}(\mathcal{C}).$$

For vectors  $\mathbf{v}, \mathbf{w} \in \mathbb{Z}_4^n$ , define the operation  $\mathbf{v} * \mathbf{w} = (v_1w_1, v_2w_2, \dots, v_nw_n)$ . In [13], it is proved that  $\phi(\mathbf{v} + \mathbf{w}) = \phi(\mathbf{v}) + \phi(\mathbf{w}) + \phi(2\mathbf{v} * \mathbf{w})$ . The following lemma follows from the last property and can be found in [9].

**Lemma 2.** *Let  $\mathcal{C}$  be a quaternary linear code.*

1. *The code  $\phi(\mathcal{C})$  is linear if and only if  $2\mathbf{v} * \mathbf{w} \in \mathcal{C}$  for all  $\mathbf{w} \in \mathcal{C}$ .*
2. *The kernel of  $\mathcal{C}$  is*

$$\mathcal{K}(\mathcal{C}) = \{\mathbf{v} \in \mathcal{C} \mid 2\mathbf{v} * \mathbf{w} \in \mathcal{C}, \forall \mathbf{w} \in \mathcal{C}\}.$$

3. *The code  $\mathcal{R}(\mathcal{C})$  is*

$$\mathcal{R}(\mathcal{C}) = \langle \mathcal{C}, 2\mathbf{v} * \mathbf{w} \mid \mathbf{v}, \mathbf{w} \in \mathcal{C} \rangle.$$

### 1. G-CODES OVER $\mathbb{Z}_4$

We now give the standard definition of group rings and show how to construct codes as ideals in these group rings. Let  $G = \{g_1, g_2, \dots, g_n\}$  be a group of order  $n$  and denote by  $e_G$  the identity element in  $G$ . If  $G$  is non-abelian then one must distinguish between left and right ideals. We shall assume throughout that we are always dealing with left ideals and multiply by group elements on the left. Similar results can be obtained for right ideals. For abelian groups, the left and right ideals coincide.

We define the group ring

$$(5) \quad \mathbb{Z}_4G = \{v_1g_1 + \dots + v_ng_n \mid v_i \in \mathbb{Z}_4, g_i \in G, 1 \leq i \leq n\},$$

where the addition in  $\mathbb{Z}_4G$  is done by coordinate addition, namely

$$(6) \quad \sum_{i=1}^n \alpha_i g_i + \sum_{i=1}^n \beta_i g_i = \sum_{i=1}^n (\alpha_i + \beta_i) g_i,$$

and the product in  $\mathbb{Z}_4G$  is given by

$$(7) \quad \left( \sum_{i=1}^n \alpha_i g_i \right) \left( \sum_{j=1}^n \beta_j g_j \right) = \sum_{i,j} \alpha_i \beta_j g_i g_j.$$

Note that the coefficient of  $g_i$  in the product is

$$\sum_{g_j g_k = g_i} \alpha_j \beta_k.$$

We shall consider linear codes over  $\mathbb{Z}_4$  that are ideals in the group ring  $\mathbb{Z}_4G$ . First, define the one-to-one map  $I : \mathbb{Z}_4^n \rightarrow \mathbb{Z}_4G$  given by

$$I(v_1, v_2, \dots, v_n) = v_1g_1 + v_2g_2 + \dots + v_ng_n.$$

If  $g \in G$ ,  $\mathbf{v} \in \mathbb{Z}_4^n$ , and  $I(\mathbf{v}) = v = v_1g_1 + v_2g_2 + \dots + v_ng_n \in \mathbb{Z}_4G$ , then  $g(\mathbf{v})$  is the vector  $I^{-1}(gv)$ , where  $gv = v_1gg_1 + v_2gg_2 + \dots + v_ngg_n$ .

If  $\mathcal{C}$  is a code over  $\mathbb{Z}_4$  then  $I(\mathcal{C}) = \{I(\mathbf{v}) \mid \mathbf{v} \in \mathcal{C}\}$ . If  $\mathcal{C}$  is linear, then  $I(\mathcal{C})$  is also linear. Note that for  $g \in G$ ,  $\mathbf{v} \in \mathbb{Z}_4^n$  and  $\lambda \in \mathbb{Z}_4$ , we have that  $\lambda g(\mathbf{v}) = g(\lambda \mathbf{v})$ . Then, we have  $I(\mathcal{C})$  is an ideal in  $\mathbb{Z}_4G$  if, for  $g \in G$  and  $v \in I(\mathcal{C})$ ,  $gv \in I(\mathcal{C})$ . If  $I(\mathcal{C})$  is an ideal in  $\mathbb{Z}_4G$ , then we say that  $\mathcal{C}$  is a  $G$ -code over  $\mathbb{Z}_4$ .

Let  $S_n$  be the symmetric group of permutations on the set  $\{1, \dots, n\}$ . Recall the standard definition of an automorphism group of a code  $C$  of length  $n$ . Namely, let  $C$  be a code and let  $\tau \in S_n$ , with  $\tau$  acting on the coordinates of  $C$ . Then we define

$$(8) \quad \text{Aut}(C) = \{\tau \in S_n \mid \tau(C) = C\}.$$

The following lemma is immediate.

**Lemma 3.** *Let  $\mathcal{C}$  be a linear code over  $\mathbb{Z}_4$ . If  $\mathcal{C}$  is a  $G$ -code, then  $\text{Aut}(\mathcal{C})$  must contain the group  $G$ .*

In many respects, this lemma is the key motivation for studying codes as ideals in a group ring. That is, we wish to find codes that are held invariant by the actions of some group.

We now give a construction of a code from an element of the group ring. This construction was given for codes over rings in [8] and for codes over fields in [14]. It was used in [12] to construct self-dual codes. Let  $v = v_1g_1 + \cdots + v_ng_n \in \mathbb{Z}_4G$ . Notice that the elements  $g_1^{-1}, g_2^{-1}, \dots, g_n^{-1}$  are simply the elements of the group  $G$  in some order. Then, define the matrix  $\sigma(v) \in M_n(\mathbb{Z}_4)$  to be

$$(9) \quad \sigma(v) = \begin{pmatrix} I^{-1}(g_1^{-1}v) \\ \vdots \\ I^{-1}(g_n^{-1}v) \end{pmatrix} = \begin{pmatrix} v_{1,1} & \cdots & v_{1,n} \\ \vdots & \vdots & \vdots \\ v_{n,1} & \cdots & v_{n,n} \end{pmatrix},$$

where  $v_{i,j} = v_k$ , for  $k$  satisfying  $g_i^{-1}g_j = g_k$ .

For a given element  $v \in \mathbb{Z}_4G$ , define  $\mathcal{C}(v)$  as the quaternary code with generator matrix  $\sigma(v)$ . It is immediate that if  $\mathbf{v}$  has weight 0 then  $\mathcal{C}(I(\mathbf{v})) = \{\mathbf{0}\}$  and if  $\mathbf{w}$  has Lee weight 1, then  $\mathcal{C}(I(\mathbf{w})) = \mathbb{Z}_4^n$ .

