© Algebra and Discrete Mathematics
Volume **33** (2022). Number 1, pp. 87–98
DOI:10.12958/adm1569

RESEARCH ARTICLE

# Central and non central codes of dihedral 2-groups

**S. Gupta*** **and P. Rani**

Communicated by I. Ya. Subbotin

Abstract. In this paper, the central and non central codes of semisimple dihedral group algebra $\mathbb{F}_qG$, over a finite field $\mathbb{F}_q$, are constructed. Further the distances of these central and non central codes are computed.

## Introduction

Let $\mathbb{F}_q$ be a finite field with $q$ elements and $G$ be the dihedral group of order $2^{m+1}$ coprime to $q$, so that the group algebra $\mathbb{F}_qG$ is semisimple. A group code over a finite field $\mathbb{F}_q$ is an ideal of the group algebra $\mathbb{F}_qG$. Semisimplicity of the group algebra ensures that every ideal is generated by an idempotent element. Central(resp. non central) idempotents correspond to central(resp. non central) codes. A code is said to be cyclic, abelian, non abelian, metacyclic or dihedral code if the underlying group is of that kind. The Hamming distance between two codewords of the code is the number of places at which they are different and distance of the code is minimum distance between any pair of distinct codewords. A code with higher minimum distance can correct more errors and hence considered an efficient code.

A minimal central code is an ideal which is minimal in the set of all two sided ideals of the semisimple group algebra and is generated by primitive central idempotent. A description of primitive central idempotents of $\mathbb{F}_qG$,

*Corresponding author.

**2020 MSC:** 11T71, 94B60, 95B65.

**Key words and phrases:** group algebra, idempotents, central codes, non central codes, distance.

$G$ metacyclic, has been given by Bakshi et al. ([1], Theorem 4) in terms of Shoda pairs. In [2], Dutra et al. expressed primitive central idempotents as elements of the group algebra $\mathbb{F}_qG$, where $G$ is the dihedral group of order $2^{m+1}$ and $q \equiv 3$ *or* $5 \pmod 8$ and computed distances of the corresponding codes. In this paper, we will express primitive central idempotents of the group algebra $\mathbb{F}_qG$, where $G$ is the dihedral group of order $2^{m+1}$ and $q \equiv \pm 1 \pmod{2^m}$, as elements of group algebra and will further compute the distances of codes generated by these primitive central idempotents. We will prove in Theorem 3 that the distances of these central codes are higher than the distances of the central codes computed in [2].

In [3], Sabin and Lomonaco proved that central metacyclic codes are combinatorially equivalent to abelian codes which are not desirable. This motivated the search for non central codes. In [4], Assuena and Milies studied certain left codes with the help of primitive central idempotents obtained by Dutra et al. in [2] and also proved the existence of certain non central codes that are combinatorially equivalent to cyclic codes. In continuation of the work in [2] and [4], we construct certain non central idempotents with the help of central ones and compare the distances of corresponding non central codes with the central ones in section 4.

## 1. Primitive central idempotents

It is known that if a group $\mathcal{G}$ is cyclic then the set $\mathrm{Irr}(\mathcal{G})$ of irreducible characters of $\mathcal{G}$ over $\overline{\mathbb{F}}_q$ forms a group with the operation: $\lambda\lambda^*(g) = \lambda(g)\lambda^*(g)$ for $\lambda, \lambda^* \in \mathrm{Irr}(\mathcal{G})$ and $g \in \mathcal{G}$. Moreover $\mathcal{G} \cong \mathrm{Irr}(\mathcal{G})$. For subgroups $H$ and $K$ of finite group $G$, $H \trianglelefteq K \leqslant G$, $K/H$ cyclic, $\mathrm{Irr}(K/H)$ is a cyclic group. For a generator $\lambda$ of $\mathrm{Irr}(K/H)$, let $C_q(\lambda) = \{\lambda, \lambda^q, \lambda^{q^2}, \ldots, \lambda^{q^{o-1}}\}$ be the $q$-cyclotomic coset of $\lambda$, where $o$ is the multiplicative order of $q$ modulo order of $K/H$. Let $\mathfrak{C}(K/H)$ be the set of $q$-cyclotomic cosets of $\mathrm{Irr}(K/H)$ containing the generators of $\mathrm{Irr}(K/H)$ and $\mathcal{R}(K/H)$ be the set of distinct orbits of $\mathfrak{C}(K/H)$ under the action $(*)$ of $N_G(H) \cap N_G(K)$ on $\mathfrak{C}(K/H)$ given by $g * C = g^{-1}Cg$.

For each $C \in \mathcal{R}(K/H)$, set

- $\varepsilon_c(K,H) = [K:H]^{-1}\widehat{H}\sum_{X \in K/H} \mathrm{tr}_{\mathbb{F}_q(\xi)/\mathbb{F}_q}(\chi(X))\, g_X^{-1}$, where $\chi$ is representative of $q$-cyclotomic coset $C$ , $\xi$ is primitive $[K:H]$-th root of unity in $\overline{\mathbb{F}}_q$, $g_X$ denotes a representative of $X \in K/H$ and $\widehat{H} = |H|^{-1}\sum_{h \in H} h$;
- $e_C(G,K,H)$ is the sum of distinct $G$-conjugates of $\varepsilon_c(K,H)$.

