Malaysian Journal of Mathematical Sciences 7(S): 101-116 (2013)
Special Issue: The 3rd International Conference on Cryptology & Computer Security 2012 (CRYPTOLOGY2012)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

Group Codes Define Over Dihedral Groups of Small Order

[1*]Denis C.K. Wong and [2]Ang M.H

[1]Department of Applied Mathematics and Actuarial Science,
Faculty of Engineering and Science,
Universiti Tunku Abdul Rahman Setapak,
Off Jalan Genting Kelang, 53300, Kuala Lumpur

[2]School of Mathematical Sciences, Universiti Sains Malaysia,
11800 Pulau Pinang, Malaysia

Email: deniswong@utar.edu.my and mathamh@cs.usm.my

*Corresponding author

ABSTRACT

The study of group codes as an ideal in a group algebra has been developed long time ago. If char(F) does not divides $|G|$, then FG is semisimple, and hence decomposes into a direct sum $FG = \bigoplus_i FGe_i$ where FGe_i are minimal ideals generated by the idempotent e_i. The idempotent e_i provides some useful information on determining the minimum distance of group codes. In this paper, we study dihedral group codes generated by linear idempotents and nonlinear idempotents for dihedral groups of order 6, 8, 10 and 12. Our primary task is to determine the parameters of these families of group codes in order to obtain codes which near to attain the Singleton bound.

Keywords: Group algebra, group codes, Singleton bound, linear idempotents, nonlinear idempotents.

1. INTRODUCTION

Error correction or detection has become an important issue with the problem of reliable communication over noisy channels. Since then group algebra codes have been a focus of interest in the mathematical community in relating codes structures by using algebraic structures. Group algebra codes gained interest after Berman showed in 1967 that cyclic codes and

Reed Muller codes can be studied as ideals in a group algebra *FG*, where *F* is a finite field and *G* is considered, in each case, a finite cyclic group and a 2-group respectively. On the other hands, the first investigations of non-Abelian group algebra code was done by F. J. Macwilliams. Recently, P. Hurley and T. Hurley (Hurley (2007)) construct group ring codes from zero divisors and unit in group rings in which case the codes defined may not be ideal. In this paper, we study codes defined over group algebra, which is an ideal.

A group algebra code in FG is defined as a one-sided (left or right) ideal in FG. If G is cyclic or Abelian, then every ideal in FG is the cyclic or Abelian code, respectively. Refer (Berman (1967) and (Berman (1989)) for more details on cyclic and abelian group codes, and (How and Denis (2004)) for a class of nonabelian group algebra codes. The studies of group algebra code in FG depended solidly on the choices of F and G. In general, we can study group algebra code in FG from the following point of views: If gcd ($char(F)$, $|G|$) = 1, then FG is semisimple (refer Theorem 15.2 in (Isaacs, 1997)), that is, FG is a direct sum of some minimal ideals, say $FG = \bigoplus_{j=1}^{s} I_j$. Each I_j is generated by an idempotent e_j, i.e., $I_j = FGe_j$. Let $E = \{e_j\}_{j=1}^{s}$. Any ideal I of FG is a direct sum of some of the I_j, say $I = \bigoplus_{k=1}^{t} I_{j_k}$, $t \le s$. We say that I is generated by $\{e_{j_k}\}_{k=1}^{t}$. Let $\mu = E \setminus \{e_{j_k}\}_{k=1}^{t}$. Then $I = \left\{u \in FG \middle| ue_{j_r} = 0 \forall e_{j_r} \in \mu\right\}$.

For technical reason, we denote I by I_μ. Note that μ plays the role of parity check matrix defining a linear code, and so we expect to derive some information about the minimum distance of I_μ from μ. Recall some notation and definitions: The length n of a group code $I_\mu \triangleleft FG$ is defined to be $|G|$. The weight of any element $u = \sum_{g \in G} \lambda_g g$ is equal to $\left|\left\{\lambda_g \middle| \lambda_g \ne 0\right\}\right|$ and is denoted by $wt(u)$. If I_μ has dimension k (as a vector space over F) and minimum distance $d = d(I_\mu) = \min\left\{wt(u) \middle| 0 \ne u \in I_u\right\}$, then I_μ is called an (n,k,d)–group code. For more information on coding theory, please refer (Sloane and Macwilliam, 1978).