**Lemma 4.** *Let  $g \in G$ . If  $v, w \in \mathbb{Z}_4G$  with  $gv = w$  then  $\mathcal{C}(v) = \mathcal{C}(w)$ .*

*Proof.* The matrix  $\sigma(gv) = \sigma(w)$  is the matrix  $\sigma(v)$  with the rows permuted. Hence they generate the same code.  $\square$

Let  $G$  be a group. We say that  $G$  is the internal semi-direct product of its subgroups  $H$  and  $N$  if  $N$  is a normal subgroup of  $G$ ,  $H \cap N = \{e_G\}$  and  $G = NH$ . It is denoted  $G = H \ltimes N$ .

Let  $H$  and  $N$  be groups and let  $\tau : H \rightarrow \text{Aut}(N)$  be an homomorphism. The external semi-direct product of  $H$  and  $N$  is  $G = H \ltimes_{\tau} N$  defined by

$$G = \{(h, n) \mid h \in H, n \in N\}$$

with the group operation  $(h_1, n_1)(h_2, n_2) = (h_1h_2, n_1^{\tau(h_2)}n_2)$ .

In both cases, we will refer to  $G$  as the semi-direct product a  $H$  and  $N$ , and it will be denoted by  $G = H \ltimes N$  even though in some cases it depends on the action  $\tau$ .

1.1. SOME FAMILIES OF  $G$ -CODES. We shall define the groups that we use in this paper. The first group is the cyclic group  $C_t$ , which is defined as

$$(10) \quad C_t = \langle a \mid a^t = 1 \rangle.$$

Codes that are ideals in  $\mathbb{F}_2C_t$  are one of the most widely studied families of codes.

The second group is the dihedral group  $D_{2t}$  (see [10], [11]). The dihedral group is defined as

$$(11) \quad D_{2t} = \langle a, b \mid b^t = 1, a^2 = 1, aba^{-1} = b^{-1} \rangle.$$

By considering the action  $\tau : C_2 \rightarrow C_t$  given by  $\tau(y)(x) = x^{-1}$ , we have  $D_{2t} = C_t \ltimes C_2$  [20].

Note that the notation for the dihedral group is not the same in all texts, as some might refer to this group as  $D_t$ . This group can be seen as the group of symmetries of a regular  $t$  sided figure in a Euclidean plane. The element  $b$  corresponds to rotating

the object  $\frac{2\pi}{t}$  radians with respect to its center and the element  $a$  corresponds to flipping the object over.

The third group is also a generalization of the cyclic group, namely the dicyclic group. The dicyclic group is defined as

$$(12) \quad Dic_{4t} = \langle a, b \mid a^{2t} = 1, b^2 = a^t, bab^{-1} = a^{-1} \rangle.$$

We note that both  $D_{2t}$  and  $Dic_{4t}$  are non-abelian groups for  $t \geq 3$ , while the cyclic group is abelian.

1.1.1. *Cyclic codes.* One of the most studied families of codes are cyclic codes. Initially, the cyclic codes were studied over a finite field. Cyclic codes may also be studied as ideals in the group algebra of a cyclic group (see [11]). In [13] cyclic codes over  $\mathbb{Z}_4$  were introduced and, since then, cyclic codes have been studied over different rings.

Cyclic codes, by definition, are invariant under the action of  $C_n$ , and therefore have  $C_n$  as a subgroup of their automorphism groups. This can also be seen by considering cyclic codes over  $\mathbb{Z}_4$  as ideals in  $\mathbb{Z}_4C_n$ . If  $\mathcal{C}$  is a cyclic code of length  $n$  then  $Aut(\mathcal{C})$  must contain  $C_n$  as a subgroup.

One of the most important aspects of cyclic codes is that they can be understood by studying ideals in a polynomial ring. Specifically, cyclic codes of length  $n$  over a ring  $R$  are ideals in  $R[x]/\langle x^n - 1 \rangle$ . This is easily generalized to constacyclic codes by studying ideals in  $R[x]/\langle x^n - \lambda \rangle$ , with  $\lambda$  a unit in the ring  $R$ . If we define  $S = \mathbb{Z}_4[x]/\langle x^n - 1 \rangle$ , then  $S$  is the ambient space where cyclic codes reside. Cyclic codes can be considered as ideals in the polynomial ring  $S$ . The following Theorem gives the generator polynomials of cyclic codes over  $\mathbb{Z}_4$ .

**Theorem 1** ([19]). *Let  $\mathcal{C}$  be a cyclic code of odd length. Then, there are unique monic polynomials  $f(x)$ ,  $g(x)$  and  $h(x)$  such that  $\mathcal{C} = \langle f(x)h(x) + 2f(x) \rangle$ , with  $f(x)g(x)h(x) = x^n - 1$ , and  $|\mathcal{C}| = 4^{deg(g(x))}2^{deg(h(x))}$ .*

Let  $v = v_1g_1 + \dots + v_n g_n \in \mathbb{Z}_4C_n$ . Then, we can consider the polynomial  $v(x) = v_1 + v_2x + \dots + v_n x^{n-1}$ . Then, the code over  $\mathbb{Z}_4$  generated by  $\sigma(v)$  is the code generated by the polynomial  $v(x)$ .

1.1.2. *Dihedral Codes.* We shall now examine the specific case when the group  $G$  is the dihedral group.

A circulant matrix with elements from the ring  $R$  is of the form:

$$(13) \quad circ(a_1, a_2, \dots, a_n) = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_n & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \dots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \dots & a_1 \end{pmatrix}$$

A reverse circulant matrix with elements from the ring  $R$  is of the form:

$$(14) \quad rcirc(a_1, a_2, \dots, a_n) = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_2 & a_3 & a_4 & \dots & a_1 \\ a_3 & a_4 & a_5 & \dots & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & a_1 & a_2 & \dots & a_{n-1} \end{pmatrix}$$

Recall that  $D_{2t} = \langle a, b \mid a^2 = b^t = 1, ab = b^{-1}a \rangle$ . Take an ordering of the elements for the map  $\sigma$  as  $1, b, b^2, \dots, b^{t-1}, a, ab, ab^2, \dots, ab^{t-1}$ . Let  $v = \sum \alpha_{a^i b^j} a^i b^j$ . In this case, the matrix  $\sigma(v)$  is of the form:

$$(15) \quad \begin{pmatrix} A & B \\ B & A \end{pmatrix},$$

with  $A$  a circulant matrix,  $A = \text{circ}(\alpha_1 \alpha_b \alpha_{b^2}, \dots, \alpha_{b^{t-1}})$ , and  $B$  a reverse circulant matrix,  $B = \text{rcirc}(\alpha_a, \alpha_{ab}, \alpha_{ab^2}, \dots, \alpha_{ab^{t-1}})$ .

We can now give a description of dihedral codes in terms of a skew polynomial ring, specifically as an Ore extension of the polynomial ring corresponding to cyclic codes [17].

