Algebra and Discrete Mathematics
Number 3. **(2009).** pp. 28 – 48

RESEARCH ARTICLE

Semisimple group codes and dihedral codes

Flaviana S. Dutra, Raul A. Ferraz and C. Polcino Milies

Communicated by guest editors

Abstract. We consider codes that are given as two-sided ideals in a semisimple finite group algebra $\mathbb{F}_qG$ defined by idempotents constructed from subgroups of G in a natural way and compute their dimensions and weights. We give a criterion to decide when these ideals are all the minimal two-sided ideals of $\mathbb{F}_qG$ in the case when G is a dihedral group and extend these results also to a family of quaternion group codes. In the final section, we give a method of decoding; i.e., of finding and correcting eventual transmission errors.

Dedicated to Professor Miguel Ferrero on occasion of his 70-th anniversary

1. Introduction

Let $\mathbb{F}_q$ denote a finite field with q elements. A *linear code* of length n over $\mathbb{F}_q$ is a subspace of $\mathbb{F}_q^n$. Given a finite group G of order n, the group algebra $\mathbb{F}_qG$ is a vector space over $\mathbb{F}_q$, with basis G and thus, isomorphic to $\mathbb{F}_q^n$ as a vector space. An important family of linear codes are the *cyclic codes* which are codes $C \subset \mathbb{F}_q^n$ such that if $(x_0, \ldots, x_{n-1}) \in C$ then also $(x_{n-1}, x_0, \ldots, x_{n-2}) \in C$. If we denote by $C_n = \langle a \rangle$ the cyclic group of order n, then it is easy to show that a code $C \subset \mathbb{F}_q^n$ is cyclic if and only if its image under the map $\mathbb{F}_q^n \to \mathbb{F}_qC_n$ given by $(x_0, \ldots, x_{n-1}) \mapsto \sum_{i=0}^{n-1} x_i a^i \in \mathbb{F}_qC_n$ is an ideal.

Research supported by FAPESP, Procs. 02/02933-0 and 00/07291-0 and CNPq Proc. 300243/79-0 (RN)

2000 Mathematics Subject Classification: *94B15, 94B60, 16S34, 20C05.*

Key words and phrases: *group code, minimal code, group algebra, idempotent, dihedral group, quaternion group.*

More generally, a *group code* over $\mathbb{F}_q$ is, by definition, an ideal of the group algebra $\mathbb{F}_q G$ of a finite group G (see, for example, [1], [2, section 4.8]).

We recall that the *support* of an element $\alpha = \sum_{g\in G} \alpha_g g$ in the group algebra FG of a group G over a field F is the set $supp(\alpha) = \{g \in G | a_g \neq 0\}$. The *Hamming distance* between two elements $\alpha = \sum_{g\in G} \alpha_g g$ and $\beta = \sum_{g\in G} \beta_g g$ in FG is

$$d(\alpha, \beta) = |\{g|\alpha_g \neq \beta_g, g \in G\}|$$

and the *weight* of an element α is $w(\alpha) = d(\alpha, 0) = |supp(\alpha)|$.

The *weight* or *minimum distance* of an ideal $I \subset FG$ is the number

$$w(I) = min\{w(\alpha)|\alpha \in FG, \alpha \neq 0\} = min\{|supp(\alpha)||\alpha \in FG, \alpha \neq 0\}.$$

If $char(\mathbb{F}_q) \nmid n$, then this group algebra is semisimple and thus every ideal is generated by an idempotent element. If H is a subgroup of G, then the element

$$\widehat{H} = \frac{1}{|H|} \sum_{h\in H} h$$

is an idempotent and it is central if and only if H is normal in G.

In the case of the rational group algebra of a finite abelian group G, it is known that the set of primitive idempotents of $\mathbb{Q}G$ is the set of all elements of the form

$$e = \widehat{H} - \widehat{H^*},$$

where H, H^* are pairs of subgroups of G such that $H \subset H^*$ and the quotient H^*/H is cyclic, together with the element $\widehat{G}$ which is called the *principal idempotent* of $\mathbb{Q}G$ [8, Theorem VII.1.4].

In [7] we gave necessary and sufficient conditions for this same formulas to describe the set of primitive idempotents of the group algebra of a finite abelian group over a finite field.

In section §2 we study ideals generated by idempotents of the form $e = \widehat{H} - \widehat{H^*}$, and by products of idempotents of this form, in group algebras of finite groups G over arbitrary fields F such that $char(F) \nmid |G|$. As an application, in the following section we give necessary and sufficient conditions for the semisimple group algebras of dihedral groups over a finite field to have a minimal number of simple components and in section §4 we describe the minimal central dihedral codes in this case. In section §5 we give necessary and sufficient conditions for the group algebras of dihedral and quaternion codes over finite fields to be isomorphic and thus obtain information on quaternion codes. In the final section, we describe decoding procedures for these kind of codes.

Our interest is mainly theoretical, since we wish to determine minimal codes. These turn out not to be *efficient* code as their minimal distance is comparatively small.

2. Ideals of Group Algebras

In what follows, we shall always assume that G is a finite group and $\mathbb{F}_q$ a finite field such that $char(\mathbb{F}_q) \nmid |G|$. As mentioned above, if H is a normal subgroup of G then

$$\widehat{H} = \frac{1}{|H|} \sum_{h \in H} h$$

is a central idempotent of $\mathbb{F}_q G$.

It is well-known [11, Proposition 3.6.7] that

$$(\mathbb{F}_q G) \cdot \widehat{H} \cong \mathbb{F}_q[G/H],$$

so

$$dim_{\mathbb{F}_q} \left((\mathbb{F}_q G) \cdot \widehat{H} \right) = [G : H].$$

Also, it is easy to see that if τ is a transversal of H in G, i.e. a complete set of representatives of cosets of H in G, then

$$\{t\widehat{H} | t \in \tau\}$$

is a basis of $(\mathbb{F}_q G) \cdot \widehat{H}$ over $\mathbb{F}_q$.

Hence, an element in such an ideal is of the form $\alpha = \sum_{t \in \tau} a_t t\widehat{H}$ which means that, when written in the basis G of $\mathbb{F}_q G$, it has the same coefficient along all the elements of the form th for a fixed $t \in \tau$ and any $h \in H$. Thus, this kind of ideals define repetition codes, which are not particularly interesting.

Now, we turn our attention to other kind of idempotents that will define more significant codes.

Proposition 2.1. *Let G be a finite group and F a field such that $char(F)$ does not divide $|G|$. Let H and H^* be normal subgroups of G such that $H \subset H^*$ and set $e = \widehat{H} - \widehat{H^*}$. Then:*

(i) $dim_F(FG)e = |G/H| - |G/H^*|$

(ii) $w((FG)e) = 2|H|$.

(iii) If $\mathcal{A}$ is a transversal of H^* in G and τ a transversal of H in H^* containing 1, then

$$\mathcal{B} = \{a(1-t)\widehat{H} | a \in \mathcal{A}, t \in \tau \setminus \{1\}\}$$

is a basis of $(\mathbb{F}_q G)e$ over $\mathbb{F}_q$.

Proof. Notice that $\widehat{H} = e + \widehat{H^*}$ and $e\widehat{H^*} = 0$ so $(FG)\widehat{H} = (FG)e \oplus (FG)\widehat{H^*}$; thus

$$dim_F(FG)\widehat{H} = dim_F(FG)e + dim_F(FG)\widehat{H^*}.$$

As $H \lhd G$ we have that $(FG)\widehat{H} \cong F(G/H)$ (see [11, Proposition 3.6.7]) so $dim_F(FG)\widehat{H} = |G/H|$, $dim_F(FG)\widehat{H^*} = |G/H^*|$ and the first result follows.

As $e\widehat{H} = (\widehat{H} - \widehat{H^*})\widehat{H} = \widehat{H} - \widehat{H^*}$, it follows that $(FG)e \subset (FG)\widehat{H}$. Let $\mathcal{T}$ be a transversal of $H \subset G$. An arbitrary element $\alpha \in FG$ can be written in the form $\alpha = \sum_{t\in\mathcal{T}} \alpha_t t$ with $\alpha_t \in FH$ so elements in the code are of the form $(\sum_{t\in\mathcal{T}} \alpha_t t)\widehat{H}$ with $a_t \in F$.

Notice that, if only one coefficient a_t were different from 0, we would have that $\widehat{H} \in (FG)e$, a contradiction. This shows that $w((FG)e) \geq 2|H|$.