Let

$$G = \langle a, b \,|\, a^{2^m} = e, b^2 = e, b^{-1}ab = a^{2^m-1} \rangle \tag{1}$$

and $\mathbb{F}_q$ be a field with $q$ elements and $q \equiv \pm 1 \,(\mathrm{mod}\, 2^m)$. The result [1, Theorem 4] gives the complete set of primitive central idempotents of semisimple group algebra $\mathbb{F}_q G$ in terms of Shoda pairs as follows:

$$\begin{aligned}\{e_c(G,G,G)|C \in \mathcal{R}\,(G/G)\} &\cup \{e_c(G,G,\langle a^2,b\rangle)|C \in \mathcal{R}\left(G/\langle a^2,b\rangle\right)\}\\ &\cup \{e_c(G,G,\langle a^2,ab\rangle)|C \in \mathcal{R}\left(G/\langle a^2,ab\rangle\right)\}\\ &\cup \{e_c(G,G,\langle a\rangle)|C \in \mathcal{R}\,(G/\langle a\rangle)\}\\ &\cup \{e_c(G,\langle a\rangle,\langle a^v\rangle)|C \in \mathcal{R}\,(\langle a\rangle/\langle a^v\rangle)\,, v=2^i, 2 \leqslant i \leqslant m\}\end{aligned}$$

Now we will express these primitive central idempotents in simpler form as elements of the group algebra. It is easy to see that the idempotent corresponding to $e_c(G,G,G)$ is $\widehat{\langle b\rangle}\widehat{\langle a\rangle}$, the idempotent corresponding to $e_c(G,G,\langle a^2,b\rangle)$ is $\widehat{\langle a^2,b\rangle} - \widehat{G}$, the idempotent corresponding to $e_c(G,G,\langle a^2,ab\rangle)$ is $\widehat{\langle a^2,ab\rangle} - \widehat{G}$, the idempotent corresponding to $e_c(G,G,\langle a\rangle)$ is $\widehat{\langle a\rangle} - \widehat{G}$.

Let us now compute the idempotent corresponding to $e_c(G,\langle a\rangle,\langle a^v\rangle)$, $v = 2^i$, $2 \leqslant i \leqslant m$, $C$ representative of an orbit of $\mathcal{R}(\langle a\rangle/\langle a^v\rangle)$. Let $\mathrm{Irr}(\langle a\rangle/\langle a^v\rangle)$ be generated by $\lambda$, where $\lambda$ is an irreducible character of $\langle a\rangle/\langle a^v\rangle$ over $\overline{\mathbb{F}}_q$, defined by $\lambda\left(\overline{a}^k\right) = \xi^k$, $0 \leqslant k \leqslant v-1$ and $\xi$ is a primitive $\left[\langle a\rangle : \langle a^v\rangle\right]$-th, i.e., $v$-th root of unity in $\overline{\mathbb{F}}_q$.

Case I: Let $q \equiv 1 (\mathrm{mod}\, 2^m)$.

In this case, $\mathfrak{C}\,(\langle a\rangle/\langle a^v\rangle) = \{C_q(\lambda), C_q(\lambda^3), \cdots, C_q(\lambda^{v-1})\}$, $C_q(\lambda^j) = \{\lambda^j\}$ and $\mathcal{R}(\langle a\rangle/\langle a^v\rangle) = \{\mathrm{orb}(C_q(\lambda)), \mathrm{orb}(C_q(\lambda^3)), \cdots, \mathrm{orb}(C_q(\lambda^{\frac{v}{2}-1}))\}$, where $\mathrm{orb}(C_q(\lambda^j)) = \{C_q(\lambda^j), C_q(\lambda^{-j})\}$.

For $C_q(\lambda^j)$, representative of $\mathrm{orb}(C_q(\lambda^j)) \in \mathcal{R}(\langle a\rangle/\langle a^v\rangle)$ and $j$ an odd natural number strictly less than $\frac{v}{2}$, we have

$$\begin{aligned}\epsilon_{C_q(\lambda^j)}(\langle a\rangle,\langle a^v\rangle) &= \frac{1}{2^m}\left[1 + a^v + a^{2v} + \cdots + a^{2^m-v}\right]\left[\lambda^j(\overline{e}) + \lambda^j(\overline{a})a^{-1}\right.\\ &\quad \left. + \lambda^j(\overline{a}^2)a^{-2} + \cdots + \lambda^j(\overline{a}^{v-1})a^{-(v-1)}\right]\\ &= \frac{1}{2^m}\left[1 + a^v + a^{2v} + \cdots + a^{2^m-v}\right]\left[1 + \xi^j a^{-1}\right.\\ &\quad \left. + \xi^{2j}a^{-2} + \cdots + \xi^{j(v-1)}a^{-(v-1)}\right]\\ &= \frac{1}{2^m}[1 + \xi^{j(v-1)}a + \xi^{j(v-2)}a^2 + \cdots + \xi^j a^{v-1}\\ &\quad + a^v + \xi^{j(v-1)}a^{v+1} + \cdots + a^{2v} + \cdots + a^{2^m-v}\\ &\quad + \xi^{j(v-1)}a^{2^m-v+1} + \cdots + \xi^j a^{2^m-1}]\end{aligned}$$