Let  $S = \mathbb{Z}_4[x]/\langle x^n - 1 \rangle$  and  $\tau \in S_n$  be a  $\mathbb{Z}_4$ -automorphism of  $S$  defined by  $\tau(x) = x^{-1}$ . We note that  $\tau$  is of order 2. Let  $\mathfrak{R}_n = S[y; \tau]/\langle y^2 - 1 \rangle$ , noting that  $y^2 - 1$  is central in  $S[y; \tau]$ . This ring is a non-commutative ring with  $|\mathfrak{R}_n| = 4^{2n}$ .

We can now make a correspondence in a canonical way between elements in the group ring and polynomials in the skew polynomial ring. For an element in  $\mathbb{Z}_4 D_{2n}$  define

$$(16) \quad \psi \left( \sum \alpha_{ij} b^i a^j \right) = \sum \alpha_{ij} x^i y^j.$$

**Theorem 2.** *Let  $\mathcal{C}$  be a left dihedral code in  $\mathbb{Z}_4 D_{2n}$  then  $\psi(\mathcal{C})$  is a left ideal in  $\mathfrak{R}_n$ .*

*Proof.* It is immediate that since  $\mathcal{C}$  is closed under addition and multiplication we have that  $\psi(\mathcal{C})$  is closed under addition and multiplication. Then we note that multiplication by  $x$  on the left corresponds to multiplication by the group element  $b$  and multiplication by  $y$  on the left corresponds to multiplication by  $a$  on the left. Moreover,  $yx = x^{-1}y$  and so  $yx y^{-1} = x^{-1}$ . Therefore, since  $\mathcal{C}$  is a left ideal in  $\mathbb{Z}_4 D_{2n}$ ,  $\psi(\mathcal{C})$  is a left ideal in  $\mathfrak{R}_n$ .  $\square$

**Example 1.** *Let  $p(x)$  be a divisor of  $x^n - 1$ . Then  $\psi^{-1}(\mathbb{Z}_4(p(x)))$  is a left dihedral code of length  $2n$ .*

Note that if  $\mathcal{C}$  is a  $\mathbb{Z}_4$ -dihedral code, then  $\mathcal{C}$  is the semi-direct product of  $\mathbb{Z}_4$ -cyclic codes [20]. In fact, any ideal in  $\mathfrak{R}_n = S[y; \tau]$  is of the form  $I_1 + yI_2$  with  $I_i$  an ideal in  $S$ , which gives that the ideal is the semi-direct product of cyclic codes.

1.1.3. *Dicyclic codes.* Recall that the dicyclic group is defined as

$$\text{Dic}_{4t} = \langle a, b \mid a^{2t} = 1, b^2 = a^t, bab^{-1} = a^{-1} \rangle.$$

Let  $v = \sum_{i=1}^{2t} \alpha_i a^{i-1} + \alpha_{i+2t} b a^{i-1}$ . In this case, the matrix  $\sigma(v)$  is of the form:

$$(17) \quad \begin{pmatrix} A & B \\ C & A \end{pmatrix},$$

with  $A = \text{circ}(\alpha_1, \alpha_2, \dots, \alpha_{2t})$ ,  $B = \text{rcirc}(\alpha_{1+2t}, \alpha_{2+2t}, \dots, \alpha_{4t})$  and

$$C = \text{rcirc}(\alpha_{1+3t}, \alpha_{2+3t}, \dots, \alpha_{4t}, \alpha_{1+2t}, \alpha_{2+2t}, \dots, \alpha_{3t}).$$

We can now give a similar description of dicyclic codes as ideal in a skew polynomial ring.

Let  $T = \mathbb{Z}_4[x]/\langle x^{2n} - 1 \rangle$ . We note that this is the ambient space for cyclic codes of length  $2n$ . Let  $\tau$  be a  $\mathbb{Z}_4$ -automorphism of  $S$  defined by  $\tau(x) = x^{-1}$ .

Let  $\mathfrak{A}_n = T[y; \tau]/\langle y^2 - x^n \rangle$ , noting that  $y^2 - x^n$  is central in  $T[y; \tau]$ . The ring  $\mathfrak{A}_n$  is a non-commutative ring with  $|\mathfrak{A}_n| = 4^{4n}$ .

We can now make a correspondence in a canonical way between elements in the group ring and polynomials in the skew polynomial ring. For an element in  $\mathbb{Z}_4\text{Dic}_{4n}$  define

$$(18) \quad \mu\left(\sum \alpha_{ij} a^i b^j\right) = \sum \alpha_{ij} a^i b^j.$$

**Theorem 3.** *Let  $\mathcal{C}$  be a left dicyclic code in  $\mathbb{Z}_4\text{Dic}_{4n}$ . Then  $\mu(\mathcal{C})$  is a left ideal in  $\mathfrak{A}_n$ .*

*Proof.* Since  $\mathcal{C}$  is closed under addition and multiplication, so is  $\mu(\mathcal{C})$ . Then we note that multiplication by  $x$  on the left corresponds to multiplication by the group element  $s$  and multiplication by  $y$  on the left corresponds to multiplication by  $b$  on the left. Moreover,  $yx = x^{-1}y$  and so  $xyy^{-1} = x^{-1}$ . Therefore, since  $\mathcal{C}$  is a left ideal in  $\mathbb{Z}_4\text{Dic}_{4n}$ ,  $\mu(\mathcal{C})$  is a left ideal in  $\mathfrak{A}_n$ .  $\square$

1.2. QUASI  $G$ -CODES. As we have seen in Lemma 3, if  $\mathcal{C}$  is a  $G$ -code, then  $\text{Aut}(\mathcal{C})$  contains the group  $G$ . For example, if  $\mathcal{C}$  is a  $C_n$ -code, then  $\text{Aut}(\mathcal{C})$  contains  $C_n$ . It may of course contain other elements, specifically it is possible that  $C_n \neq \text{Aut}(\mathcal{C})$ . The image of the cyclic code under the Gray map is a quasi-cyclic code. We shall now generalize this notion.

If  $\mathcal{D}$  is a code in  $R^{sn}$  with the coordinates partitioned into  $n$  sets of size  $s$ , where each set is assigned an element of  $G$  and the code is held invariant by the action of multiplying the coordinate set marker by every element of  $G$ , then the code  $\mathcal{D}$  is called a quasi-group code of index  $s$ . The word group can be replaced by the specific group in question. For example, it might be a quasi-cyclic code or a quasi-dihedral code.

**Theorem 4.** *If  $\mathcal{C}$  is an ideal in  $\mathbb{Z}_4G$  where  $G$  is a finite group of order  $N$ , then  $\phi(\mathcal{C})$  is a (possibly non-linear) quasi-group code of index 2 and length  $2N$ .*

*Proof.* The length of the image is immediate from the definition of  $\phi$ . Then since  $g\mathbf{v} \in \mathcal{C}$ , for all  $g \in G$ , we have that  $G$  acts on pairs of coordinates and gives a quasi-group code of index 2.  $\square$

Just as it is possible that  $G$  is not the full automorphism group of a  $G$ -code, it is also possible that a code may be a quasi- $G$  code for different groups with possibly different partitions of the coordinates.