On the other hand, if $h \in H^* \setminus H$, we have that

$$(1-h)e = (1-h)(\widehat{H} - \widehat{H^*}) = (1-h)\widehat{H}.$$

As $supp(\widehat{H}) \cap \mathrm{supp}(h\widehat{H}) = \emptyset$, we have that $w((1-h)e) = 2|H|$. Hence, $w((FG)e) = 2|H|$.

To prove (iii) we shall show first that the elements of $\mathcal{B}$ do belong to $(\mathbb{F}_qG)e$. In fact, since $(1-t)\widehat{H^*} = 0$, we have that

$$a(1-t)\widehat{H} = a(1-t)\widehat{H}(\widehat{H} - \widehat{H^*}) = a(1-t)\widehat{H}e \in (\mathbb{F}_qG)e.$$

Now, we shall show that the elements in $\mathcal{B}$ are linearly independent. So, assume that we have a linear combination over $\mathbb{F}_q$:

$$0 = \sum_{a,t} x_{at}(a(1-t)\widehat{H} = \sum_a \left(\sum_t x_{at}\right) a\widehat{H} - \sum_{a,t} x_{at} at\widehat{H}.$$

Notice that, for a fixed pair $a \in \mathcal{A}, t \in \tau$ the element $at\widehat{H}$ has a support that is disjoint with the support of every other element in this linear combination; hence, $x_{at} = 0$, for all $a \in \mathcal{A}, t \in \tau$.

On the other hand, we have that the cardinality of $\mathcal{B}$ is

$$\begin{aligned} |\mathcal{B}| &= |\mathcal{A}|\,(|\tau| - 1) = \left|\frac{G}{H^*}\right| \left(\left|\frac{H^*}{H}\right| - 1\right) \\ &= \left|\frac{G}{H}\right| - \left|\frac{G}{H^*}\right| = dim_{\mathbb{F}_q}(FG)e, \end{aligned}$$

and the proof is complete. □

We wish to extend the results of Proposition 2.1 to an ideal generated by a product of idempotents of the type under consideration. For the applications we have in mind, it will suffice to do so for a product of two idempotents, but the result extends easily, by induction.

Lemma 2.2. *Let $H_i \subset H_i^*$, be normal subgroups of a group $G, i = 1, 2$, such that $H_1^* \cap H_2^* = \{1\}$. Set $e = (\widehat{H_1} - \widehat{H_1^*})(\widehat{H_2} - \widehat{H_2^*})$. Then:*

(i) $dim_F(FG)e = \frac{|G|}{|H_1 H_2|}\left(1 - \frac{|H_1|}{|H_1^*|}\right)\left(1 - \frac{|H_2|}{|H_2^*|}\right)$

(ii) $w\left((FG)e\right) = 4|H_1 H_2|$.

(iii) If $\mathcal{A}$ is a transversal of H^* in G and τ_i a transversal of H_i in H_i^* containing 1, $i = 1, 2$. Then

$$\mathcal{B} = \{a(1 - t_1)(1 - t_2)\widehat{H} | a \in \mathcal{A}, t_i \in \tau_i, t_i \neq 1, i = 1, 2\}$$

is a basis of $(\mathbb{F}_q G)e$ over $\mathbb{F}_q$.

Proof. We compute

$$e = (\widehat{H_1} - \widehat{H_1^*})(\widehat{H_2} - \widehat{H_2^*}) = \widehat{H_1 H_2} - \widehat{H_1 H_2^*} - \widehat{H_1^* H_2} + \widehat{H_1^* H_2^*}.$$

If we set $f_1 = \widehat{H_1 H_2} - \widehat{H_1 H_2^*}$, $f_2 = \widehat{H_1^* H_2} - \widehat{H_1^* H_2^*}$ and $\mathcal{I} = (FG)e$, we see that $e = f_1 - f_2$ and that e and f_2 are orthogonal, so

$$dim_F \mathcal{I} = dim_F(FG)f_1 - dim_F(FG)f_2.$$

Also

$$dim_F(FG)f_1 = |G/H_1 H_2| - |G/H_1 H_2^*|$$

and

$$dim_F(FG)f_2 = |G/H_1^* H_2| - |G/H_1^* H_2^*|,$$

so

$$dim_F \mathcal{I} = \frac{|G|}{|H_1 H_2|}\left(1 - \frac{|H_1|}{|H_1^*|}\right)\left(1 - \frac{|H_2|}{|H_2^*|}\right).$$

To compute the weight of this code we consider elements $\gamma \in H_1^* \setminus H_1$ and $\delta \in H_2^* \setminus H_2$. We claim that $\alpha = (1 - \gamma)(1 - \delta)\widehat{H_1 H_2} \in \mathcal{I}$. In fact, we have

$$\begin{aligned} \alpha e_1 e_2 &= (1 - \gamma)(1 - \delta)\widehat{H_1 H_2}(\widehat{H_1} - \widehat{H_1^*})(\widehat{H_2} - \widehat{H_2^*}) \\ &= (1 - \gamma)(\widehat{H_1} - \widehat{H_1^*})(1 - \delta)(\widehat{H_2} - \widehat{H_2^*}) \\ &= (1 - \gamma)\widehat{H_1}(1 - \delta)\widehat{H_2} = \alpha, \end{aligned}$$

so $\alpha = \alpha e_1 e_2 \in \mathcal{I}$. Since $w(\alpha) = 4|H_1H_2|$ it follows that $w(\mathcal{I}) \leq 4|H_1H_2|$.

Let $\mathcal{T}$ be a transversal of H_1H_2 in G. Since $e = e\widehat{H_1H_2}$, any element $x \in \mathcal{I}$ can be written in the form

$$x = \sum_{t\in\mathcal{T}} a_t t\widehat{H_1H_2},$$

where $a_t \in F$. We claim that such an element $x \neq 0$ cannot be written as a sum with less than four terms. As in Lemma 2.1, it is easy to see that x cannot have only one coefficient different from 0. Assume, by way of contradiction, that we have in $\mathcal{I}$ an element of the form

$$x = (a_1t_1 + a_2t_2)\widehat{H_1H_2},$$

with $t_1 \neq t_2$. As $x = x(\widehat{H_1} - \widehat{H_1^*})$ we have

$$(a_1t_1 + a_2t_2)\widehat{H_1^*H_2} = 0.$$

Since $t_1H_1^*H_2$ and $t_2H_1^*H_2$ are cosets of $H_1^*H_2$ they are either equal or disjoint. Hence, we must have $t_1H_1^*H_2 = t_2H_1^*H_2$ and there exist elements $h_1^* \in H_1^*$ and $h_2 \in H_2$ such that $t_1 = t_2h_1^*h_2$. In a similar way, multiplying by $\widehat{H_2} - \widehat{H_2^*}$ we see that there exist elements $h_1 \in H_1$ and $h_2^* \in H_2^*$ such that $t_1 = t_2h_1h_2^*$. This clearly implies that $h_1^*h_1^{-1} = h_2^{-1}h_2^* \in H_1^* \cap H_2^* = \{1\}$. So $h_1^* \in H_1$, $h_2^* \in H_2$ and $t_1H_1H_2 = t_2H_1H_2$, a contradiction.

Finally, if $x = (a_1t_1 + a_2t_2 + a_3t_3)\widehat{H_1H_2}$, multiplying by $\widehat{H_1} - \widehat{H_1^*}$ and by $\widehat{H_2} - \widehat{H_2^*}$ we get $(a_1t_1 + a_2t_2 + a_3t_3)\widehat{H_1^*H_2} = 0$ and $(a_1t_1 + a_2t_2 + a_3t_3)\widehat{H_1H_2^*} = 0$ respectively. Then, it is easy to conclude, as before, that $t_1H_1H_2 = t_2H_1H_2 = t_3H_1H_2$, a contradiction.

The proof of (iii) is very similar to that of part (iii) in Proposition 2.3. As

$$\begin{aligned} a(1-t_1)(1-t_2)\widehat{H}(\widehat{H_1} - \widehat{H_1^*})(\widehat{H_2} - \widehat{H_2^*}) &= \\ = a\widehat{H}(1-t_1)(\widehat{H_1} - \widehat{H_1^*})(1-t_2)(\widehat{H_2} - \widehat{H_2^*}) &= \\ = a\widehat{H}(1-t_1)\widehat{H_1}(1-t_2)\widehat{H_2} = a(1-t_1)(1-t_2)\widehat{H}, & \end{aligned}$$

it follows that $\mathcal{B} \subset (\mathbb{F}_qG)e$.