Since $e_{C_q(\lambda^j)}(G, \langle a\rangle, \langle a^v\rangle)$ is the sum of distinct $G$-conjugates of $\epsilon_{c_q(\lambda^i)}(\langle a\rangle, \langle a^v\rangle$, we have

$$\begin{aligned}
e_{C_q(\lambda^j)}(G, \langle a\rangle, \langle a^v\rangle) &= \epsilon_{C_q(\lambda^i)}(\langle a\rangle, \langle a^v\rangle) + \epsilon_{C_q(\lambda^i)}(\langle a\rangle, \langle a^v\rangle)^b \\
&= \frac{1}{2^m}\big[1 + \xi^{j(v-1)}a + \cdots + \xi^j a^{v-1} + a^v \\
&\quad + \xi^{j(v-1)}a^{v+1} + \cdots + a^{2v} + \cdots + a^{2^m-v} \\
&\quad + \xi^{j(v-1)}a^{2^m-v+1} + \cdots + \xi^j a^{2^m-1}\big] \\
&\quad + \frac{1}{2^m}\big[1 + \xi^j a + \cdots + \xi^{j(v-1)}a^{v-1} \\
&\quad + a^v + \xi^j a^{v+1} + \cdots + a^{2v} + \cdots + a^{2^m-v} \\
&\quad + \xi^j a^{2^m-v+1} + \cdots + \xi^{j(v-1)}a^{2^m-1}\big] \\
&= \frac{1}{2^m}\big[2 + (\xi^j + \xi^{-j})a + (\xi^{2j} + \xi^{-2j})a^2 + \cdots \\
&\quad + (\xi^j + \xi^{-j})a^{v-1} + 2a^v + (\xi^j + \xi^{-j})a^{v+1} \\
&\quad + (\xi^{2j} + \xi^{-2j})a^{v+2} + \cdots + 2a^{2v} + \cdots \\
&\quad + 2a^{2^m-v} + (\xi^j + \xi^{-j})a^{2^m-v+1} + \cdots \\
&\quad + (\xi^j + \xi^{-j})a^{2^m-1}\big] \\
&= \frac{1}{2^m}\big[1 + a^v + a^{2v} + \cdots + a^{2^m-v}\big]\big[2 + (\xi^j + \xi^{-j})a \\
&\quad + (\xi^{2j} + \xi^{-2j})a^2 + \cdots + (\xi^j + \xi^{-j})a^{v-1}\big]
\end{aligned}$$

We will denote $e_{C_q(\lambda^j)}(G, \langle a\rangle, \langle a^v\rangle)$ for $v = 2^i, 2 \leqslant i \leqslant m$ by $e_i^j$ and take $\alpha_{j(k)} = \xi^{jk} + \xi^{-jk}$, $1 \leqslant k \leqslant 2^i - 1$.

$$e_i^j = \frac{1}{2^m}\left(\sum_{l=0}^{2^{m-i}-1} a^{2^i l}\right)\left(\sum_{k=0}^{2^i-1} \alpha_{j(k)}a^k\right)$$

For $1 \leqslant l \leqslant 2^{i-1} - 1$, $\alpha_{j(2^{i-1}+l)} = \xi^{j(2^{i-1}+l)} + \xi^{-j(2^{i-1}+l))} = -\xi^{jl} - \frac{1}{\xi^{jl}} = -\alpha_{j(l)}$,

$$e_i^j = \frac{1}{2^m}\left(\sum_{l=0}^{2^{m-i}-1} a^{2^i l}\right)\left(\sum_{k=0}^{2^{i-1}-1} \alpha_{j(k)}\left\{a^k - a^{2^{i-1}+k}\right\}\right)$$

$$= \frac{1}{2^m}\left(1 - a^{2^{i-1}}\right)\left(\sum_{l=0}^{2^{m-i}-1} a^{2^i l}\right)\left(\sum_{k=0}^{2^{i-1}-1} \alpha_{j(k)} a^k\right)$$
$$= 2^{1-i}\left(\widehat{\langle a^{2^i}\rangle} - \widehat{\langle a^{2^{i-1}}\rangle}\right)\left(\sum_{k=0}^{2^{i-1}-1} \alpha_{j(k)} a^k\right)$$

where $j$ is an odd natural number strictly less than $2^{i-1}$.

Case II: Let $q \equiv -1 (\mathrm{mod}\, 2^m)$.

In this case, $\mathfrak{C}(\langle a\rangle/\langle a^v\rangle) = \{C_q(\lambda), C_q(\lambda^3), \cdots, C_q(\lambda^{\frac{v}{2}-1})\}$, where $C_q(\lambda^j) = \{\lambda^j, \lambda^{-j}\}$ and $\mathcal{R}(\langle a\rangle/\langle a^v\rangle) = \{\mathrm{orb}(C_q(\lambda)), \mathrm{orb}(C_q(\lambda^3)), \ldots, \mathrm{orb}(C_q(\lambda^{\frac{v}{2}-1}))\}$, $\mathrm{orb}(C_q(\lambda^j)) = \{C_q(\lambda^j), C_q(\lambda^{-j})\}$.

For $C_q(\lambda^j) \in \mathcal{R}(\langle a\rangle/\langle a^v\rangle)$, $j$ an odd natural number strictly less than $\frac{v}{2}$, we have