In this paper, we consider group algebra codes defined over dihedral groups of order 6, 8, 10 and 12. Some basics properties of nonabelian group codes will be derived in Section 2, then some properties in dihedral group will be derived. Finally, the minimum distance of dihedral groups of order 6, 8, 10 and 12 will be studies in Section 3 and hence some group algebra codes which near to attain the Singleton bound will be obtained.

2. PRELIMINARY

Most objects in this paper are represented in term of group algebra FG. The group algebra $FG=\left\{\sum_{g\in G} a_g g \mid a_g \in F\right\}$ is the free $F-$module over a finite group G where G can be regarded as an $F-$basis for FG. The addition and scalar multiplication are defined as follows. For any $u=\sum_{g\in G}\lambda_g g$, $v=\sum_{g\in G}\beta_g g\in FG$ and $\lambda\in F$, $u+v=\sum_{g\in G}\left(\lambda_g+\beta_g\right)g$ and $\lambda u=\sum_{g\in G}(\lambda\lambda_g)g$. Moreover, multiplication in G induces multiplication in FG as $u.v=\sum_{k\in G}\gamma_k k$ where $\gamma_k=\sum_{gh=k\in G}\lambda_g\beta_h$. By these operations, FG is an associative $F-$algebra with identity $1=1_F 1_G$ where 1_G and 1_F are the identity elements of G and F, respectively. G can be viewed as contained in FG, and hence the elements of G constitute the coding basis for codes viewed as subspaces of FG. We view G as $\sum_{g\in G} g$ in FG. Moreover, for $A=\sum_{g\in G}a_g g\in FG$, define $A^{(-1)}=\sum_{g\in G}a_g g^{-1}$. For more information on group algebra, please refer (Passman (1977)).

From now onward, we use the following definition.

Definition 2.1. Let G be a group and F be a field such that $\gcd\left(char\left(F\right),\left|G\right|\right)=1$. If E is the set of all idempotents of FG and $\mu\subseteq E$, then the group code generated by μ is $I_\mu=\left\{u\in FG \,\middle|\, ue=0\forall e\in\mu\right\}$.

Proposition 2.2. The group algebra codes I_μ defined in Definition 2.1 is a linear code over F.

For any positive integer $n\geq 2$, the dihedral group of order $2n$ can be represented as $D_{2n}=\left\{r^i s^j \mid 0\leq i\leq n-1, 0\leq j\leq 1, r^n=s^2=1, rs=sr^{-1}\right\}$. From now onward, all groups G are D_{2n} and all group algebra codes I_μ are defined over D_{2n} . First, to obtain the dimension of I_μ, we need the following results.

Theorem 2.3. (Theorem 8.7, James and Liebeck (1993)). Let K be a finite group of order n, and F be an algebraically closed field with $\gcd\left(char\left(F\right),\left|G\right|\right)=1$. Then $FK \cong Mat_{n_1}(F)\oplus ...\oplus Mat_{n_s}(F)$, where $n = n_1^{\ 2} + ... + n_s^{\ 2}$. FK has exactly s nonisomorphic irreducible modules, of dimensions $n_1,...,n_s$, and s is the number of conjugacy classes of K .

Remark 2.4. Since $FG=\left(\underset{e_i\in E_L}{\oplus} FGe_i\right)\oplus\left(\underset{e_j\in E_N}{\oplus} FGe_j\right)$ where E_L is the set consists of all linear idempotents in FG and E_N is the set consists of all nonlinear idempotents in FG; and furthermore $E = E_L \cup E_N$. Note that if $e_i \in E_L$, then $\dim\left(FGe_i\right)=1$; and if $e_i \in E_N$, then $\dim\left(FGe_i\right)=2$. (Section 18.3, James and Liebeck (1993)).

Therefore, if $\mu = \mu_L \cup \mu_N$ where $\mu_L \subseteq E_L$ and $\mu_N \subseteq E_N$, then $\dim\left(I_\mu\right)=\dim\left(FG\right)-\left|\mu_L\right|-2^2\left|\mu_N\right|$.

As $\dim\left(FG\right)=\left|G\right|=2n$, then $\dim\left(I_\mu\right)=2n-\left|\mu_L\right|-2^2\left|\mu_N\right|$.

The next theorem on the number of conjugacy classes of D_{2n} can be found in (Section 18.3; James and Liebeck (1993)).

Theorem 2.5. The conjugacy classes of D_{2n} are as follows:

(i) If n is odd, then D_{2n} has $\frac{1}{2}(n+3)$ conjugacy classes: $\{1\},\{r,r^{-1}\},...,\{r^{(n-1)/2},r^{-(n-1)/2}\},\{s,rs,...,r^{n-1}s\}$.