To prove that the elements of $\mathcal{B}$ are linearly independent assume, as before, that there exists a linear combination

$$\begin{aligned} 0 &= \sum_{a,t_1,t_2} x_{at_1t_2}a(1-t_1)(1-t_2)\widehat{H} = \\ &= \sum_{a}\left(\sum_{t_1t_2} x_{at_1t_2}\right)a\widehat{H} - \sum_{t_2}\sum_{a,t_1} x_{at_1t_2}at_1\widehat{H} \end{aligned}$$

$$-\sum_{t_1}\sum_{a,t_2} x_{at_1t_2}at_2\widehat{H} + \sum_{a,t_1,t_2} x_{at_1t_2}at_1t_2\widehat{H}.$$

Clearly, the support of the elements of the form $at_1t_2\widehat{H}$ are disjoint with the support of every other element in this sum, so we get that $x_{at_1t_2} = 0$ for all $a \in \mathcal{A}, t_i \in \tau_i, i = 1, 2$.

Finally, notice that the number of elements in $\mathcal{B}$ is

$$\begin{aligned}|\mathcal{B}| &= \frac{|G|}{|H_1^*H_2^*|}\left(\frac{|H_1^*|}{|H_1|} - 1\right)\left(\frac{|H_2^*|}{|H_2|} - 1\right)\\ &= \frac{|G|}{|H_1H_2|}\left(1 - \frac{|H_1|}{|H_1^*|}\right)\left(1 - \frac{|H_2|}{|H_2^*|}\right)\\ &= dim_{\mathbb{F}_q}(\mathbb{F}_qG)e.\end{aligned}$$

□

An easy induction now proves the first two statements of the following.

Proposition 2.3. *Let $H_i \subset H_i^*$, be normal subgroups of a group $G, 1 \leq i \leq k$, such that $H_i^* \cap N_i^* = \{1\}$, where N_i denotes the subgroup generated by all H_j^* with $j \neq i$. Set $e = (\widehat{H_1} - \widehat{H_1^*})(\widehat{H_2} - \widehat{H_2^*})\cdots(\widehat{H_k} - \widehat{H_k^*})$. Then,*

(i) $dim_F(FG)e = \frac{|G|}{|H_1H_2\cdots H_k|}\left(1 - \frac{|H_1|}{|H_1^*|}\right)\left(1 - \frac{|H_2|}{|H_2^*|}\right)\cdots\left(1 - \frac{|H_k|}{|H_k^*|}\right)$

(ii) $w\left((FG)e\right) = 2^k|H_1H_2\cdots H_k|$.

(iii) If $\mathcal{A}$ is a transversal of H^* in G and τ_i a transversal of H_i in H_i^* containing 1, $1 \leq i \leq k$. Then, the set $\mathcal{B} =$

$$\{a(1-t_1)(1-t_2)\cdots(1-t_k)\widehat{H} | a \in \mathcal{A}, t_i \in \tau_i, t_i \neq 1\}$$

is a basis of $(\mathbb{F}_qG)e$ over $\mathbb{F}_q$.

If $e_1, \ldots, e_n$ are central idempotents in a ring R and we set $e = e_1\cdots e_k$, it is easy to see that $Re = Re_1 \cap \cdots \cap Re_k$. Since $\Delta(G : H^*) = (\mathbb{F}_qG)(1 - \widehat{H^*})$ (see [11, Proposition 3.6.7]) and $\widehat{H}(1 - \widehat{H^*}) = \widehat{H} - \widehat{H^*} = e$ we see immediately that

$$(\mathbb{F}_qG)e = (\mathbb{F}_qG)\widehat{H} \cap \Delta(G : H^*).$$

Also, if $H_i \subset H_i^*$, are normal subgroups of a group $G, 1 \leq i \leq k$, and we set $e = \prod_{i=1}^k(\widehat{H_i} - \widehat{H_i^*})$, it follows easily, by induction, that:

$$(\mathbb{F}_qG)e = \left(\cap_{i=1}^k(\mathbb{F}_qG)\widehat{H_i}\right) \cap \left(\cap_{i=1}^k\Delta(G : H_i^*)\right).$$

3. Semisimple dihedral group algebras

Let $\mathbb{F}_q$ be a finite field with q elements and let D_n be the dihedral group of order $2n$, i.e.

$$D_n = \langle a, b | a^n = b^2 = 1, bab = a^{-1} \rangle.$$

We shall assume throughout that $char(\mathbb{F}_q)$ does not divide $2n$. It was shown in [7] that, for an arbitrary semisimple group algebra FG of a finite group G, the number of simple components of FG is greater or equal to the number of simple components of $\mathbb{Q}G$, where $\mathbb{Q}$ denotes the field of rational numbers. We shall determine conditions on q and n for F_qD_n to have minimum number of simple components, i.e., to have precisely the same number of simple components as $\mathbb{Q}G$. To do so, we will first determine the structure of $\mathbb{Q}D_n$.

We begin by exhibiting the primitive central idempotents of the algebra $\mathbb{Q}\langle a \rangle$. Let $n = p_1^{n_1} \cdots p_t^{n_t}$. According to [8, Theorem VII.1.4] these are elements of the form

$$\epsilon_1 \epsilon_2 \dots \epsilon_t,$$

with either

$$\epsilon_i = \widehat{\langle a^{n/p_i^{n_i}} \rangle} \quad \text{or} \quad \epsilon_i = \widehat{K_i} - \widehat{H_i}, \tag{1}$$

where K_i and H_i are all the p_i-subgroups of $\langle a \rangle$ such that $K_i \subset H_i$ and $|H_i/K_i| = p_i$ for $1 \leq i \leq t$.

Let $L_i = supp(\epsilon_i)$, $1 \leq i \leq t$. Then $\langle L_1 \times \cdots \times L_t \rangle = \langle a^m \rangle$, a subgroup of $\langle a \rangle$ and it is easy to see that every such subgroup correspondes to exactly one of the idempotents above. So, each idempotents corresponds to precisely one divisor d of n and shall be denoted by e_d.

Since every subgroup of $\langle a \rangle$ is normal in D_n, it follows that the idempotents $e_d, d|n$, are central in $\mathbb{Q}D_n$.

We can write the idempotent $e_1 = \widehat{\langle a \rangle}$ as the sum of the idempotents:

$$e_{11} = \frac{1+b}{2} e_1 \quad \text{and} \quad e_{12} = \frac{1-b}{2} e_1 \tag{2}$$

and, when n is even, we also write the idempotent e_2 as the sum of:

$$e_{21} = \frac{1+b}{2} e_2 \quad \text{and} \quad e_{22} = \frac{1-b}{2} e_2. \tag{3}$$

A straightforward computation shows that $\{e_{11}, e_{12}\} \cup \{e_d | d|n, d \neq 1\}$ and $\{e_{11}, e_{12}, e_{21}, e_{22}\} \cup \{e_d | d \neq 1, 2\}$ are sets of pairwise orthogonal central idempotents whose sums are equal to 1.

To prove that these are the sets of primitive central idempotents, we shall compute the number of simple components of $\mathbb{Q}D_n$.

Let G be a group, F any field such that $char(F) \nmid |G|$ and e the exponent of G. Let ζ be a primitive e^{th} root of unity. For each element θ in $Gal(F(\zeta), F)$ we have that $\zeta^\theta = \zeta^r$ for some positive integer r, and we define an action of θ on G by $g^\theta = g^r$, for all $g \in G$. We note that, if Γ_g is the class sum of the class of an element g, then $\Gamma_g^\theta = \Gamma_{g^\theta}$. Two conjugacy classes of G are said to be F-conjugate if they correspond under this action.

The Theorem of Witt-Berman [4, Theorems 21.5 and 21.25] shows that the number of simple components of the group algebra FD_n equals the number of F-conjugate classes of D_n (for a proof in purely group ring theoretical terms, see [5]).

The conjugacy classes of D_n are:

$$\{1\},\ \{a, a^{-1}\}, \ldots \{a^{\frac{n-1}{2}}, a^{-\frac{n+1}{2}}\},\ \{b, ab, \ldots, a^{n-1}b\},$$

if n is odd, and

$$\{1\}, \{a, a^{-1}\}, \ldots \{a^{\frac{n-2}{2}}, a^{-\frac{n+2}{2}}\}, \{a^{\frac{n}{2}}\}$$

$$\{b, a^2b, \ldots, a^{n-2}b\}, \{ab, a^3b, \ldots, a^{n-1}b\},$$

if n is even, so we set

$$A_0 = 1, \quad A_i = a^i + a^{-i},\ 1 \leq i \leq \frac{n-1}{2}, \quad B = \sum_{j=0}^{n-1} a^j b,$$

and

$$\mathcal{B} = \{A_0, A_1, \ldots, A_{\frac{n-1}{2}}, B\}$$

if n is odd and

$$A_0 = 1, \quad A_i = a^i + a^{-i},\ 1 \leq i \leq \frac{n-2}{2}, \quad A_{\frac{n}{2}} = a^{\frac{n}{2}}$$

and

$$B_0 = \sum_{j=0}^{\frac{n-2}{2}} a^{2j} b, \quad B_1 = \sum_{j=0}^{\frac{n-2}{2}} a^{2j+1} b,$$

and

$$\mathcal{B} = \{A_0, A_1, \ldots, A_{\frac{n-2}{2}}, A_{\frac{n}{2}}, B_0, B_1\}$$

if n is even.