$$\begin{aligned}
\epsilon_{c_q(\lambda^j)}(\langle a\rangle, \langle a^v\rangle) &= \frac{1}{2^m}\left[1 + a^v + a^{2v} \cdots + a^{2^m - v}\right] \\
&\quad \left[2 + \mathrm{tr}_{\mathbb{F}_q(\xi)/\mathbb{F}_q}\left(\xi^j\right) a^{-1} + \mathrm{tr}_{\mathbb{F}_q(\xi)/\mathbb{F}_q}\left(\xi^{2j}\right) a^{-2}\right. \\
&\qquad \left. + \cdots + \mathrm{tr}_{\mathbb{F}_q(\xi)/\mathbb{F}_q}\left(\xi^{j(v-1)}\right) a^{-(v-1)}\right] \\
&= \frac{1}{2^m}\left[1 + a^v + a^{2v} \cdots + a^{2^m - v}\right] \\
&\quad \left[2 + (\xi^j + \xi^{-j})a^{-1} + (\xi^{2j} + \xi^{-2j})a^{-2}\right. \\
&\qquad \left. + \cdots + (\xi^j + \xi^{-j})a^{-(v-1)}\right] \\
&= \frac{1}{2^m}\left[2 + (\xi^j + \xi^{-j})a + (\xi^{2j} + \xi^{-2j})a^2\right. \\
&\quad + \cdots + 2a^v + (\xi^j + \xi^{-j})a^{v+1} \\
&\quad + (\xi^{2j} + \xi^{-2j})a^{v+2} + \cdots + 2a^{2v} + \cdots \\
&\quad + 2a^{2^m - v} + (\xi^j + \xi^{-j})a^{2^m - v + 1} \\
&\quad + (\xi^{2j} + \xi^{-2j})a^{2^m - v + 2} + \cdots \\
&\quad \left. + (\xi^j + \xi^{-j})a^{2^m - 1}\right]
\end{aligned}$$

Since $e_{C_q(\lambda^j)}(G, \langle a\rangle, \langle a^v\rangle)$ is the sum of distinct $G$-conjugates of $\epsilon_{c_q(\lambda^j)}(\langle a\rangle, \langle a^v\rangle$ which gives us

$$e_{C_q(\lambda^j)}(G, \langle a\rangle, \langle a^v\rangle) = \epsilon_{C_q(\lambda^j)}(\langle a\rangle, \langle a^v\rangle)$$

The primitive central idempotent $e_i^j = e_{C_q(\lambda^j)}(G, \langle a\rangle, \langle a^v\rangle)$ for $v = 2^i, 2 \leqslant i \leqslant m$ will have same expression as in Case I. Thus we have the following theorem.

**Theorem 1.** *Let $G$ be the dihedral group of order $2^{m+1}$ and $\mathbb{F}_q$ be a finite field with $q$ elements such that $q \equiv \pm 1 \pmod{2^m}$. Then the primitive central idempotents of $\mathbb{F}_q G$ are as follows:*

| | idempotent |
|---|---|
| $e_1'$ | $\widehat{b}\widehat{a}$ |
| $e_2'$ | $\widehat{\langle a^2, b\rangle} - \widehat{G}$ |
| $e_3'$ | $\widehat{\langle a^2, ab\rangle} - \widehat{G}$ |
| $e_4'$ | $\widehat{\langle a\rangle} - \widehat{G}$ |
| $e_i^j$ | $2^{1-i}\left(\widehat{\langle a^{2^i}\rangle} - \widehat{\langle a^{2^{i-1}}\rangle}\right)\left(\sum_{k=0}^{2^{i-1}-1} \alpha_{j(k)} a^k\right)$ |

*where $2 \leqslant i \leqslant m$, $j$ is odd natural number strictly less than $2^{i-1}$, $\alpha_{j(k)} = \xi^{jk} + \xi^{-jk}$, $\xi$ is a primitive $2^i$-th root of unity and $0 \leqslant k \leqslant 2^{i-1} - 1$, $k \neq 2^{i-2}$.*

## 2. Central codes

In [2], Dutra et al. computed the complete set of primitive central idempotents of group algebra $\mathbb{F}_q G$, where $G$ is the dihedral group of order $2^{m+1}$ and $q \equiv 3$ *or* $5 \pmod 8$ and computed the distances of the codes using these primitive central idempotents as follows:

**Theorem 2** ([2])**.** *Let $\mathbb{F}_q$ be a finite field with $q$ elements and $G$ be the dihedral group of order $2^{m+1}$, $m \geqslant 3$ and $q \equiv 3$ or $5 \pmod 8$. Then the complete set of primitive central idempotents and the distances of respective codes in the group algebra $\mathbb{F}_q G$ is:*

| | $e$ | *distance of* $d[(\mathbb{F}_q G)e]$ |
|---|---|---|
| $e_1'$ | $\widehat{b}\widehat{a}$ | $2^{m+1}$ |
| $e_2'$ | $\widehat{\langle a^2, b\rangle} - \widehat{G}$ | $2^{m+1}$ |
| $e_3'$ | $\widehat{\langle a^2, ab\rangle} - \widehat{G}$ | $2^{m+1}$ |
| $e_4'$ | $\widehat{\langle a\rangle} - \widehat{G}$ | $2^{m+1}$ |
| $e_i$ | $\widehat{\langle a^{2^i}\rangle} - \widehat{\langle a^{2^{i-1}}\rangle}$ | $2^{m-i+1}$ |

*where $2 \leqslant i \leqslant m$.*

In the following theorem, we will compute bounds on the distances of codes generated by the primitive central idempotents of $\mathbb{F}_q G$, $G$ is the dihedral group of order $2^{m+1}$, $q \equiv \pm 1 (\mathrm{mod}\ 2^m)$. We will prove that in this case, central codes possess higher minimum distance than the central codes with the condition $q \equiv 3$ *or* $5 \pmod 8$.