**Lemma 5.** *Let  $\mathcal{C}_1$  and  $\mathcal{C}_2$  be two  $G$ -codes over  $\mathbb{Z}_4$ , then  $\mathcal{C}_1 \oplus \mathcal{C}_2$  is a  $G$ -code.*

*Proof.* Let  $\mathbf{v} \in \mathcal{C}_1, \mathbf{w} \in \mathcal{C}_2, \alpha, \beta \in \mathbb{Z}_4$ . Then  $g\alpha\mathbf{v} + g\beta\mathbf{w} \in \mathcal{C}_1 \oplus \mathcal{C}_2$  and then  $g(\alpha\mathbf{v} + \beta\mathbf{w}) \in \mathcal{C}_1 \oplus \mathcal{C}_2$ . Therefore,  $\mathcal{C}_1 \oplus \mathcal{C}_2$  is a  $G$ -code.  $\square$

Let  $\mathcal{C}$  and  $\mathcal{D}$  be linear codes over  $\mathbb{Z}_4$ . We define  $\mathcal{C} * \mathcal{D}$  as  $\{\mathbf{u} * \mathbf{v} \mid \mathbf{u} \in \mathcal{C}, \mathbf{v} \in \mathcal{D}\}$ .

**Theorem 5.** *Let  $\mathcal{C}_1$  and  $\mathcal{C}_2$  be binary  $G$ -codes of length  $n$ . Then  $\mathcal{C} = \mathcal{C}_1 \oplus 2\mathcal{C}_2$  is a quaternary  $G$  code. Moreover, if  $\mathcal{C}_1 * \mathcal{C}_1 \subseteq \mathcal{C}_2$  then the image under the Gray map is a linear quasi- $G$  code of length  $2n$ .*

*Proof.* It is well known, see [18] that if  $\mathcal{C}_1 * \mathcal{C}_1 \subseteq \mathcal{C}_2$  then the code has a linear binary image. By the previous lemma, the code  $\mathcal{C}$  is a quaternary  $G$  code since both  $\mathcal{C}_1$  and  $\mathcal{C}_2$  are held invariant by the action of  $G$ . Therefore the Gray image is a binary linear quasi- $G$  code.  $\square$

This theorem shows that given binary  $G$  codes of length  $n$  we can construct binary quasi- $G$  codes of length  $2n$  by using quaternary codes.



2. RANK AND KERNEL

We shall now examine the rank and kernel of  $G$  codes, viewed as an ideal in a group ring. When the size of the kernel of a code is the minimal size, we say that the kernel is a minimum. In the case the size of the kernel is the maximal, then we say that it is a maximum.

The result is a broad generalization of the fact that the kernel of a cyclic code is cyclic, which can be found in [6].

**Theorem 6.** *Let  $\mathcal{C}$  be a linear code over  $\mathbb{Z}_4$ . If  $\mathcal{C}$  is a  $G$ -code, then  $\mathcal{K}(\mathcal{C})$  is a  $G$ -code.*

*Proof.* Since  $\mathcal{K}(\mathcal{C})$  is linear, all we need to show is that, for all  $g \in G, v \in I(\mathcal{K}(\mathcal{C})), gv \in I(\mathcal{K}(\mathcal{C}))$ . We have  $\mathbf{v} = I^{-1}(v) \in \mathcal{K}(\mathcal{C})$ . Then, we have to show that  $g(\mathbf{v}) \in \mathcal{K}(\mathcal{C})$ ; that is, by Lemma 2,  $2g(\mathbf{v}) * \mathbf{w} \in \mathcal{C}$  for all  $\mathbf{w} \in \mathcal{C}$ .

For  $\mathbf{w} \in \mathcal{C}, 2g(\mathbf{v}) * \mathbf{w} = g(2\mathbf{v}) * \mathbf{w} = g(2v * g^{-1}\mathbf{w})$ . Since  $\mathbf{v} \in \mathcal{K}(\mathcal{C}), g^{-1}\mathbf{w} \in \mathcal{C}$  and  $I(\mathcal{C})$  is an ideal, we have  $2\mathbf{v} * g^{-1}\mathbf{w} \in \mathcal{C}$ . Therefore  $I(\mathcal{K}(\mathcal{C}))$  is an ideal of  $\mathbb{Z}_4G$ .  $\square$

Similarly, the next result is a broad generalization of the fact that  $\mathcal{R}(\mathcal{C})$  is cyclic when  $\mathcal{C}$  is cyclic which can also be found in [6].

**Theorem 7.** *Let  $\mathcal{C}$  be a linear code over  $\mathbb{Z}_4$ . If  $\mathcal{C}$  is a  $G$ -code, then  $\mathcal{R}(\mathcal{C})$  is a  $G$ -code.*

*Proof.* Since  $\mathcal{R}(\mathcal{C})$  is linear, we only have to check that, for  $x \in I(\mathcal{R}(\mathcal{C}))$  and  $g \in G$ , we have  $gx \in I(\mathcal{R}(\mathcal{C}))$ . If  $\mathbf{x} = I^{-1}(x)$ , then we have to check that  $g(\mathbf{x}) \in \mathcal{R}(\mathcal{C})$ .

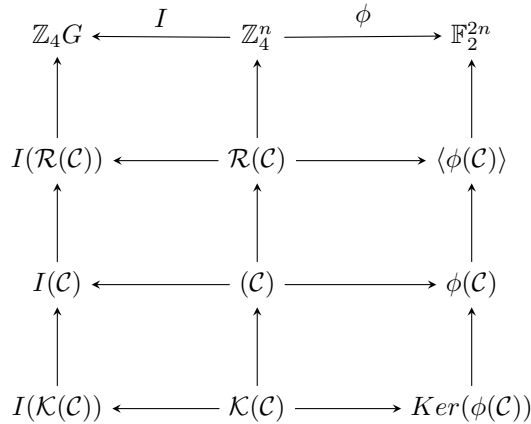
By Lemma 2, that  $\mathcal{R}(\mathcal{C}) = \langle \mathcal{C}, 2\mathbf{v} * \mathbf{w} \mid \mathbf{v}, \mathbf{w} \in \mathcal{C} \rangle$ . If  $\mathbf{x} \in \mathcal{R}(\mathcal{C})$ , then  $\mathbf{x} = \mathbf{u} + 2\mathbf{v} * \mathbf{w}$ , for some  $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{C}$ .

Since  $I(\mathcal{C})$  is an ideal,  $g(\mathbf{u}), g(\mathbf{v}), g(\mathbf{w}) \in \mathcal{C}$ . Then  $g(\mathbf{x}) = g(\mathbf{u}) + 2g(\mathbf{v}) * g(\mathbf{w}) \in \mathcal{R}(\mathcal{C})$  and so  $I(\mathcal{R}(\mathcal{C}))$  is an ideal of  $\mathbb{Z}_4G$ .  $\square$

Hence, for a  $G$ -code  $\mathcal{C}$  over  $\mathbb{Z}_4$ , we have

$$(19) \quad I(\mathcal{K}(\mathcal{C})) \subseteq I(\mathcal{C}) \subseteq I(\mathcal{R}(\mathcal{C})).$$

We summarize the relations between the codes in the following diagram.