With this notation, the number of simple components of FD_n is the number of orbits of elements in $\mathcal{B}$ under the action of $Gal(F(\zeta), F)$.

Let e be the exponent of D_n; i.e., $e = 2n$ if n is odd and $e = n$ if n is even. The group $Gal(\mathbb{Q}(\zeta), \mathbb{Q})$ is isomorphic to the group of units $U(\mathbb{Z}_n) \cong U(\mathbb{Z}_e)$. Hence, two elements of the form a^i and a^j are $\mathbb{Q}$-conjugates if and only if there exists an integer r, such that $gcd(r, n) = 1$ and $j \equiv ir \pmod{n}$; i.e., if and only if $gcd(i, n) = gcd(j, n)$. So, the conjugacy class of an element A_i in $\mathcal{B}$ is

$$\mathcal{A}_i = \{A_j | gcd(i, n) = gcd(j, n)\}.$$

In particular, if $gcd(i, n) = d$ we have that $\mathcal{A}_i = \mathcal{A}_d$ and the number of $\mathbb{Q}$-classes containing elements of this form is equal to the number of divisors of n, which we shall denote by $d(n)$.

Consequently, the number of $\mathbb{Q}$-classes, and thus of simple components of $\mathbb{Q}D_n$, is $d(n) + 1$ if n is odd and $d(n) + 2$ if n is even. Since this number coincides with the number of orthogonal central idempotents found above, we have shown the following, which is implicit in [9, p. 230].

Theorem 3.1. *The set of primitive central idempotents of the group algebra $\mathbb{Q}D_n$ is*

$$\{e_{11}, e_{12}\} \cup \{e_d | d | n, d \neq 1\} \quad \textit{if } n \textit{ is odd,}$$

and

$$\{e_{11}, e_{12}, e_{21}, e_{22}\} \cup \{e_d | d \neq 1, 2\} \quad \textit{if } n \textit{ is even.}$$

Notice that expressions on equations (1), (2) and (3) also define idempotents over a finite field $\mathbb{F}_q$, which are pairwise orthogonal and add up to 1. To decide whether these are, in fact, the primitive central idempotents of $\mathbb{F}_q D_n$ we must determine when they are as many as the number of simple components of this algebra. In view of Theorem 3.1, this is equivalent to decide when $\mathbb{Q}D_n$ and $\mathbb{F}_q D_n$ have the same number of simple components. We shall determine conditions on n for this to happen.

Lemma 3.2. *Let $\mathbb{F}_q$ be a finite field and let ζ be an e^{th}-root of unity, where e is the exponent of D_n. Then, the number of simple components of $\mathbb{F}_q D_n$ equals the number of simple components of $\mathbb{Q}D_n$ if and only if, denoting by $\overline{q}$ the residue class of q in $\mathbb{Z}_n$, we have that either $\langle \overline{q} \rangle = U(\mathbb{Z}_n)$ or $\langle \overline{q} \rangle$ is a subgroup of index 2 in $U(\mathbb{Z}_n)$ and $-\overline{1} \notin \langle \overline{q} \rangle$.*

Proof. Set $q = |\mathbb{F}_q|$. We recall that $Gal(\mathbb{F}_q(\zeta), \mathbb{F}_q)$ is a cyclic group, generated by the Frobenius automorphism $\zeta \mapsto \zeta^q$.

Assume first that n is odd. Clearly, A_0 and B are fixed under the action of $Gal(\mathbb{F}_q(\zeta), \mathbb{F}_q)$. The orbit of A_i is

$$\mathcal{S}_i = \{a^i + a^{-i}, a^{iq} + a^{-iq}, a^{iq^2} + a^{-iq^2}, \ldots, a^{iq^{s-1}} + a^{-iq^{s-1}}\},$$

where s is the least positive integer such that $a^{iq^s} = a^i$.

Set

$$\mathcal{A}_i = \{A_r | gcd(r,n) = gcd(i,n)\}.$$

Clearly, $\mathcal{S}_i \subset \mathcal{A}_i$. So, the number of simple components of $\mathbb{F}_q D_n$ equals the number of simple components of $\mathbb{Q}D_n$ if and only if $\mathcal{S}_i = \mathcal{A}_i$ for all indexes i. A similar argument holds if n is even.

Assume now that $\mathcal{S}_i \subset \mathcal{A}_i$ for all indeces i. Hence, in particular

$$\mathcal{S}_1 \subset \mathcal{A}_1 = \{A_r | gcd(r,n) = 1\}.$$

So, for each r coprime with n we have that $a^r + a^{-r} = a^{q^t} + a^{-q^t}$ for some positive integer t. This means that either $a^r = a^{q^t}$ or $a^r = a^{-q^t}$. This shows that, given any element $\overline{r} \in \mathbb{Z}_n$ we have that either $\overline{r} \in \langle \overline{q} \rangle$ or $-\overline{r} \in \langle \overline{q} \rangle$; thus $[U(\mathbb{Z}_n) : \langle \overline{q} \rangle] \leq 2$, as stated. We still need to prove that $-\overline{1} \notin \langle \overline{q} \rangle$ when $\langle \overline{q} \rangle \neq U(\mathbb{Z}_n)$. Since for each r coprime with n either $\overline{r}$ or $-\overline{r}$ is in $\langle \overline{q} \rangle$, if $-\overline{1}$ were in this group, we would have $\langle \overline{q} \rangle = U(\mathbb{Z}_n)$, a contradiction.

Conversely, first we notice that if $\langle \overline{q} \rangle = U(\mathbb{Z}_n)$, then clearly $\mathcal{S}_1 = \mathcal{A}_1$. So, assume that $\langle \overline{q} \rangle$ is a subgroup of index 2 in $U(\mathbb{Z}_n)$ and $-\overline{1} \notin \langle \overline{q} \rangle$.

Since $-1 \notin \langle \overline{q} \rangle$ we have that either $\overline{r} \in \langle \overline{q} \rangle$ or $-\overline{r} \in \langle \overline{q} \rangle$ for each r such that $gcd(r,n) = 1$, which shows that $\mathcal{S}_1 = \mathcal{A}_1$.

If d is a divisor of n, we shall denote by q^* the congruence class of q in $U(\mathbb{Z}_{n/d})$. Since $U(\mathbb{Z}_n) = \langle \overline{q} \rangle \cup \langle -\overline{q} \rangle$, the natural projection shows that $U(\mathbb{Z}_{n/d}) = \langle q^* \rangle \cup \langle -q^* \rangle$. Hence, for every positive integer r such that $gcd(r,n) = d$ we have that $(r/d)^* \in U(\mathbb{Z}_{n/d})$ so one of $\pm r/d$ is in $\langle q^* \rangle$ and there exist integers t, j such that $r/d = \pm q^j + t(n/d)$ so $a^{r/d} = a^{\pm q^j} . a^{t(n/d)}$ and taking d-powers, we obtain that $a^r = a^{\pm dq^j}$. This shows that also $\mathcal{S}_d = \mathcal{A}_d$. □

Theorem 3.3. *The number of simple components of $\mathbb{F}_q D_n$ and $\mathbb{Q}D_n$ are equal if and only if one of the following conditions holds:*

(i) $n = 2$ *or* 4 *and* q *is odd.*

(ii) $n = 2^m$, *with* $m \geq 3$ *and* q *is congruent to either* 3 *or* 5, *modulo* 8.

(iii) $n = p^m$ *with* p *an odd prime and the class* $\overline{q}$ *is a generator of the group* $\mathcal{U}(\mathbb{Z}_{p^m})$.

(iv) $n = p^m$ *with* p *an odd prime, the class* $\overline{q}$ *is a generator of the group* $\mathcal{U}^2(\mathbb{Z}_{p^m}) = \{x^2 | x \in \mathcal{U}(\mathbb{Z}_{p^m}\}$ *and* -1 *is not a square modulo* p^m.

(v) $n = 2p^m$ *with* p *an odd prime and the class* $\overline{q}$ *is a generator of the group* $\mathcal{U}(\mathbb{Z}_{2p^m})$.