**Theorem 3.** *In the semisimple group algebra defined $\mathbb{F}_qG$, $G$ is the dihedral group of order $2^{m+1}$ and $q \equiv \pm 1 (\mathrm{mod}\ 2^m)$, the distances of codes generated by primitive central idempotents of the group algebra $\mathbb{F}_qG$ defined in Theorem 1 are as follows:*

| | *idempotent* | *distance of $C_l^{'}$(or $C_i^j$)* |
|---|---|---|
| $e_1^{'}$ | $\widehat{ba}$ | $2^{m+1}$ |
| $e_2^{'}$ | $\widehat{\langle a^2, b\rangle} - \widehat{G}$ | $2^{m+1}$ |
| $e_3^{'}$ | $\widehat{\langle a^2, ab\rangle} - \widehat{G}$ | $2^{m+1}$ |
| $e_4^{'}$ | $\widehat{\langle a\rangle} - \widehat{G}$ | $2^{m+1}$ |
| $e_i^j$ | $2^{1-i}\left(\widehat{\langle a^{2^i}\rangle} - \widehat{\langle a^{2^{i-1}}\rangle}\right)$ $\left(\sum_{k=0}^{2^{i-1}-1} \alpha_{j(k)} a^k\right)$ | $2^{m-i+1} \leqslant d(C_i^j) \leqslant 2^m(1-2^{1-i})$ |

*where $C_l^{'}$(resp. $C_i^j$) is the code corresponding to an ideal $\mathbb{F}_qGe_l^{'}$(resp. $\mathbb{F}_qGe_i^j$) generated by primitive central idempotent $e_l^{'}$(resp. $e_i^j$), $2 \leqslant i \leqslant m$, $1 \leqslant l \leqslant 4$, $j$ is odd natural number strictly less than $2^{i-1}$, $\alpha_{j(k)} = \xi^{jk} + \xi^{-jk}$, $\xi$ is a primitive $2^i$-th root of unity and $0 \leqslant k \leqslant 2^{i-1}-1$, $k \neq 2^{i-2}$.*

*Proof.* It follows from [4, Lemma 2.3] that $d(C_l^{'}) = 2^{m+1}$, $1 \leqslant l \leqslant 4$. Now we will compute bounds for the distance of the codes generated by primitive central idempotents $e_i^j$.

$$e_i^j = 2^{1-i}\left(\widehat{\langle a^{2^i}\rangle} - \widehat{\langle a^{2^{i-1}}\rangle}\right)\left(\sum_{k=0}^{2^{i-1}-1} \alpha_{j(k)} a^k\right)$$

Distance of the codes generated by the idempotents $\widehat{\langle a^{2^i}\rangle} - \widehat{\langle a^{2^{i-1}}\rangle}$, $2 \leqslant i \leqslant m$ is $2^{m-i+1}$ so $d(C_i^j) \geqslant 2^{m-i+1}$. Since $\alpha_{j(k)} = 0$ only when $k = 2^{i-2}$, the number of non-zero coefficients of $e_i^j$ are $2^m - \frac{2^m}{2^{i-1}} = 2^m(1-2^{1-i})$ which implies that $d(C_i^j) \leqslant 2^m(1-2^{1-i})$. We conclude that $2^{m-i+1} \leqslant d(C_i^j) \leqslant 2^m(1-2^{1-i})$. □

### 2.1. Dihedral codes of order 16

In [2], Dutra et al. proved that the number of simple components of rational group algebra $\mathcal{Q}G$ and $\mathbb{F}_qG$ are equal when $G$ is dihedral group of order 16 and $q \equiv 3\,or\,5\,(\mathrm{mod}\ 8)$. Further they have computed the distances of codes generated by primitive central idempotents of $\mathbb{F}_qG$, $q \equiv 3\,or\,5\,(\mathrm{mod}\ 8)$. In the following theorem, we will compute distances

of codes generated by primitive central idempotents of group algebra $\mathbb{F}_qG$ for $\gcd(q,16)=1$ thus modifying the result of Dutra et al.:

**Theorem 4.** *Let $G$ be the dihedral group of order 16 and $\mathbb{F}_q$ be a finite field with $q$ elements . Then the complete set of primitive central idempotents of the semisimple group algebra $\mathbb{F}_qG$ and the distances of respective codes in the group algebra $\mathbb{F}_qG$ are as follows:*

$$q \equiv 1 \text{ or } 7 \pmod 8, \qquad q \equiv 3 \text{ or } 5 \pmod 8$$

| $e$ | $d[(\mathbb{F}_qG)e]$ | $e$ | $d[(\mathbb{F}_qG)e]$ |
|---|---|---|---|
| $\widehat{b}\widehat{a}$ | 16 | $\widehat{b}\widehat{a}$ | 16 |
| $\widehat{\langle a^2, b\rangle} - \widehat{G}$ | 16 | $\widehat{\langle a^2, b\rangle} - \widehat{G}$ | 16 |
| $\widehat{\langle a^2, ab\rangle} - \widehat{G}$ | 16 | $\widehat{\langle a^2, ab\rangle} - \widehat{G}$ | 16 |
| $\widehat{\langle a\rangle} - \widehat{G}$ | 16 | $\widehat{\langle a\rangle} - \widehat{G}$ | 16 |
| $\widehat{\langle a^4\rangle} - \widehat{\langle a^2\rangle}$ | 4 | $\widehat{\langle a^4\rangle} - \widehat{\langle a^2\rangle}$ | 4 |
| $\frac{1}{8}(1-a^4)$ $(2+\alpha a-\alpha a^3)$ | $2 \leqslant d[(\mathbb{F}_qG)e] \leqslant 6$ | $\widehat{\langle e\rangle} - \widehat{\langle a^4\rangle}$ | 2 |
| $\frac{1}{8}(1-a^4)$ $(2-\alpha a+\alpha a^3)$ | $2 \leqslant d[(\mathbb{F}_qG)e] \leqslant 6$ | - | - |

*where $\alpha^2 = 2$.*

## 3. Non central codes

Now we turn our attention towards certain non central codes that will give us codes of higher minimum distance than the codes generated by central ones. In [4], Assuena and Milies computed some non central idempotents with the help of central ones of the semisimple group algebra $\mathbb{F}_qG$, where $G$ is split metacyclic group of order $p^m l^n$, $p$ and $l$ distinct odd primes and also for dihedral group of order $2p^m$, $p$ odd. In continuation of the work done in [4], we will construct certain non central dihedral codes that will give us higher minimum distance than the distance of central codes obtained in Theorems 2 and 3.