(ii) If n is even and $n = 2m$, then D_{2n} has $m+3$ conjugacy classes:

$$\{1\},\{r^m\},\{r,r^{-1}\},...,\{r^{m-1},r^{-(m-1)}\},\{r^{-2j}s:0\le j\le m-1\},\{r^{2j+1}s:0\le j\le m-1\}.$$

By using Theorem 2.5 and results from (Chapter 13, 14 and 15; James and Liebeck (1993)), we obtain the following proposition. Note that $D_{2n}{}'$ denote the commutator subgroup of D_{2n} .

Proposition 2.6. Let D_{2n} be the dihedral group of order $2n$, where n is any integer, then

(a) $$\left|Irr\left(D_{2n}\right)\right| = \begin{cases} \frac{1}{2}(n+3), & \text{if } n \text{ is prime,} \\ \frac{1}{2}(n+6), & \text{if } n = 2p, \text{ where } p \text{ is any prime.} \end{cases}$$

(b) $$D_{2n}' = \begin{cases} \langle r \rangle, & \text{if } n \text{ is prime,} \\ \langle r^2 \rangle, & \text{if } n = 2p, \text{ where } p \text{ is a prime.} \end{cases}$$

(c) D_{2n} has $\left| D_{2n} / D_{2n}' \right|$ linear characters, where

$$\left| D_{2n} / D_{2n}' \right| = \begin{cases} 2, & \text{if } n \text{ is prime,} \\ 4, & \text{if } n = 2p, \text{ where } p \text{ is a prime.} \end{cases}$$

(d) D_{2n} has ϖ non-linear characters, where

$$\varpi = \begin{cases} \frac{n-1}{2}, & \text{if } n \text{ is prime,} \\ \frac{n-2}{2}, & \text{if } n = 2p, \text{ where } p \text{ is a prime.} \end{cases}$$

Proof. Part (a) is just a direct consequence from the fact that the number of irreducible characters is equal to the number of conjugacy classes. For part (b), since $\left| D_{2n} / \langle r \rangle \right| = 2$ and so $D_{2n} / \langle r \rangle$ is abelian, then $D_{2n}' \subseteq \langle r \rangle$, refer Theorem 3.10 in (Isaacs, 1992). If n is prime, then $D_{2n}' = 1$ or $D_{2n}' = \langle r \rangle$. If $D_{2n}' = 1$, then D_{2n} is abelian which is impossible. Therefore, we conclude that $D_{2n}' = \langle r \rangle$. Next, assume $n = 2p$, where p is a prime. Note that $\left| D_{2n} / \langle r^2 \rangle \right| = \left| D_{2n} / \langle r \rangle \right| \left| \langle r \rangle / \langle r^2 \rangle \right| = 4$ and so $D_{2n} / \langle r^2 \rangle$ is abelian, then $D_{2n}' \subseteq \langle r^2 \rangle$. Since $\left| \langle r^2 \rangle \right| = p$, then either $D_{2n}' = 1$ or $D_{2n}' = \langle r^2 \rangle$, and hence the result will follow directly. Part (c) follows from part (b). Part (d) follows directly from part (a) and (c). **Q.E.D.**

The following lemma is used to obtain the minimum distance of I_μ.

Lemma 2.7. If $\mu_1 \subseteq \mu_2$, then $I_{\mu_2} \subseteq I_{\mu_1}$ and so $d\left(I_{\mu_1}\right) \leq d\left(I_{\mu_2}\right)$.

Proof. If $u \in I_{\mu_2}$, then $ue = 0$ for all $e \in \mu_2$. Since $\mu_1 \subseteq \mu_2$, then $ue = 0$ for all $e \in \mu_1$ and so $u \in I_{\mu_1}$. For the second assertion, assume $d\left(I_{\mu_2}\right) = t$. If $u \in I_{\mu_2}$ with $wt(u) = t$ and $wt(u) \leq wt(v)$, $\forall v \in I_{\mu_1}$, then $d\left(I_{\mu_1}\right) = t$. On the other hand, if $u \in I_{\mu_2}$ with $wt(u) = t$ and $wt(u) > wt(v)$, for some $v \in I_{\mu_1}$, then $d\left(I_{\mu_1}\right) < t$. Thus, the result follows directly. **Q.E.D.**