**Theorem 8.** *Let  $\mathcal{C}$  be a  $G$ -code over  $\mathbb{Z}_4$ . Then  $\mathcal{K}(\mathcal{C})$  is the intersection of all maximal  $G$ -codes  $\mathcal{C}_i \subseteq \mathcal{C}$  satisfying that  $\phi(\mathcal{C}_i)$  is linear.*

*Proof.* We know that  $\mathcal{K}(\mathcal{C})$  is the intersection of all maximal codes  $\mathcal{C}_i \subseteq \mathcal{C}$  such that  $\phi(\mathcal{C}_i)$  is linear and, by Theorem 6,  $\mathcal{K}(\mathcal{C})$  is a  $G$ -code.

Let  $\mathcal{C}_i \subseteq \mathcal{C}$  be a maximal linear code over  $\mathbb{Z}_4$ . We have  $\mathcal{K}(\mathcal{C}) \subseteq \mathcal{C}_i$ . Since  $\mathcal{K}(\mathcal{C})$  is a  $G$ -code, there exists a code  $\mathcal{C}'_i$  that is a  $G$ -code with  $\mathcal{K}(\mathcal{C}) \subseteq \mathcal{C}'_i \subseteq \mathcal{C}_i$ . Hence, if  $\mathcal{K}(\mathcal{C})$  is the intersection of such  $\mathcal{C}_i$ , then  $\mathcal{K}(\mathcal{C})$  is also contained in the intersection of such  $\mathcal{C}'_i$  which gives the result.  $\square$

**Theorem 9.** *Let  $v \in \mathbb{Z}_4G$  and  $\mathcal{C}(v)$  be a  $G$ -code. Then  $\mathcal{C}(2v) \subseteq \mathcal{K}(\mathcal{C}(v))$ .*

*Proof.* If  $\mathbf{w} \in \mathcal{C}(2v)$  then  $\mathbf{w} \in \mathcal{C}(v)$  and  $\mathbf{w}$  has order 2, so  $2\mathbf{w} * \mathbf{u} = \mathbf{0} \in \mathcal{C}(\mathbf{v})$ , for all  $\mathbf{u} \in \mathcal{C}(v)$ , which implies  $\mathbf{w} \in \mathcal{K}(\mathcal{C}(v))$ .  $\square$

Therefore, the minimal kernel for any code  $\mathcal{C}(v)$  is  $\mathcal{C}(2v)$  and we have

$$\mathcal{C}(2v) = \mathcal{K}(\mathcal{C}(v)) = \mathcal{C}(v),$$

for all  $v$ .

Note that if  $v$  is of additive order 2 in  $\mathbb{Z}_4G$ , then  $\mathcal{C}(2v) = \{\mathbf{0}\}$ . However, in this case, we have that  $\phi(\mathcal{C}(v))$  is linear as it is shown in the following proposition.

**Proposition 1.** *Let  $v \in \mathbb{Z}_4G$  and  $\mathcal{C}(v)$  be a  $G$ -code. If  $v \in \mathcal{K}(\mathcal{C}(v))$ , then  $\mathcal{K}(\mathcal{C}(v)) = \mathcal{C}(v)$ .*

*Proof.* Let  $\mathbf{u} \in \mathcal{C}(v)$ ; that is,  $u = \sum_{i=1}^n \lambda_i g_i v$ , or  $\mathbf{u} = \sum_{i=1}^n \lambda_i g_i(\mathbf{v})$ , for  $\lambda_i \in \mathbb{Z}_4$ . For all  $\mathbf{w} \in \mathcal{C}(v)$ , we have that  $2\mathbf{u} * \mathbf{w} = 2(\sum_{i=1}^n g_i(\mathbf{v})) * \mathbf{w} = \sum_{i=1}^n g_i(2\mathbf{v} * g_i^{-1}(\mathbf{w})) \in \mathcal{C}(v)$  because  $\mathbf{v} \in \mathcal{K}(\mathcal{C}(v))$  and, therefore,  $\mathbf{u} \in \mathcal{K}(\mathcal{C}(v))$ .  $\square$

**Corollary 1.** *Let  $v \in \mathbb{Z}_4G$  and  $\mathcal{C}(v)$  be a  $G$ -code. If  $v$  has additive order 2 in  $\mathbb{Z}_4G$  then  $\mathcal{K}(\mathcal{C}(v)) = \mathcal{C}(v)$ .*

*Proof.* If  $v$  has additive order 2, then for all  $\mathbf{u} \in \mathcal{C}(v)$ ,  $2\mathbf{v} * \mathbf{u} = \mathbf{0} \in \mathcal{C}(v)$  and  $v \in \mathcal{K}(\mathcal{C})$ . Therefore, the results follows by Proposition 1.  $\square$

It is proven in [8] that if  $I(\mathcal{C})$  is an ideal in  $\mathbb{Z}_4G$  then  $I(\mathcal{C}^\perp)$  is an ideal in  $\mathbb{Z}_4G$ .

The following gives an example where the kernel of a group code over  $\mathbb{Z}_4$  is a minimum for all groups  $G$ . Specifically, where  $\mathcal{K}(\mathcal{C}(v)) = \mathcal{C}(2v)$ .

**Theorem 10.** *Let  $v = 1e_G - h$  for some  $h \in G - \{e_G\}$ , where  $e_G$  is the identity element of the group  $G$ . Then  $|\mathcal{C}(v)| = 4^{n-2}$ ,  $\mathcal{C}(v) = \langle \mathbf{1}_{\frac{n}{2}} \rangle^\perp \times \langle \mathbf{1}_{\frac{n}{2}} \rangle^\perp$ , where*

$$\mathcal{K}(\mathcal{C}(v)) = 2(\mathcal{C}(v)) = \mathcal{C}(2v)$$

and

$$\mathcal{R}(\mathcal{C}(v)) = \langle \mathcal{C}(v), (2, 0, 0, \dots, 0), (\mathbf{0}_{\frac{n}{2}}, 2, 0, 0, \dots, 0) \rangle.$$

*Proof.* It is immediate that  $|\mathcal{C}(v)| = 4^{n-2}$ , by examining the generator matrix  $\sigma(v)$  and seeing the code as  $\langle \mathbf{1}_{\frac{n}{2}} \rangle^\perp \times \langle \mathbf{1}_{\frac{n}{2}} \rangle^\perp$ .