Let $G$ be the dihedral group of order $2^{m+1}$ given by presentation (1), $q \equiv 3 \text{ or } 5 \pmod 8$ and $e_i = \widehat{\langle a^{2^i}\rangle} - \widehat{\langle a^{2^{i-1}}\rangle}$, $2 \leqslant i \leqslant m$ be as in Theorem 2. It is easy to see that $\widehat{b}e_i$ and $(1-\widehat{b})e_i$ are non central idempotens of $\mathbb{F}_qG$.

**Theorem 5.** *With the notations above, $(\mathbb{F}_qG)\,\widehat{b}e_i$ and $(\mathbb{F}_qG)\,(1-\widehat{b})e_i$ are isomorphic to abelian codes as vector spaces.*

*Proof.* Consider an abelian group $C = C_{2^m} \times C_2$, where $C_{2^m} = \langle u \rangle$ is a cyclic group of order $2^m$ and $C_2 = \langle v \rangle$ of order 2. Denote by $k_i = \langle u^{2^i} \rangle - \langle u^{2^{i-1}} \rangle$, $2 \leqslant i \leqslant m$. Consider a map $\Lambda : G \to C$, where $\Lambda(a^i b^j) = u^i v^j$. It follows directly from the definition of $\Lambda$ that $\Lambda(e_i) = k_i$. We claim that

$$\Lambda(g\widehat{b}e_i) = \Lambda(g)\widehat{v}k_i \quad \forall\ g \in G.$$

If $g$ is of the form $a^r$, $1 \leqslant r \leqslant 2^m$,

$$\Lambda(g\widehat{b}e_i) = \Lambda(a^r\widehat{b}e_i) = \frac{1}{2}\big[\Lambda(a^r e_i) + \Lambda(a^r b e_i)\big] = \frac{1}{2}\big[\Lambda(a^r e_i) + \Lambda(a^r e_i b)\big]$$
$$= \frac{1}{2}\big[u^r k_i + u^r v k_i)\big] = u^r \widehat{v} k_i = \Lambda(g)\widehat{b}e_i$$

If $g$ is of the form $a^r b$, $1 \leqslant r \leqslant 2^m$,

$$\Lambda(a^r b\widehat{b}e_i) = \Lambda(a^r\widehat{b}e_i) = \Lambda(g)\widehat{b}e_i$$

and

$$\Lambda(g(1-\widehat{b})e_i) = \Lambda(ge_i) - \Lambda(g\widehat{b}e_i) = \Lambda(g)k_i - \Lambda(g)\widehat{v}k_i = \Lambda(g)(1-\widehat{v})$$

This completes the proof. □

Now we will construct more non central idempotents of dihedral group algebra with the help of central ones.

**Theorem 6.** *Let $G$ be the dihedral group of order $2^{m+1}$, $m \geqslant 3$ given by presentation (1) and $\mathbb{F}_q$ be finite field with $q$ elements. Then $\widehat{x}_k e$ are non central idempotents of semisimple group algebra $\mathbb{F}_q G$ where $x_k = a^k b$, $0 \leqslant k \leqslant 2^m - 1$ and $e$ is a primitive central idempotent of $\mathbb{F}_q G$.*

| | |
|---|---|
| $\widehat{x}_k e$ | $d[(\mathbb{F}_q G)\widehat{x}_k e]$ |
| $\widehat{x}_k e_i$ | $2^{m-i+2}$ |
| $\widehat{x}_k e_i^j$ | $d[(\mathbb{F}_q G)e_i^j] \leqslant d[(\mathbb{F}_q G)\widehat{x}_k e_i^j] \leqslant 2^{m+1}(1-2^{1-i})$ |

*where $e_i$ and $e_i^j$ are defined in Theorems 2 and 3.*

*Proof.* Let $0 \leqslant k \leqslant 2^m - 1$.

Case I: $q \equiv 3$ or $5 \pmod 8$

$$\widehat{x}_k e_i = \frac{1}{2^{m-i+2}}\big[1 - a^{2^{i-1}} + a^{2^i} - a^{3.2^{i-1}} + \cdots + a^{2^m-2^i} - a^{2^m-2^{i-1}}$$
$$+ a^k b - a^{k+2^{i-1}} b + a^{k+2^i} b - a^{k+3.2^{i-1}} b + \cdots + a^{k+2^m-2^i} b$$
$$- a^{k+2^m-2^{i-1}} b\big]$$

$$a \cdot \widehat{x}_k e_i = -\widehat{x}_k e_i \cdot a.$$

Since $\widehat{x}_k e_i$ are not commuting with $a$, hence $\widehat{x}_k e_i$ are non central idempotents and $w(\widehat{x}_k e_i) = 2^{m-i+2}$ so distance of the code is atmost $2^{m-i+2}$.