3. MINIMUM DISTANCE OF DIHEDRAL GROUP CODES

3.1 Codes defined over FD_6

Let $H = \langle r \mid r^3 = 1 \rangle$ and so $D_6 = H \cup sH$. From Proposition 2.6, D_6 consists of three irreducible characters (two are linear and one is nonlinear) χ_1, χ_2 and χ_3, and each of these characters will correspond to a unique idempotent (refer Proposition 14.10; James and Liebeck, 1993) as follows:

$$\chi_1 \leftrightarrow e_1 = \frac{1}{6}(H + sH),\ \chi_2 \leftrightarrow e_2 = \frac{1}{6}(H - sH) \text{ and } \chi_3 \rightarrow e_3 = 1 - \frac{1}{3}H.$$

Let $u = \lambda_1 + \lambda_2 r + \lambda_3 r^2 + \lambda_4 s + \lambda_5 rs + \lambda_6 r^2 s$ be any elements in $FD_6, \lambda_i \in F$ for i = 1, 2, 3, 4, 5, 6, then

$$ue_1 = \left(\sum_{i=1}^{6} \lambda_i\right) e_1 \tag{1}$$

$$ue_2 = \left(\sum_{i=1}^{3} \lambda_i - \sum_{i=4}^{6} \lambda_i\right) e_2 \tag{2}$$

$$\begin{aligned} ue_3 = \frac{1}{3}\big[&(2\lambda_1 - \lambda_2 - \lambda_3) + (-\lambda_1 + 2\lambda_2 - \lambda_3)r + (-\lambda_1 - \lambda_2 + 2\lambda_3)r^2 + \\ &(2\lambda_4 - \lambda_5 - \lambda_6)s + (-\lambda_4 + 2\lambda_5 - \lambda_6)rs + (-\lambda_4 - \lambda_5 + 2\lambda_6)r^2 s\big] \end{aligned} \tag{3}$$

Lemma 3.1. Let e_1, e_2 and e_3 be those idempotents in FD_6 as constructed above, then:

(i) $d\left(I_{\{e_i\}}\right) = 2$ for $i = 1, 2$.

(ii) $d\left(I_{\{e_3\}}\right) = 3$.

Proof. We prove part (i) for the case $i=1$. The case $i=2$ can be proved in a similar manner. Assume $u=\lambda g\in I_{\{e_1\}}$ for any $g\in D_6$ and $0\neq\lambda\in F$ such that $wt(u)=1$. By equation (1), $ue_1=\lambda e_1\neq 0$. Hence, we conclude that $u=\lambda g\notin I_{\{e_1\}}$ and so $d\left(I_{\{e_1\}}\right)\geq 2$. Clearly, $u=g-h\in I_{\{e_1\}}$ for any distinct $g,h\in D_6$ because by equation (1), $ue_1=(1-1)e_1=0$ and so $d\left(I_{\{e_1\}}\right)=2$.

For part (ii): if $u=\lambda g\in I_{\{e_3\}}$ with $wt(u)=1$, then $0\neq\lambda\in F$. However, by using equation (3), $ue_3=\lambda ge_3\neq 0$ and so $u=\lambda g\notin I_{\{e_3\}}$ which implies $d\left(I_{\{e_3\}}\right)>1$. Next, we check whether $I_{\{e_3\}}$ consist of codewords of weight 2. Assume $u=\lambda_1 g_1+\lambda_2 g_2\in I_{\{e_3\}}$ such that $wt(u)=2$, then we have either $g_1,g_2\in H$, $g_1,g_2\in sH$ or $g_1\in H$ and $g_2\in sH$. For each of these possibilities, by using equation (3), we will obtain a set of equations in terms of λ_1 and λ_2, and upon solving will give the solution $\lambda_1=\lambda_2=0$ which is impossible. Thus, $d\left(I_{\{e_3\}}\right)>2$. Finally, consider $u=H$, then $ue_3=H\left(1-\frac{1}{3}H\right)=H-H=0$ and so $u=H\in I_{\{e_3\}}$ and hence $d\left(I_{\{e_3\}}\right)=3$. **Q.E.D.**

From Lemma 3.1 and Remark 2.4, we see that $I_{\{e_i\}}$ is a $(6,5,2)-$group code for $i=1,2$ which attain the singleton bound and so are *MDS* codes. However, $I_{\{e_3\}}$ is a $(6,2,3)-$group code which is not an *MDS* code.