(vi) $n = 2p^m$ *with* p *an odd prime, the class* $\overline{q}$ *is a generator of the group* $\mathcal{U}^2(\mathbb{Z}_{p^m}) = \{x^2 | x \in \mathcal{U}(\mathbb{Z}_{2p^m}\})$ *and* -1 *is not a square modulo* $2p^m$.

(vii) $n = 4p^m$ *with* p *an odd prime and both* q *and* $-q$ *have order* $\varphi(p^m)$ *modulo* $4p^m$.

(viii) $n = p_1^{m_1}p_2^{m_2}$ *with* p_1, p_2 *odd primes,* $(\varphi(p_1^{m_1}), \varphi(p_2^{m_2})) = 2$ *and both* q *and* $-q$ *have order* $\varphi(p_1^{m_1})\varphi(p_2^{m_2})/2$ *modulo* $p_1^{m_1}p_2^{m_2}$.

(ix) $n = 2p_1^{m_1}p_2^{m_2}$ *with* p_1, p_2 *odd primes,* $(\varphi(p_1^{m_1}), \varphi(p_2^{m_2})) = 2$ *and both* q *and* $-q$ *have order* $\varphi(p_1^{m_1})\varphi(p_2^{m_2})/2$ *modulo* $p_1^{m_1}p_2^{m_2}$.

Proof. Assume that the number of simple components of $\mathbb{F}_q D_n$ and $\mathbb{Q}D_n$ are equal. Then, according to the previous lemma, the order of $\overline{q}$ in $U(\mathbb{Z}_n)$ must be equal to either $\varphi(n)$ or $\varphi(n)/2$, where φ denotes Euler's Totient function and, in the second case, we must also have that $-\overline{1} \notin \langle\overline{q}\rangle$.

Let $n = 2^m p_1^{m_1} \cdots p_t^{m_t}$, be the decomposition of n into prime factors, with $m \geq 0$. Then

$$\mathbb{Z}_n \cong \mathbb{Z}_{2^m} \oplus \mathbb{Z}_{p_1^{m_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{m_t}}$$

and

$$U(\mathbb{Z}_n) \cong U(\mathbb{Z}_{2^m}) \times U(\mathbb{Z}_{p_1^{m_1}}) \times \cdots \times U(\mathbb{Z}_{p_t^{m_t}}).$$

The group $U(\mathbb{Z}_{2^m})$ is cyclic if and only if $m \leq 2$ and, in the case when $m > 2$, then it is isomorphic to $C_{2^{m-2}} \times C_2$ [10, Theorem 2.43]. Each direct factor $U(\mathbb{Z}_{p_i^{m_i}})$ is cyclic if and only if p_i is odd [10, Theorem 2.41].

We shall divide our proof in several cases.

(*a*) *The order of* $\overline{q}$ *in* $U(\mathbb{Z}_n)$ *is equal to* $\varphi(n)$. In this case, $U(\mathbb{Z}_n)$ is cyclic and thus contains only one subgroup of order 2. Since $\varphi(p_i^{m_i})$ is even any factor of the form $U(\mathbb{Z}_{p_i}^{m_i})$ contains a subgroup of order 2. So either n is of the form $n = 2^m$ with $m = 1$ or 2, or then $t = 1$ with $m = 0$ or 1; i.e. $n = 2, 4, p^m$ or $2p^m$. In these cases, either (i), (iii) or (v) holds. Notice that, in the case when $n = 4$ we must have $q \equiv 3 \pmod 4$.

(*b*) *The order of* $\overline{q}$ *in* $U(\mathbb{Z}_n)$ *is equal to* $\varphi(n)/2$ *and* $U(\mathbb{Z}_n)$ *is cyclic.* Since the only subgroup of index 2 in a cyclic group is the subgroup of all squares, we see that (iv) or (vi) follows and also (i) in the case when $n = 4$ and $q \equiv 1 \pmod 4$.

(*c*) *The order of* $\overline{q}$ *in* $U(\mathbb{Z}_n)$ *is equal to* $\varphi(n)/2$ *and* $U(\mathbb{Z}_n)$ *is not cyclic.* Notice that, in this case, the exponent of $U(\mathbb{Z}_n)$ is precisely $\varphi(n)/2$, so this group contains a direct cyclic factor of that order and as $\varphi(n)/2 = |U(\mathbb{Z}_n)|/2$ then $U(\mathbb{Z}_n) \cong C_{\varphi(n)/2} \times C_2$. Hence, the maximal elementary abelian 2-groups are of the form $C_2 \times C_2$.

Since every factor of the form $U(\mathbb{Z}_{p_i^{m_i}})$, with p_i odd, has even order, the decomposition of $U(\mathbb{Z}_n)$ above can have at most two of these factors, so either $n = 2^m$, $n = 4p^m$, $n = p_1^{m_1}p_2^{m_2}$, or $n = 2p_1^{m_1}p_2^{m_2}$. We shall study separately these cases.

$(c-(i))$ $n = 2^m$. Notice that [10, Theorem 2.43] actually gives a decomposition of $U(\mathbb{Z}_{2^m})$ as

$$U(\mathbb{Z}_{2^m}) = \langle -\overline{1}\rangle \times \langle \overline{5}\rangle.$$

In this group, there are only two cyclic subgroups of index 2, namely $\langle\overline{5}\rangle$ and $\langle -\overline{5}\rangle$, so $\overline{q}$ is congruent to $\pm 5^r \pmod{2^m}$, for some odd positive integer r, with $m > 2$, and hence also to $\pm 5^r \pmod 8$. Writing $r = 2k+1$ we have:

$$q \equiv (\pm 5)^{2k}(\pm 5) \equiv \pm 5 \pmod 8.$$

Hence, $q \equiv 3$ or $5 \pmod 8$ and (ii) follows.

$(c-(ii))$ $n = 4p^m$. As $\varphi(4p^m) = 2\varphi(p^m)$ we have that (vii) follows immediately.

$(c-(iii))$ $n = p_1^{m_1}p_2^{m_2}$. Since $|U(\mathbb{Z}_n)| = \varphi(p_1^{m_1})\varphi(p_2^{m_2})$ we readily see that the order of $\overline{q}$ modulo $p_1^{m_1}p_2^{m_2}$ is $\varphi(p_1^{m_1})\varphi(p_2^{m_2})/2$ and, as $-\overline{1} \notin \langle\overline{q}\rangle$, it is also the order of $-\overline{q}$, so $(viii)$ follows.

$(c-(iv))$ $n = 2p_1^{m_1}p_2^{m_2}$. In this case, (ix) follows, as above.

Now, we note that if (i) holds and $q \equiv 3 \pmod 4$ holds, the considerations in (a) show that the converse holds in this case. If $q \equiv 1 \pmod 4$, the arguments in (b) show that the converse holds also in this case.

Assume that (ii) holds. Since, as mentioned in $(c-(i))$, for $m \geq 3$ we have that $U(\mathbb{Z}_{2^m}) = \langle\overline{5}\rangle \times \langle -\overline{1}\rangle$ and thus also $U(\mathbb{Z}_{2^m}) = \langle -\overline{5}\rangle \times \langle -\overline{1}\rangle$, we have that $o(\overline{5}) = o(-\overline{5}) = 2^{m-2}$ and hence every element in $U(\mathbb{Z}_{2^m})$ is of the form $\overline{5}^{2i}, \overline{5}^{2i+1}, -\overline{5}^{2i}$ or $-\overline{5}^{2i+1}$, for some positive integer i. Also, we have

$$\begin{aligned} \overline{5}^{2i} &\equiv 1 \pmod 8, & \overline{5}^{2i+1} &\equiv 5 \pmod 8,\\ -\overline{5}^{2i} &\equiv 7 \pmod 8, & -\overline{5}^{2i+1} &\equiv 3 \pmod 8. \end{aligned}$$

So, if $q \equiv 3$ or $5 \pmod 8$ we have that $q \equiv \overline{5}^{2i+1}$ or $-\overline{5}^{2i+1} \pmod{2^m}$ and thus $\langle\overline{q}\rangle = \langle\overline{5}\rangle$ or $\langle\overline{q}\rangle = \langle -\overline{5}\rangle$. Then clearly $-\overline{1} \notin \langle\overline{q}\rangle$ and the converse holds.

If one of $(iii), (iv), (v)$ or (vi) holds, then the converse follows directly from Lemma 3.2.