Then for every  $gv$  there exists  $g'v$  where  $2(gv) * (g'v) = (0, 0, \dots, 0, 2, 0, \dots, 0)$  which is not in  $\mathcal{C}(v)$ . It follows that the kernel is a minimum. It is a simple consequence that  $\mathcal{R}(\mathcal{C})$  is  $\langle \mathcal{C}(v), (2, 0, 0, \dots, 0), (\mathbf{0}_{\frac{n}{2}}, 2, 0, 0, \dots, 0) \rangle$ . Namely, we have adjoined  $2gv * (g'v)$  and that gives us the rank.  $\square$

2.1. RANK AND KERNEL OF  $I(\mathcal{C})$  FOR SOME FAMILIES OF CODES. Recall that the minimal kernel of a code  $\mathcal{C}(v)$  is given when  $\mathcal{K}(\mathcal{C}(v)) = \mathcal{C}(2v)$  and the maximal when  $\mathcal{K}(\mathcal{C}(v)) = \mathcal{C}(v)$ . In this section we will see that there exist  $G$ -codes with both minimal and maximal kernel when  $G$  is  $C_n$ ,  $D_{2n}$  and  $Dic_{4t}$ .

The rank and kernel of cyclic codes over  $\mathbb{Z}_4$  were studied in [6]. In that paper, it was shown that there exist cyclic codes over  $\mathbb{Z}_4$  with the minimal and maximal kernels. We give just some example.

**Example 2.** Consider the cyclic code of length  $n$  generated by the polynomial  $x-1$ , that is, the ideal  $\mathcal{C}_1 = \langle x-1 \rangle$  in  $\mathbb{Z}_4[x]/\langle x^n-1 \rangle$ . Theorem 10 gives that for this code  $\mathcal{K}(\mathcal{C}_1)$  is a minimum. The code  $\mathcal{C}_2 = \langle 2(x-1) \rangle$  has  $\mathcal{K}(\mathcal{C}_2) = \mathcal{C}$  and hence the kernel is a maximum.

In fact, in Theorem 17 in [6], if  $C = \langle f(x)h(x) + 2f(x) \rangle$  is a quaternary cyclic code of odd length  $n = p^2$  and  $x^n - 1 = (x-1)a(x)b(x)$  with  $a(x)$  and  $b(x)$  irreducible polynomials over  $\mathbb{Z}_4$ , then for  $h(x) = 1$  and  $f(x) = a(x)$ , we have  $\mathcal{K}(C) = \langle 1 + x + \dots + x^{n-1} + 2a(x) \rangle$ . Moreover, if  $f(x) = b(x)$  then  $\mathcal{K}(C) = C$ .

**Theorem 11.** Let  $G$  be the dihedral group  $D_{2t}$ . Let  $v = \sum \alpha_i g_i$ , with  $\alpha_i = 0$  if  $g_i = ab^s$ . Then  $\mathcal{C}(v) = \mathcal{C}_1 \times \mathcal{C}_2$ , with  $\mathcal{C}_1$  and  $\mathcal{C}_2$  cyclic codes, and

$$(20) \quad \mathcal{K}(C) = \mathcal{K}(\mathcal{C}_1) \times \mathcal{K}(\mathcal{C}_2)$$

and

$$(21) \quad \mathcal{R}(C) = \mathcal{R}(\mathcal{C}_1) \times \mathcal{R}(\mathcal{C}_2).$$

*Proof.* If  $\alpha_i = 0$ , when  $g_i = b^s a$ , then the generator matrix  $\sigma(v)$  is of the form

$$(22) \quad \begin{pmatrix} A & \mathbf{0} \\ \mathbf{0} & A \end{pmatrix}$$

with  $A$  generating a cyclic code. The result follows.  $\square$

**Example 3.** Consider the dihedral group  $D_{2t}$ . Let  $v = 1-b$ , then Theorem 10 gives  $\mathcal{K}(\mathcal{C}(v)) = \mathcal{C}(2v)$ , hence it is a minimum. As in the previous example, if  $v = 2-2b$ , then  $\mathcal{K}(\mathcal{C}(v)) = \mathcal{C}(v)$  and hence it is a maximum.

Let  $\mathcal{C}_1$  and  $\mathcal{C}_2$  be quaternary cyclic codes of odd length  $n = p^2$  and  $x^n - 1 = (x-1)ab$  with  $a$  and  $b$  irreducible polynomials over  $\mathbb{Z}_4$ . Let  $\mathcal{C}_1 = \mathcal{C}_2 = \langle b, 2bg \rangle$ . Let  $C$  be the dihedral code  $C = \mathcal{C}_1 \times \mathcal{C}_2$  as given in Theorem 11. By Theorem 11, we have  $\mathcal{K}(C) = C$  and the kernel is a maximum. Theorem 10 has already given examples of dihedral codes with minimum kernel. Therefore we have the following.

**Theorem 12.** There exists dihedral codes with minimal kernel and with maximal kernel.

**Example 4.** For length 4, (here the dihedral group is really the Klein 4 group), it is a simple computation to see that, for all  $v$ , we have  $\mathcal{K}(v) = C(v) = \mathcal{R}(v)$ .

We can now mimic the technique used in Theorem 11 to get a similar result for dicyclic codes.

**Theorem 13.** Let  $G$  be the dicyclic group  $Dic_{4t}$ . Let  $v = \sum \alpha_i g_i$ , with  $\alpha_{i+2t} = 0$  for  $i \in \{1, \dots, 2t\}$ . Then  $\mathcal{C}(v) = \mathcal{C}_1 \times \mathcal{C}_2$ , where  $\mathcal{C}_1$  and  $\mathcal{C}_2$  are cyclic codes and

$$(23) \quad \mathcal{K}(C) = \mathcal{K}(\mathcal{C}_1) \times \mathcal{K}(\mathcal{C}_2)$$

and

$$(24) \quad \mathcal{R}(\mathcal{C}) = \mathcal{R}(\mathcal{C}_1) \times \mathcal{R}(\mathcal{C}_2).$$

*Proof.* If  $\alpha_i = 0$ , when  $i > 2t$ , then the generator matrix  $\sigma(v)$  is of the form

$$(25) \quad \begin{pmatrix} A & \mathbf{0} \\ \mathbf{0} & A \end{pmatrix}$$

with  $A$  generating a cyclic code. The result follows. □

Again using Theorem 17 in [6], we can let  $\mathcal{C}_1$  and  $\mathcal{C}_2$  be quaternary cyclic codes of odd length  $n = p^2$  and  $x^n - 1 = (x - 1)a(x)b(x)$  where  $a(x)$  and  $b(x)$  are irreducible polynomials. Let  $\mathcal{C}_1 = \mathcal{C}_2 = \langle b(x), 2b(x)g(x) \rangle$ . Let  $\mathcal{C}$  be the dicyclic code  $\mathcal{C} = \mathcal{C}_1 \times \mathcal{C}_2$  as given in Theorem 13. Hence, by Theorem 13, we have that  $\mathcal{K}(\mathcal{C}) = \mathcal{C}$  and the kernel is a maximum. Theorem 10 has already given examples of dicyclic codes with minimum kernel. Therefore we have the following.

**Theorem 14.** *There exists dicyclic codes with minimal kernel and with maximal kernel.*

### 3. SELF-DUAL CODES

We will discuss self-dual dihedral and dicyclic codes over  $\mathbb{Z}_4$  in this section. Self-dual codes over the ring  $\mathbb{Z}_4$  were first studied in [3]. Self-dual codes are an important class of codes as they are related to many other structures such as lattices, designs, etc. In particular, self-dual codes over  $\mathbb{Z}_4$  have been used to construct even unimodular lattices in [1].