Theorem 3.2. Let e_1, e_2 and e_3 be those idempotents in FD_6, then:

(i) $d\left(I_{\{e_1,e_2\}}\right)=2$

(ii) $d\left(I_{\{e_i,e_3\}}\right)=6$ for $i=1,2$.

Proof. By Lemma 2.7 and Lemma 3.1, we notice that $d\left(I_{\{e_i,e_j\}}\right)\geq 2$ for all $i\neq j$, $i=1,2$ and $j=2,3$. For part (i), if $u=\lambda_4 s+\lambda_5 rs+\lambda_4\neq 0$ and $\lambda_5\neq 0$, then by using equation (1) and (2), $ue_1=(\lambda_4+\lambda_5)e_1$ and $ue_2=(-\lambda_4-\lambda_5)e_2$

then $ue_1 = ue_2 = 0$ if and only if $\lambda_4 = -\lambda_5$. Hence, $u = \lambda_4 s + \lambda_5 rs \in I_{\{e_1, e_2\}}$. Therefore, $d\left(I_{\{e_1, e_2\}}\right) = 2$.

For part (ii), the proof will be similar. We need to find an element with weight equal to 6. It can be checked that there are no codewords with weight less than 6 in $I_{\{e_2, e_3\}}$.

We now check that $u = \lambda_1 + \lambda_2 r + \lambda_3 r^2 + \lambda_4 s + \lambda_5 rs + \lambda_6 r^2 s$ is a word of $I_{\{e_2, e_3\}}$. By using equation (2) and (3), we obtain

$$ue_2 = (\lambda_1 + \lambda_2 + \lambda_3 - \lambda_4 - \lambda_5 - \lambda_6)e_2 \text{ and}$$

$$\begin{aligned} ue_3 = \frac{1}{3}\big[&(2\lambda_1 - \lambda_2 - \lambda_3) + (-\lambda_1 + 2\lambda_2 - \lambda_3)r + (-\lambda_1 - \lambda_2 + 2\lambda_3)r^2 \\ &+ (2\lambda_4 - \lambda_5 - \lambda_6)s + (-\lambda_4 + 2\lambda_5 - \lambda_6)rs + (-\lambda_4 - \lambda_5 + 2\lambda_6)r^2 s\big]. \end{aligned}$$

Thus, $ue_2 = ue_3 = 0$ if and only if

$$(\lambda_1 + \lambda_2 + \lambda_3 - \lambda_4 - \lambda_5 - \lambda_6) = 0 \qquad \text{(i)}$$

$$\left.\begin{array}{l} 2\lambda_1 - \lambda_2 - \lambda_3 = 0 \\ -\lambda_1 + 2\lambda_2 - \lambda_3 = 0 \\ -\lambda_1 - \lambda_2 + 2\lambda_3 = 0 \end{array}\right\} \qquad \text{(ii)}$$

$$\left.\begin{array}{l} 2\lambda_4 - \lambda_5 - \lambda_6 = 0 \\ -\lambda_4 + 2\lambda_5 - \lambda_6 = 0 \\ -\lambda_4 - \lambda_5 + 2\lambda_6 = 0 \end{array}\right\} \qquad \text{(iii)}$$

The unique solution for (ii) is $\lambda_1 = \lambda_2 = \lambda_3 \neq 0$ and for (iii) is $\lambda_4 = \lambda_5 = \lambda_6 \neq 0$. Hence, from (i), $\lambda_1 + \lambda_1 + \lambda_1 - \lambda_4 - \lambda_4 - \lambda_4 = 0$ which implies that $\lambda_1 = \lambda_4 \neq 0$. Therefore, we obtain a nonzero solution and so $d\left(I_{\{e_2, e_3\}}\right) = 6$. **Q.E.D.**

In Theorem 3.2, we have constructed two families of group codes, $I_{\{e_1, e_2\}}$ is a $(6,4,2)-MDS$ group code and $I_{\{e_i, e_3\}}$ is a $(6,1,6)-$group code for $i = 1,2$.