Assume (vii) holds. If $n = 4p^m$ with p an odd prime then $U(\mathbb{Z}_n) \cong C_2 \times C_{\varphi(p^m)}$. Since in (vii) we assume that $o(\overline{q}) = \varphi(p^m)$ it is clear that this element generates a subgroup of index 2. We must show that $-\overline{1} \notin \langle \overline{q} \rangle$. Assume, by way of contradiction, that $-\overline{1} \in \langle \overline{q} \rangle$. Since this group is cyclic, of order $\varphi(p^m)$ and $o(-\overline{1}) = 2$ we must have $-\overline{1} = \overline{q}^{\varphi(p^m)/2}$.

If the exponent were odd, we would have

$$(-\overline{q})^{\varphi(p^m)/2} = (-\overline{1})^{\varphi(p^m)/2}\overline{q}^{\varphi(p^m)/2} = \overline{1},$$

contradicting the fact that $o(-\overline{q}) = \varphi(p^m)$. So, $\varphi(p^m)/2$ is even and, since q is odd, we have $q^{\varphi(p^m)/2} \equiv 1 \pmod 4$, so $q^{\varphi(p^m)/2}$ is not congruent to $-1 \pmod{4p^m}$, as desired.

Assume now that either $(viii)$ or (ix) holds. In both cases, $U(\mathbb{Z}_n) \cong C_{\varphi(p_1^{m_1})} \times C_{\varphi(p_2^{m_2})}$ so $\langle \overline{q} \rangle$ is a subgroup of index 2 (notice that $C_{\varphi(p_1^{m_1})} \times C_{\varphi(p_2^{m_2})}$ contains a cyclic group of index 2 if and only if $\gcd(\varphi(p_1^{m_1}), \varphi(p_2^{m_2})) = 2$, so this condition is implicit in our hypotheses).

As in the previous case, it suffices to show that $-\overline{1} \notin \langle \overline{q} \rangle$ and the proof is the same as above, taking into account that, in this case, if $-\overline{1} \in \langle \overline{q} \rangle$ we would have $-\overline{1} = \overline{q}^r$ with $r = \frac{\varphi(p_1^{m_1})\varphi(p_2^{m_2})}{2}$. □

4. Dihedral codes

We recall that a **dihedral (central) code** over a finite field F is any ideal I in the group algebra FD_n of a dihedral group D_n. A **minimal dihedral code** is an ideal I which is minimal in the set of all ideals of $\mathbb{F}_q D_n$; i.e., generated by a primitive central idempotent.

In this section, we shall determine the dimensions and weights of minimal dihedral codes in the cases described in Theorem 3.3.

We recall that, according to Theorems 3.1 and 3.3, the idempotents determining these codes are

$$\{e_{11}, e_{12}\} \cup \{e_d | d|n, d \neq 1\} \quad \text{if } n \text{ is odd,}$$

and

$$\{e_{11}, e_{12}, e_{21}, e_{22}\} \cup \{e_d | d|n, d \neq 1, 2\} \quad \text{if } n \text{ is even.}$$

where the idempotents of the form e_d, $d|n$ are as described in formula (1).

Lemma 4.1. *Let F a field such that $char(F) \nmid |D_n|$. For $1 \leq i, j \leq 2$ we have*

$$dim_F(FD_n)e_{ij} = 1$$

and

$$w[(FD_n)e_{ij}] = 2n.$$

Proof. Notice that

$$FD_n\widehat{a} \cong F\langle b\rangle = (F\langle b\rangle)\frac{1+b}{2} \oplus (F\langle b\rangle)\frac{1-b}{2} \cong F \oplus F.$$

So,

$$(dim_F(FD_n)\frac{1+b}{2}\widehat{a} = (dim_F(FD_n)\frac{1-b}{2}\widehat{a} = 1.$$

If n is even, if we denote by $\overline{a}$ and $\overline{b}$ the images of a and b in $D_n/\langle a^2\rangle$, we have that

$$(FD_n)\widehat{a^2} \cong F(\langle\overline{b}\rangle \times \langle\overline{a}\rangle) \cong F \oplus F \oplus F \oplus F \oplus F.$$

The principal idempotents of $F(\langle\overline{b}\rangle \times \langle\overline{a}\rangle)$ are

$$\frac{1+\overline{b}}{2}\cdot\frac{1+\overline{a}}{2} \qquad \frac{1-\overline{b}}{2}\cdot\frac{1+\overline{a}}{2}$$
$$\frac{1+\overline{b}}{2}\cdot\frac{1-\overline{a}}{2} \qquad \frac{1-\overline{b}}{2}\cdot\frac{1-\overline{a}}{2}$$

The corresponding idempotents in FD_n are

$$\left(\frac{1+b}{2}\cdot\frac{1+a}{2}\right)\widehat{a^2} = e_{11} \quad \left(\frac{1-b}{2}\cdot\frac{1+a}{2}\right)\widehat{a^2} = e_{12}$$
$$\left(\frac{1+b}{2}\cdot\frac{1-a}{2}\right)\widehat{a^2} = e_{21} \quad \left(\frac{1-b}{2}\cdot\frac{1-a}{2}\right)\widehat{a^2} = e_{22}$$

and the result follows.

Since the code generated by one of the idempotents $e_{ij}, 1 \leq i, j \leq 2$ is of dimension 1, elements of the code differ in a scalar multiple of e_{ij} and, as $supp(e_{ij}) = D_n$, so our claim follows. □

In what follows, we shall compute the parameters of the minimal ideals generated by all the other principal idempotents, different from the ones given above.

In Table 1.1, we describe the dimensions and weights of minimal central codes in the case when n involves only one prime.

In the case when n is of the form $n = p_1^{m_1}\cdots p_t^{m_t}$ the cyclic group $\langle a\rangle$ of order n is a direct product of cyclic groups C_i of orders $p_i^{m_i}, 1 \leq i \leq t$, and the primitive idempotents e of $F\langle a\rangle$ are products of the form $e = e_1\cdots e_t$ where each e_i is a primitive idempotent of $FC_i, 1 \leq i \leq t$. Taking this fact into account, there is an easy way to compute weights and dimensions in some of the cases under consideration.

n	e	$dim[FD_n)e]$	$w[(FD_n)e]$
4	$1-a^2$	4	2
2^m	$e_{2^i} = \widehat{C_{2^i}} - \widehat{C_{2^{i+1}}}$	2^{m-i}	2^{i+1}
p^m	$e_{p^i} = \widehat{C_{p^i}} - \widehat{C_{p^{i+1}}}$	$2\varphi(p^{m-i})$	$2p^i$

Table 1.1.

Lemma 4.2. *Assume that $n = p_1^{m_1}p_2^{m_2}$ where p_1, p_2 are different primes. Let $e_i(1) = \widehat{H_1} - \widehat{H_1^*}$ be an idempotent of $F\langle a^{p_2^{m_2}}\rangle$, the algebra of the group of order $p_1^{m_1}$ corresponding to the subgroup H_1 of order p_1^i and, similarly, let $e_j(2) = \widehat{H_2} - \widehat{H_2^*}$ be an idempotent of $F\langle a^{p_1^{m_1}}\rangle$ corresponding to a subgroup H_2 of order p_2^j. Then*

$$dim_K[FD_n]e_i(1)e_j(2) = 2\varphi(p_1^{m_1-i})\varphi(p_2^{m_2-j}).$$

$$w\left([FD_n]e(1)e(2)\right) = 4|H_1H_2|.$$

Proof. We know, from Lemma 2.2 that:

$$\begin{aligned} &dim_K[FD_n]e_i(1)e_j(2) = \\ &= \frac{|G|}{|H_1H_2|}\left(1-\frac{|H_1|}{|H_1^*|}\right)\left(1-\frac{|H_2|}{|H_2^*|}\right) \\ &= 2p_1^{m_1-i}p_2^{m_2-j}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \\ &= 2\varphi(p_1^{m_1-i})\varphi(p_2^{m_2-j}). \end{aligned}$$

The value of the weight follows directly from Lemma 2.1. □

Using the information above we give, in Table 1.2, the idempotents and corresponding dimensions and weights of the ideals they generate in the case when n involves two different primes. To simplify notations, we shall denote by C_k the cyclic subgroup of $\langle a\rangle$ of order k.

Finally, in Table 1.3 we consider the case when $n = 2p_1^{m_1}p_2^{m_2}$.