Many of the construction methods in the literature for self-dual codes use generator matrices of the form  $[I_n|A]$ , with  $A$  a special type of matrix, such as a circulant or bordered circulant matrix. However, self-dual codes obtained from these constructions all fall into the category of *free* self-dual codes. It is well known from [3] that free self-dual codes over  $\mathbb{Z}_4$  exist only for lengths that are multiples of 8. Thus, following these constructions would restrict the lengths of the self-dual codes that we can obtain quite considerably. The dihedral and dicyclic matrix structures that we have discussed above suggest an alternative way of constructing self-dual codes over  $\mathbb{Z}_4$ , through which we could obtain self-dual codes of different lengths.

It is well known that self-dual codes over  $\mathbb{Z}_4$  exist for all lengths, see [3] or [5]. However, we are concerned with self-dual codes that are also group codes. Therefore, we are only concerned with lengths that are the order of a finite group. So for example, dihedral codes only exist for even lengths and dicyclic codes only exist for lengths a multiple of 4. The following existence theorem shows that if the length is appropriate then there is a self-dual  $\mathbb{Z}_4$  group code of that length.

**Theorem 15.** *For any positive integer  $n$ , there exists a self-dual  $\mathbb{Z}_4$   $G$ -codes for all finite groups  $G$  with  $|G| = n$ .*

*Proof.* Let  $\mathcal{C}$  be the code of length 1 generated by 2, namely  $\mathcal{C} = \{0, 2\}$ . This code is a self-dual code of length 1.

Let  $\mathcal{C}$  be a linear code over  $\mathbb{Z}_4$  and let  $\mathcal{C}_n = \{(\mathbf{c}, \dots, \mathbf{c}) : \mathbf{c} \in \mathcal{C}\}$  be the  $n$ -fold direct product of  $\mathcal{C}$ . Since the direct product of quaternary self-dual codes is self-dual we have that  $\mathcal{C}_n$  is a quaternary self-dual code of length  $n$ , see [5] for details.

If  $\tau$  is any permutation of the coordinates of  $\mathcal{C}$  we have  $\tau(\mathcal{C}) = \mathcal{C}$ . Therefore  $\mathcal{C}$  is held invariant by the action of any group. Therefore,  $\mathcal{C}$  is a self-dual  $G$  code of length  $n$  for any group  $G$  of order  $n$ .  $\square$

Naturally, the minimum Lee distance of all the self-dual codes that are generated by Theorem 15 is 2, which is, in general, not of interest for longer lengths.

Cyclic self-dual codes over  $\mathbb{Z}_4$  have been studied in [18]. Now we will study self-dual dihedral and dicyclic codes. For the rest of the section, the computer searches have been done by using the computer algebra system Magma [2].

**3.1. SELF-DUAL DIHEDRAL CODES.** We begin with a theorem which follows naturally from the fact that the dihedral code is the semi-direct product of  $\mathbb{Z}_4$ -cyclic codes as it was mentioned in Section 1.1.2.

**Theorem 16.** *Let  $\mathcal{C}$  and  $\mathcal{D}$  be self-dual cyclic codes of length  $n$ . Then  $\mathcal{C} \times \mathcal{D}$  is a self-dual Dihedral code of length  $2n$ .*

*Proof.* We have that  $\mathcal{C} \times \mathcal{D}$  is a dihedral code. Then if  $\mathbf{v}_1, \mathbf{w}_1 \in \mathcal{C}$  and  $\mathbf{v}_2, \mathbf{w}_2 \in \mathcal{D}$  then

$$[\mathbf{v}_1 \times \mathbf{w}_1, \mathbf{v}_2 \times \mathbf{w}_2] = [\mathbf{v}_1, \mathbf{w}_1] + [\mathbf{v}_2, \mathbf{w}_2] = 0 + 0 = 0.$$

Therefore, the code is self-dual.  $\square$

We ran some computer searches for all dihedral self-dual  $\mathbb{Z}_4$ -codes of lengths 4, 6, 8, 10 and 12. The results we obtained are of interest.

TABLE 1. (Extremal) Dihedral Self-dual Codes of length 4

First Row of A	First row of B	Min Lee Weight	Lee Weight Distribution
(1,1)	(1,3)	4	$1 + 14z^4 + z^8$
(1,1)	(3,1)	4	$1 + 14z^4 + z^8$
(1,3)	(1,1)	4	$1 + 14z^4 + z^8$
(1,3)	(3,3)	4	$1 + 14z^4 + z^8$
(3,1)	(1,1)	4	$1 + 14z^4 + z^8$
(3,1)	(3,3)	4	$1 + 14z^4 + z^8$
(1,3)	(1,3)	4	$1 + 14z^4 + z^8$
(3,3)	(3,1)	4	$1 + 14z^4 + z^8$

**Remark 1.** *Note that the Lee weight distribution of all the self-dual codes obtained in Table 1 is the same as the Hamming weight distribution of the extended binary Hamming code, which is an extremal Type II code of length 8. In fact, it turns out that the Gray image of all the codes in Table 1 are linear over the binary field, and moreover they are all self-dual. So, the Gray maps of codes in Table 1 are precisely the extended binary Hamming code of length 8.*

**Remark 2.** *We obtained many self-dual dihedral codes of length 8 and minimum Lee distance 4. We just put a few of them in Table 2, which represent the typical case. Unlike the case of length 4, we obtained both Type I and Type II weight enumerators for extremal binary self-dual codes of length 16. Indeed, upon checking the Gray images, we see that the Gray images of all the self-dual dihedral codes of length 8 and minimum Lee distance 4 are (linear) extremal binary self-dual codes of length 16, with some being Type I and some Type II.*

TABLE 2. (Extremal) Dihedral Self-dual Codes of length 8

First Row of $A$	First row of $B$	Min Lee Weight	Lee Weight Distribution
(0,0,2,2)	(1,1,3,1)	4	$1 + 28z^4 + 198z^8 + \dots$
(0,0,0,0)	(1,3,1,1)	4	$1 + 28z^4 + 198z^8 + \dots$
(0,0,0,2)	(3,1,3,1)	4	$1 + 12z^4 + 64z^6 + 102z^8 + \dots$
(0,0,2,0)	(1,1,3,3)	4	$1 + 12z^4 + 64z^6 + 102z^8 + \dots$

Upon running an exhaustive search over all dihedral self-dual codes of length 6 and 10 we found that the highest minimum Lee distance is 2 and when we ran the search over all dihedral self-dual codes of length 12, the highest minimum Lee distance that we obtained turned out to be 4.