An arbitrary element $\gamma \in (\mathbb{F}_q G)\widehat{x}_k e_i$ is of the form $\sum_{l=0}^{2^m-1}\{\alpha_l a^l + \beta_l a^l b\}\widehat{x}_k e_i$ then

$$\begin{aligned}\gamma = \frac{1}{2^{m-i+2}} \sum_{j=0}^{2^{i-1}-1} \{&(\alpha_j - \alpha_{j+2^{i-1}} + \alpha_{j+2.2^{i-1}} - \cdots - \alpha_{j+2^m-2^{i-1}} \\ &+ \beta_{j+k} - \beta_{j+k+2^{i-1}} + \beta_{j+k+2.2^{i-1}} \cdots - \beta_{j+k+2^m-2^{i-1}}) \\ &(a^j - a^{j+2^{i-1}} + a^{j+2^i} - \cdots + a^{j+2^m-2^i} - a^{j+2^m-2^{i-1}} \\ &+ a^{j+k}b - a^{j+k+2^{i-1}}b + a^{j+k+2^i}b - \cdots + a^{j+k+2^m-2^i}b \\ &- a^{j+k+2^m-2^{i-1}}b)\}\end{aligned}$$

where $\alpha_l = \alpha_{l+2^m}$, $\beta_l = \beta_{l+2^m}$.

Since each coefficient is shared by $2^{m-i+2}$ elements of the group. So distance of the code is at least $2^{m-i+2}$. So we conclude that distance of the code is $2^{m-i+2}$.

Case II: $q \equiv \pm 1 (\text{mod } 2^m)$.

Note that if $\widehat{x}_k e_i^j = 0$ then $e_i^j + x_k e_i^j = 0$. But $\text{supp}(e_i^j) \in \langle a \rangle$ and $\text{supp}(x_k e_i^j) \in \langle a \rangle b$, so these elements have disjoint support. Consequently, $\widehat{x}_k e_i^j \neq 0$ for all indices $i$ and $j$ mentioned above. So $\widehat{x}_k e_i^j$ are non zero and non central idempotents. Moreover $w\left(\widehat{x}_k e_i^j\right) = 2^{m+1}(1 - 2^{1-i})$. So distance of the code is atmost $2^{m+1}(1-2^{1-i})$. Hence the result follows. □

**Theorem 7.** *The elements $e + \widehat{x}_k a(1 - \widehat{x}_k)e$ are units inside the ideals $(\mathbb{F}_q G)e$, where $x_k = a^k b$, $0 \leqslant k \leqslant 2^m - 1$ and $e$ is an idempotent defined in Theorems 2 and 3 other than $e_l^{'}$, $1 \leqslant l \leqslant 4$.*

*Proof.* Take $\Delta_k = e + \widehat{x}_k a(1 - \widehat{x}_k)e$ and $\Delta_k^{'} = e - \widehat{x}_k a(1 - \widehat{x}_k)e$. We will prove that $\Delta_k \Delta_k^{'} = \Delta_k^{'} \Delta_k = e$.

$$\begin{aligned}\Delta_k \Delta_k^{'} &= \{e + \widehat{x}_k a(1 - \widehat{x}_k)e\}\{e - \widehat{x}_k a(1 - \widehat{x}_k)e\} \\ &= e^2 - e\widehat{x}_k a(1 - \widehat{x}_k)e + \widehat{x}_k a(1 - \widehat{x}_k)e^2 + 0 \\ &= e - \widehat{x}_k a(1 - \widehat{x}_k)e + \widehat{x}_k a(1 - \widehat{x}_k)e \\ &= e\end{aligned}$$

Similarly $\Delta_k^{'} \Delta_k = e$ which tells us $\Delta_k^{'}$ is inverse of $\Delta_k$. □

It is easy to see that $\Delta_k(\widehat{x}_k e)\Delta_k^{-1}$ and $\Delta_k^{-1}(\widehat{x}_k e)\Delta_k$ are equal to $(\widehat{x}_k \pm \widehat{x}_k a(1-\widehat{x}_k))\, e$ and these elements are non central idempotents of $(\mathbb{F}_q G)e$. The codes corresponding to idempotents $(\widehat{x}_k \pm \widehat{x}_k a(1-\widehat{x}_k))\, e$ are better than central codes in terms of distance.

## 4. Examples

In the following examples, we will show that the distances of non central codes of dihedral groups of order 8 and 16 are better than the distances of central ones.

**Example 1.** Set $G = \langle a, b \,|\, a^4 = e, b^2 = e, b^{-1}ab = a^3\rangle$. The primitive central idempotents of the semisimple group algebra $\mathbb{F}_q G$ by [2, Table 1.1] are $e_1^{'} = \widehat{b}\widehat{a}$, $e_2^{'} = \widehat{\langle a^2, b\rangle} - \widehat{G}, e_3^{'} = \widehat{\langle a^2, ab\rangle} - \widehat{G}$, $e_4^{'} = \widehat{\langle a\rangle} - \widehat{G}$ and $e_1 = \frac{1}{2}[1 - a^2]$. It follows from [4, Lemma 2.3] that $d[(\mathbb{F}_q G)e_l^{'}] = 8$, $1 \leqslant l \leqslant 4$. For $x_k = a^k b$,

| $e$ | $d[(\mathbb{F}_q G)e]$ |
|---|---|
| $e_1$ | 2 |
| $\widehat{x}_k e_1$ | 4 |
| $f_1$ | $2 \leqslant d[(\mathbb{F}_q G)f_1]$ |
| $f_2$ | $2 \leqslant d[(\mathbb{F}_q G)f_2]$ |

where $f_1 = (\widehat{x}_k + \widehat{x}_k a(1-\widehat{x}_k))\, e_1$ and $f_2 = (\widehat{x}_k - \widehat{x}_k a(1-\widehat{x}_k))\, e_1$.