5. Quaternion codes

In this section, we shall consider group algebras of generalized quaternion groups $\mathcal{Q}_n$ with n even; i.e, groups given by the presentation:

$$\mathcal{Q}_n = \langle \alpha, \beta | \alpha^n = 1 \beta^2 = \alpha^{n/2}, \beta^{-1}\alpha\beta = \alpha^{-1}\rangle$$

n			$dim[\mathcal{I}]$	$w[\mathcal{I}]$
$2p^m$	$e_2 = \widehat{C_2}$	$e_{p^i} = \widehat{C_{p^i}} - \widehat{C_{p^{i+1}}}$	$2\varphi(p^{m-i})$	$4p^i$
	$e_2 = 1 - \widehat{C_2}$	$e_p = \widehat{C_{p^m}}$	2	$2p^i$
	$e_2 = 1 - \widehat{C_2}$	$e_{p^i} = \widehat{C_{p^i}} - \widehat{C_{p^{i+1}}}$	$2\varphi(p^{m-i})$	$4p^i$
$4p^m$	$e = \widehat{C_4}$	$e_p^i = \widehat{C_{p^i}} - \widehat{C_{p^{i+1}}}$	$2\varphi(p^{m-i})$	$8p^i$
	$e_{2^i} = \widehat{C_{2^i}} - \widehat{C_{2^{i+1}}}$	$e_p = \widehat{C_{p^m}}$	$\varphi(2^i)$	$2.2^i p^m$
	$e_{2^i} = \widehat{C_{2^i}} - \widehat{C_{2^{i+1}}}$	$e_{p^i} = \widehat{C_{p^i}} - \widehat{C_{p^{i+1}}}$	$2\varphi(2^i)\varphi(p^j)$	$4.2^i p^j$
$p_1^{m_1} p_2^{m_2}$	$e_{p_1} = \widehat{C_{p_1^{m_1}}}$	$e_{p_2^j} = \widehat{C_{p_2^j}} - \widehat{C_{p_2^{j+1}}}$	$2\varphi(p_2^{m_2-j})$	$2p_1^{m_1} p_2^j$
	$e_{p_1^i} = \widehat{C_{p_1^i}} - \widehat{C_{p_1^{i+1}}}$	$e_{p_2} = \widehat{C_{p_2^{m_2}}}$	$2\varphi(p_1^{m_1-i})$	$2p_1^i p_2^{m_2}$
	$e_{p_1^i} = \widehat{C_{p_1^i}} - \widehat{C_{p_1^{i+1}}}$	$e_{p_2^j} = \widehat{C_{p_2^j}} - \widehat{C_{p_2^{j+1}}}$	$2\varphi(p_1^{m_1-i})\varphi(p_2^{m_2-j})$	$4p_1^i p_2^j$

Table 1.2.

e	e_1	e_2	$dim[(FD_n)ee_1e_2]$	$w[(FD_n)ee_1e_2]$
$\widehat{C_2}$	$\widehat{C_{p_1^{m_1}}}$	$\widehat{C_{p_2^j}} - \widehat{C_{p_2^{j+1}}}$	$2\varphi(p_2^{m_2-j})$	$4p_1^{m_1} p_2^j$
$\widehat{C_2}$	$\widehat{C_{p_1^i}} - \widehat{C_{p_1^{i+1}}}$	$\widehat{C_{p_2^{m_2}}}$	$2\varphi(p_1^{m_1-i})$	$4p_1^i p_2^{m_2}$
$1 - \widehat{C_2}$	$\widehat{C_{p_1^{m_1}}}$	$\widehat{C_{p_2^j}} - \widehat{C_{p_2^{j+1}}}$	$2\varphi(p_2^{m_2-j})$	$4p_1^{m_1} p_2^j$
$1 - \widehat{C_2}$	$\widehat{C_{p_1^i}} - \widehat{C_{p_1^{j+i}}}$	$\widehat{C_{p_2^{m_2}}}$	$2\varphi(p_1^{m_1-i})$	$4p_1^i p_2^{m_2}$
$\widehat{C_2}$	$\widehat{C_{p_1^i}} - \widehat{C_{p_1^{j+i}}}$	$\widehat{C_{p_2^j}} - \widehat{C_{p_2^{j+1}}}$	$2\varphi(p_1^{m_1-i}\varphi(p_2^{m_2-j})$	$8p_1^i p_2^j$
$1 - \widehat{C_2}$	$\widehat{C_{p_1^i}} - \widehat{C_{p_1^{j+i}}}$	$\widehat{C_{p_2^j}} - \widehat{C_{p_2^{j+1}}}$	$2\varphi(p_1^{m_1-i}\varphi(p_2^{m_2-j})$	$8p_1^i p_2^j$

Table 1.3.

with $n \geq 2$. Then $|\mathcal{Q}_n| = 2n$ and this group can be explicitely described as

$$\mathcal{Q}_n = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \beta, \alpha\beta, \alpha^2\beta, \ldots, \alpha^{n-1}\beta\}.$$

We begin with the following.

Theorem 5.1. *The group algebras $\mathbb{F}_q D_n$ and $\mathbb{F}_q \mathcal{Q}_n$ are isomorphic if and only if $4|n$ or $q \equiv 1 \pmod 4$.*

Proof. We shall first describe the structure of $\mathbb{F}_q \mathcal{Q}_n$. Write:

$$\mathbb{F}_q \mathcal{Q}_n \cong \mathbb{F}_q(\mathcal{Q}_n/\mathcal{Q}_n') \oplus \Delta(\mathcal{Q}_n, \mathcal{Q}_n').$$

If $4|n$ then $\mathcal{Q}_n/\mathcal{Q}_n'$ is the Klein group of order 4 and it is clear that $\mathbb{F}_q(\mathcal{Q}_n/\mathcal{Q}_n') \cong \mathbb{F}_q \oplus \mathbb{F}_q \oplus \mathbb{F}_q \oplus \mathbb{F}_q$. Notice that, if $4 \nmid n$ then $\mathcal{Q}_n/\mathcal{Q}_n'$ is a cyclic group of order 4 so, if $q \equiv 1$ *(mod 4)*, then $\mathbb{F}_q$ is a splitting field for $\mathcal{Q}_n/\mathcal{Q}_n'$ and again $\mathbb{F}_q(\mathcal{Q}_n/\mathcal{Q}_n') \cong \mathbb{F}_q \oplus \mathbb{F}_q \oplus \mathbb{F}_q \oplus \mathbb{F}_q$ whereas, if $q \equiv 3$ *(mod 4)*, then $\mathbb{F}_q(\mathcal{Q}_n/\mathcal{Q}_n') \cong \mathbb{F}_q \oplus \mathbb{F}_q \oplus E$, where $[E; \mathbb{F}_q] = 2$.

Write $\Delta(\mathcal{Q}_n, \mathcal{Q}_n') = B_1 \oplus \cdots \oplus B_t$ a sum of simple algebras and recall that these are all the non-commutative simple components of $\mathbb{F}_q \mathcal{Q}_n$ [11,

Prop 3.6.11]. We claim that they are 2×2 matrix algebras over their respective centers.

The class sums of this algebra form a basis for its center, which we denote $\mathcal{Z}(\mathbb{F}_q\mathcal{Q}_n)$; they are:

$$\Lambda_0 = 1, \quad \Lambda_1 = \alpha_1 + \alpha_1^{-1}, \ \ldots,$$

$$\Lambda_{\frac{n}{2}-1} = \alpha^{\frac{n}{2}-1} + \alpha^{-(\frac{n}{2}-1)}, \ \Lambda_{\frac{n}{2}} = \alpha^{\frac{n}{2}},$$

$$\Omega_0 = \beta + \alpha^2\beta + \cdots + \alpha^{n-2}\beta, \quad \Omega_1 = \alpha\beta + \alpha^3\beta + \cdots + \alpha^{n-1}\beta.$$

So, $dim_{\mathbb{F}_q}\mathcal{Z}(\mathbb{F}_q\mathcal{Q}_n) = n/2 + 3$.

Write

$$\mathcal{Z}(\mathbb{F}_q\mathcal{Q}_n) \cong \mathbb{F}_q(\mathcal{Q}_n/\mathcal{Q}_n') \oplus \mathcal{Z}(\Delta(\mathcal{Q}_n, \mathcal{Q}_n'))$$

and

$$\mathcal{Z}(\Delta(\mathcal{Q}_n, \mathcal{Q}_n')) = \mathcal{Z}(B_1) \oplus \cdots \oplus \mathcal{Z}(B_t),$$

so $dim_{\mathbb{F}_q}\Delta(\mathcal{Q}_n, \mathcal{Q}_n') = 2n - 4$ and $dim_{\mathbb{F}_q}\mathcal{Z}(\Delta(\mathcal{Q}_n, \mathcal{Q}_n')) = n/2 - 1$. Since $dim_{\mathbb{F}_q}\mathbb{F}_q(\mathcal{Q}_n/\mathcal{Q}_n') = 4$ and $dim_{\mathcal{Z}(B_i)}B_i \geq 4, 1 \leq i \leq t$, we have that

$$2n - 4 = dim_{\mathbb{F}_q}\Delta(\mathcal{Q}_n, \mathcal{Q}_n')$$

$$= \sum_{i=1}^{t} dim_{\mathbb{F}_q}B_i \geq 4\sum_{i=1}^{t} dim_{\mathbb{F}_q}\mathcal{Z}(B_i)$$

$$= 4dim_{\mathbb{F}_q}\mathcal{Z}(\Delta(\mathcal{Q}_n, \mathcal{Q}_n')) = 4(\frac{n}{2} - 1) = 2n - 4.$$

Hence, $dim_{\mathcal{Z}(B_i)}B_i = 4$, for $1 \leq i \leq t$, as claimed.