3.2. SELF-DUAL DICYCLIC CODES. We first recall that, because of their structure, dicyclic codes have to be of lengths  $4k$  for  $k \in \mathbb{Z}^+$ . Thus, we searched over all self-dual dicyclic  $\mathbb{Z}_4$ -codes of lengths 4, 8 and 12. Out of the many self-dual codes of best parameters that we obtained, we put a sample in the following table:

TABLE 3. Best Dicyclic Self-dual Codes of lengths 4, 8 and 12

$n$	1st row of $A$	1st row of $B$	1st row of $C$	Min Lee Weight	Gray Image Linear
4	(1,3)	(3,3)	(3,3)	4	Yes
8	(0,0,0,2)	(3,3,3,3)	(3,3,3,3)	4	Yes
8	(0,0,1,1)	(0,0,1,3)	(1,3,0,0)	4	No
8	(0,0,1,1)	(0,1,1,2)	(1,2,0,1)	6*	No
12	(0,0,0,0,0,0)	(0,1,3,0,1,1)	(0,1,1,0,1,3)	4	Yes

**Remark 3.** In Table 3, the code marked with  $*$  is the well-known octacode, which is a self-dual code of length 8, whose binary image is a non-linear code of length 16, size  $2^8$  and minimum distance 6. This is better than the best known binary linear code of the same length and dimension, as the minimum distance of a binary linear code of length 16 and dimension 8 can be at most 5. Thus we have obtained the octacode from the dicyclic construction.

**Remark 4.** An exhaustive search reveals that all the dicyclic self-dual codes of lengths 4 and 12 have 4 as the highest minimum Lee distance and all such examples have linear Gray map images.

#### 4. CONCLUSION

As a broad generalization of cyclic codes we have studied  $G$ -codes over the ring  $\mathbb{Z}_4$ , which are codes held invariant by the action of a finite group  $G$ . As an analogue to the results for cyclic codes, we have shown that the quaternary kernel and rank of a  $G$ -code is itself a  $G$ -code. We have found bounds for the size of the kernel and gave examples of minimal and maximal kernels for  $G$ -codes. Examining the image of  $G$ -codes under the canonical Gray map, we have shown how to construct binary quasi- $G$  codes. Finally, we have studied self-dual  $G$ -codes and given examples for the dihedral and dicyclic groups, in particular we have been able to obtain the octacode from the dicyclic construction.

We believe quaternary  $G$ -codes are a deep topic that would warrant further studies. As possible directions for future research, we can suggest different groups than dicyclic and dihedral groups, or a search for self-dual codes of higher lengths. Different rings than  $\mathbb{Z}_4$  can also be considered within the same context.

<doughertys1@scranton.edu; cristina.fernandez@uab.cat; rten@deic.uab.cat; bahattin.yildiz@nau.edu  
>

#### REFERENCES

- [1] E. Bannai, S.T. Dougherty, M. Harada and M. Oura, “Type II codes, even unimodular lattices, and invariant rings”, *IEEE Trans. Inform. Theory*, Vol. 45, No. 4, pp. 1194–1205, 1999.
- [2] W. Bosma, J.J. Cannon, C. Fieker, A. Steel: Handbook of Magma functions, Edition 2.22 5669 pages (2016). <http://magma.maths.usyd.edu.au/magma/>.
- [3] J. H. Conway and N. J. A. Sloane, “Self-dual codes over the integers modulo 4”, *J. Combin. Theory Ser. A*, Vol. 62, No. 1, pp. 30–45, 1993.
- [4] S.T. Dougherty, “Algebraic Coding Theory Over Finite Commutative Rings”, SpringerBriefs in Mathematics. Springer, Cham, 2017, ISBN: 978-3-319-59805-5; 978-3-319-59806-2.
- [5] S.T. Dougherty and C. Fernández-Córdoba, “Codes over  $\mathbb{Z}_{2^k}$ , Gray maps and Self-Dual Codes”, *Adv. in Math. of Commun.*, Vol. 5, No. 4, pp. 571–588, 2011.
- [6] S.T. Dougherty and C. Fernández-Córdoba, “Kernels and Ranks of Cyclic and Negacyclic Quaternary Codes”, *Des. Codes Cryptogr.*, Vol. 81, No. 2, pp. 347–364, 2016.
- [7] S.T. Dougherty, C. Fernández-Córdoba and R. Ten-Valls, “Quasi-Cyclic Codes as Cyclic Codes over a Family of Local Rings”, *Finite Fields Appl.*, Vol. 40, pp. 138–149, 2016.
- [8] S.T. Dougherty, J. Gildea, R. Taylor and A. Tylshchak, “Group Rings, G-Codes and Constructions of Self-Dual and Formally Self-Dual Codes”, *Des. Codes Cryptogr.*, **Online**: 10.1007/s10623-017-0440-7.
- [9] C. Fernández-Córdoba, J. Pujol and M. Villanueva, “On rank and kernel of  $\mathbb{Z}_4$ -linear codes”, *Lecture Notes in Computer Science*, No. 5228, pp. 46–55, 2008.
- [10] R. A. Ferraz, F.S. Dutra, C. Polcino Milies, “Semisimple group codes and dihedral codes”, *Algebra Discrete Math*, Vol. 3, pp. 28–48, 2009.
- [11] M. Guerreiro, “Group algebras and coding theory”, *So Paulo Journal of Mathematical Sciences*, Vol. 10, pp.346–371, 2016.
- [12] J. Gildea, A. Kaya, R. Taylor and B. Yildiz, “Constructions for self-dual codes induced from group rings”, *Finite Fields Appl.*, Vol. 51, pp. 71–92, 2018.
- [13] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, “The  $\mathbb{Z}_4$ -linearity of Kerdock, Preparata, Goethals, and related codes”, *IEEE Trans. Inform. Theory*, Vol. 40, No. 2, pp. 301–319, 1994.
- [14] T. Hurley, “Group Rings and Rings of Matrices”, *Int. Jour. Pure and Appl. Math*, Vol. 31, No. 3, pp. 319–335, 2006.
- [15] F.J. MacWilliams, “Binary codes which are ideals in the group algebra of an Abelian group”, *Bell System Tech. J.*, Vol. 49, pp. 987–1011, 1970.
- [16] F. J. MacWilliams, “Codes and ideals in group algebras”, *Combinatorial Mathematics and its Applications* (Proc. Conf., Univ. North Carolina, Chapel Hill, N.C., 1967) pp. 317–328, Univ. North Carolina Press, Chapel Hill, N.C., 1969.
- [17] O. Ore, “Theory of non-commutative polynomials”, *Annals of Mathematics*, Vol. 34, No. 3, pp. 480–508, 1933.
- [18] V. Pless, P. Solé and Z. Qian, “Cyclic self-dual  $\mathbb{Z}_4$ -codes, with an appendix by Pieter Moree”, *Finite Fields Appl.*, Vol. 3, No. 1, pp. 48–69, 1997.
- [19] V. Pless and Z. Qian, “Cyclic codes and quadratic residue codes over  $\mathbb{Z}_4$ ”, *IEEE Trans. Inform. Theory*, Vol. 42, No. 5, pp. 1594–1600, 1996.
- [20] D. J. S. Robinson, “A course in the Theory of Groups”, Graduate Texts in Mathematics Vol. 80, Springer-Verlag, 1993.