**Example 2.** Set $G = \langle a, b \,|\, a^8 = e,\ b^2 = e,\ b^{-1}ab = a^7\rangle$.

Case I: When $q \equiv 1$ or $7 \pmod 8$.

The primitive central idempotents of the semisimple group algebra $\mathbb{F}_q G$ by Theorem 3 are $e_1^{'} = \widehat{b}\widehat{a}$, $e_2^{'} = \widehat{\langle a^2, b\rangle} - \widehat{G}, e_3^{'} = \widehat{\langle a^2, ab\rangle} - \widehat{G}$, $e_4^{'} = \widehat{\langle a\rangle} - \widehat{G}$ and $e_2^1 = \frac{1}{4}[1 - a^2 + a^4 - a^6]$, $e_3^1 = \frac{1}{8}(1 - a^4)(2 + \alpha a - \alpha a^3)$ and $e_3^3 = \frac{1}{8}(1 - a^4)(2 - \alpha a + \alpha a^3)$. For $x_k = a^k b$,

| $e$ | $d[(\mathbb{F}_q G)e]$ |
|---|---|
| $\widehat{x}_k e_2^1$ | $4 \leqslant d[(\mathbb{F}_q G)\widehat{x}_k e_2^1] \leqslant 8$ |
| $\widehat{x}_k e_3^1$ | $d[(\mathbb{F}_q G)e_3^1] \leqslant d[(\mathbb{F}_q G)\widehat{x}_k e_3^1] \leqslant 12$ |
| $\widehat{x}_k e_3^3$ | $d[(\mathbb{F}_q G)e_3^3] \leqslant d[(\mathbb{F}_q G)\widehat{x}_k e_3^3] \leqslant 12$ |
| $f_1$ | $4 \leqslant d[(\mathbb{F}_q G)f_1] \leqslant 12$ |
| $f_2$ | $d[(\mathbb{F}_q G)e_3^1] \leqslant d[(\mathbb{F}_q G)f_2]$ |
| $f_3$ | $d[(\mathbb{F}_q G)e_3^3] \leqslant d[(\mathbb{F}_q G)f_3]$ |

where $f_1 = (\widehat{x}_k \pm \widehat{x}_k a(1-\widehat{x}_k))\, e_2^1$, $f_2 = (\widehat{x}_k \pm \widehat{x}_k a(1-\widehat{x}_k))\, e_3^1$ and $f_3 = (\widehat{x}_k \pm \widehat{x}_k a(1-\widehat{x}_k))\, e_3^3$.

Case II: When $q \equiv 3$ or $5 \pmod 8$.

The primitive central idempotents of the semisimple group algebra $\mathbb{F}_q G$ by Theorem 2 are $e_1' = \widehat{ba}$, $e_2' = \widehat{\langle a^2, b\rangle} - \widehat{G}$, $e_3' = \widehat{\langle a^2, ab\rangle} - \widehat{G}$, $e_4' = \widehat{\langle a\rangle} - \widehat{G}$, $e_1 = \frac{1}{4}[1 - a^2 + a^4 - a^6]$ and $e_2 = \frac{1}{2}(1 - a^4)$. For $x_k = a^k b$,

| $e$ | $d[(\mathbb{F}_q G)e]$ |
|---|---|
| $\widehat{x}_k e_1$ | 8 |
| $\widehat{x}_k e_2$ | 4 |
| $f_1$ | $4 \leqslant d[(\mathbb{F}_q G) f_1]$ |
| $f_2$ | $2 \leqslant d[(\mathbb{F}_q G) f_2] \leqslant 12$ |

where $f_1 = (\widehat{x}_k \pm \widehat{x}_k a(1 - \widehat{x}_k))\, e_1$ and $f_2 = (\widehat{x}_k \pm \widehat{x}_k a(1 - \widehat{x}_k))\, e_2$.

**Acknowledgement**

Research supported by CSIR, India, is gratefully acknowledged.

## References

[1] G. K. Bakshi, S. Gupta and I. B. S. Passi, *The algebraic structure of finite metabelian group algebras*, Communications in Algebra, Vol.**43**, N.**6**, 2015, pp.2240-2257.

[2] F. S. Dutra, R. A. Ferraz, C.P. Milies, *Semisimple group codes and dihedral codes*, Algebra and Discrete Mathematics, N.**3**, 2009, pp.28-48.

[3] R. E. Sabin, S. J. Lomonaco, *Metacyclic error-correcting codes*, Applicable Algebra in Engineering, Communication and Computing, Vol.**6**, N.**3**, 1995, pp.191-210.

[4] S. Assuena, C. P. Milies, *Good codes from metacyclic groups*, Contemporary Math., Vol.**727**, 2019, pp.39-47.

### CONTACT INFORMATION

**Shalini Gupta, Priya Rani**

Department of Mathematics,
Punjabi University, Patiala,
P.O. Box 147002, Punjab, India.
*E-Mail*(*s*): shalini@pbi.ac.in, priyaahuja149@gmail.com

Received by the editors: 19.03.2020
and in final form 17.03.2021.