We also have that

$$\mathbb{F}_qD_n \cong \mathbb{F}_q(D_n/D_n') \oplus \Delta(D_n, D_n'),$$

where $\mathbb{F}_q(D_n/D_n') \cong \mathbb{F}_q \oplus \mathbb{F}_q \oplus \mathbb{F}_q \oplus \mathbb{F}_q$ and a similar argument shows that all simple components of $\Delta(D_n, D_n')$ are 2×2 matrix algebras over their respective centers (this fact is well-known and also follows from [3, §47] or [9, p. 229]).

By comparing the sum of commutative simple components, it is clear that $\mathbb{F}_qD_n$ and $\mathbb{F}_q\mathcal{Q}_n$ are isomorphic only if $4|n$ or $q \equiv 1$ *(mod 4)*. To show that these conditions are also sufficient write

$$\mathbb{F}_qD_n \cong \mathbb{F}_q \oplus \mathbb{F}_q \oplus \mathbb{F}_q \oplus \mathbb{F}_q \oplus M_2(E_1) \oplus \cdots \oplus M_2(E_t)$$

and

$$\mathbb{F}_q\mathcal{Q}_n \cong \mathbb{F}_q \oplus \mathbb{F}_q \oplus \mathbb{F}_q \oplus \mathbb{F}_q \oplus M_2(K_1) \oplus \cdots \oplus M_2(K_s)$$

where E_i, K_j denote the centers of the respective noncommutative simple components. Clearly, it will be enough to show that $\mathcal{Z}(\mathbb{F}_q D_n) \cong \mathcal{Z}(\mathbb{F}_q \mathcal{Q}_n)$; i.e., that $E_1 \oplus \cdots \oplus E_t \cong K_1 \oplus \cdots \oplus K_s$.

We recall, once again that, for a group G, if $\theta : G \to G$ denotes the map given by $g^\theta = g^q, \forall g \in G$ then the number of simple components of $\mathbb{F}_q G$ and hence also of $\mathcal{Z}(\mathbb{F}_q G)$ is equal to the number of orbits of class sums under this action. Moreover, if $\{F_1, \dots F_k\}$ is the set of simple components of $\mathcal{Z}(\mathbb{F}_q G)$, there is a bijection between this set and the set $\{S_1, \dots, S_k\}$ of orbits, such that $dim_{\mathbb{F}_q} F_i = |S_i|, 1 \leq i \leq k$ [6, Theorem 1.3].

Since $\langle a \rangle$ and $\langle \alpha \rangle$ are both cyclic groups of order n, the classes A_i and Λ_i, $0 \leq i \leq n/2$, define the same number of orbits, with corresponding equal cardinality.

Also, it is easy to show that $B_0^\theta = B_0$ and $B_1^\theta = B_1$.

Since $o(\beta) = 4$ and q is odd, we have that $\beta^\theta = \beta$ or $\beta^\theta = \beta^3$. If $4|n$ then $\beta^3 = \beta a^{\frac{n}{2}} \in \Omega_0$ so, in both cases we have $\Omega_0^\theta = \Omega_0$ and $\Omega_1^\theta = \Omega_1$. If $q \equiv 1 \pmod 4$, then $\beta^\theta = \beta$. Hence, in all possible cases the set of orbits of class sums in both group algebras are esentially equal and we obtain the desired isomorphism. □

As an immediate consequence of the result above and Theorem 3.3 we obtain the following.

Theorem 5.2. *The number of simple components of $\mathbb{F}_q \mathcal{Q}_n$ and $\mathbb{Q}\mathcal{Q}_n$ are equal if and only if one of the following conditions holds:*

(i) $n = 4$ *and* q *is odd.*

(ii) $n = 2^m$, *with* $m \geq 3$ *and* q *is congruent to either* 3 *or* 5, *modulo* 8.

(iii) $n = 4p^m$ *with* p *an odd prime and both* q *and* $-q$ *have order* $\varphi(p^m)$ *modulo* $4p^m$.

Proof. First, notice that if $4 \nmid n$, then $\mathcal{Q}_n/\mathcal{Q}_n'$ is cyclic of order 4, so the abelian part of the rational quaternion group algebra in this case is $\mathbb{Q}\mathcal{Q}_n/\mathcal{Q}_n' \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}(i)$ (even when $q \equiv 1 \pmod 4$). Hence, in this case, $\mathbb{F}_q \mathcal{Q}_n$ has more simple components than $\mathbb{Q}\mathcal{Q}_n$.

On the other hand, if $4|n$ the result follows immediately from Theorem 3.3. □

In the cases of Theorem 5.2 above, due to the isomorphism between $\mathbb{F}_q D_n$ and $\mathbb{F}_q \mathcal{Q}_n$ it is clear that both algebras have the same number of

simple components. As the elements of the form

$$\{e_{11}, e_{12}, e_{21}, e_{22}\} \cup \{e_d | d \neq 1, 2\}$$

described in section §3 are also a set of orthogonal idempotents which add up to 1 for $\mathbb{F}_q\mathcal{Q}_n$ and their number is equal to the number of simple components, it follows that they are the primitive idempotents of this algebra.

The results of section §2 then apply and show that the minimal codes have the same dimensions and weights as the corresponding ones in the dihedral case.

References

[1] S.D. Berman, *Semisimple cyclic and abelian code II*, Cybernetics, **3**, 3 (1967), 17-23.

[2] I.F. Blake and R.C. Mullin, *The Mathematical Theory of Coding*, Academic Press, New York, 1975.

[3] C.W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras* Wiley, New York, 1962.

[4] C.W. Curtis and I. Reiner, *Methods of Representation Theory*, Vol I, Wiley Interscience, New York, 1981.

[5] R. Ferraz, Simple components and central units in group algebras, *J. Algebra*, **279** (2004), 191-203.

[6] R. Ferraz, Simple components of the center of $FG/J(FG)$, *Commun. Algebra*, to appear.

[7] R. Ferraz and C. Polcino Milies, Idempotents in Group Algebras and Minimal Abelian codes, *Finite Fields and Appl.*, to appear.

[8] E.G. Goodaire, E. Jespers and C. Polcino Milies, *Alternative Loop Rings*, North Holland Math. Studies N. 184, Elsevier, Amsterdam, 1996.

[9] E. Jespers, G. Leal and C. Polcino Milies, Units of integral group rings of some metacyclic groups, *Can. Math. Bull.*, **37**, 2 (1994), 228-237.

[10] I. Niven, H.S. Zukermann and H.L. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley & Sons, New York, 1960.

[11] C. Polcino Milies and S.K. Sehgal, *An introduction to Group Rings*, Kluwer Academic Publishers, Dordrecht, The Netherlands, 2002.

[12] C. R.G. Vergara, Wedderburn decompositions of small rational group algebras, in *Groups, Rings and Group Rings*, ed. by A. Giambruno, C. Polcino Milies and S.K. Sehgal, Lecture Notes in Pure and Appl. Math. **248**, Chapman and Hall & CRC, Boca Raton, 2006, pp. 191-200.

CONTACT INFORMATION

F. S. Dutra Departamento de Matemática e Estatística (DME), Pontifícia Universidade Católica de Minas Gerais, Av. Dom José Gaspar, 500, Cep 30.535-901,Belo Horizonte, MG, Brazil
E-Mail: flaviana@pucminas.br

R. A. Ferraz Instituto de Matemática e Estatística, Universidade de São Paulo, Caixa Postal 66281, Cep 05311-970, São Paulo, SP, Brazil
E-Mail: raul@ime.usp.br

C. Polcino Milies Instituto de Matemática e Estatística, Universidade de São Paulo, Caixa Postal 66281, Cep 05311-970, São Paulo, SP, Brazil
E-Mail: polcino@ime.usp.br
URL: http://www.ime.usp.br/ polcino/

Received by the editors: 20.08.2009
and in final form 24.09.2009.