3.2 Codes defined over FD_8

Let $H = \langle r \mid r^4 = 1 \rangle$ and so $D_8 = H \cup sH$. Note that $K = \langle r^2 \mid r^4 = 1 \rangle \leq H$. From Lemma 2.6, we see that D_8 consists of 5 irreducible characters, in which case, four of them are linear characters and one is nonlinear character. Each of this character will correspond to a unique idempotent as follows:

(a) Idempotents correspond to linear characters:

$$\chi_1 \leftrightarrow e_1 = \frac{1}{8}(H+sH), \chi_2 \leftrightarrow e_2 = \frac{1}{8}(H-sH),$$

$$\chi_3 \leftrightarrow e_3 = \frac{1}{8}(1-r)(1+s)K, \text{ and } \chi_4 \leftrightarrow e_4 = \frac{1}{8}(1-r)(1-s)K.$$

(b) Idempotents correspond to the nonlinear character χ_5 of degree 2:

$$\chi_5 \rightarrow e_5 = \frac{1}{4}(2-2r^2) = \frac{1}{2}(1-r^2).$$

Let $u = \lambda_1 + \lambda_2 r + \lambda_3 r^2 + \lambda_4 r^3 + \lambda_5 s + \lambda_6 rs + \lambda_7 r^2 s + \lambda_8 r^3 s$ be any element in FD_8 such that $\lambda_i \in F$ for i = 1, 2, 3, 4, 5, 6, 7 and 8, then

$$ue_1 = \left(\sum_{i=1}^{8} \lambda_i\right) e_1 \tag{4}$$

$$ue_2 = \left(\sum_{i=1}^{4} \lambda_i - \sum_{i=5}^{8} \lambda_i\right) e_2 \tag{5}$$

$$ue_3 = \left(\sum_{i=1,3,5,7} \lambda_i - \sum_{i=2,4,6,8} \lambda_i\right) e_3 \tag{6}$$

$$ue_4 = \left(\sum_{i=1,3,6,8} \lambda_i - \sum_{i=2,4,5,7} \lambda_i\right) e_4 \tag{7}$$

$$\begin{aligned} ue_5 = \frac{1}{2}\big[&(\lambda_1 - \lambda_3) + (\lambda_2 - \lambda_4) r + (-\lambda_1 + \lambda_3) r^2 + (-\lambda_2 + \lambda_4) r^3 \\ &+ (\lambda_5 - \lambda_7) s + (\lambda_6 - \lambda_8) rs + (-\lambda_5 + \lambda_7) r^2 s + (-\lambda_6 + \lambda_8) r^3 s\big] \end{aligned} \tag{8}$$

Lemma 3.3. Let $\mu = \{e_1, e_2, e_3, e_4\}$, where e_1, e_2, e_3 and e_4 are the linear idempotents in FD_8 if $\beta \subseteq \mu$, then $d(I_\beta) = 2$.

Proof. If $\beta \subseteq \mu$, then there are four cases to be considered, which are $|\beta| = 1, 2, 3,$ or 4. From Lemma 2.7, we only need to show that $d(I_\beta) = 2$ for $|\beta|$ = 4. If $|\beta|$ = 4, then e_1, e_2, e_3, e_4 are all in β. If $u = \lambda_i g_i, \lambda_i \neq 0$ and $wt(u) = 1$, then $ue_1 = \lambda_i e_1 \neq 0, ue_2 = (\lambda_i \chi_2(g_i)) e_2 \neq 0, ue_3 = (\lambda_i \chi_3(g_i)) e_3 \neq 0$ and $ue_4 = (\lambda_i \chi_4(g_i)) e_4 \neq 0$. Hence, $u = \lambda_i g_i \notin I_\beta$ indicates that $d(I_\beta) \geq 2$.

Next, consider $u = \lambda_1 + \lambda_3 r^2$, by using equation (4) to (7):

$ue_1 = (\lambda_1 + \lambda_3)e_1, ue_2 = (\lambda_1 + \lambda_3)e_2, ue_3 = (\lambda_1 + \lambda_3)e_3$ and $ue_4 = (\lambda_1 + \lambda_3)e_4$. $ue_1 = ue_2 = ue_3 = ue_4 = 0$ if and only if $\lambda_1 = -\lambda_3 \neq 0$. Clearly, $u \in I_\beta$ and so $d(I_\beta) = 2$. **Q.E.D.**

From this lemma, we immediately conclude that i $\beta \subseteq \mu$, then I_β is a $(8, 8-|\beta|, 2)-$ group code. Furthermore, I_β is a *MDS* code if and only if $|\beta| = 1$. The next result can be proved by using similar method as Lemma 3.3.

Lemma 3.4. Let $\mu = \{e_5\}$ where e_5 is the nonlinear idempotent in FD_8, then $d(I_{\{e_5\}}) = 2$ and $\dim(I_{\{e5\}}) = 4$. Furthermore, let $u = \lambda_i g_i + \lambda_j g_j, \lambda_i \neq 0$ and $\lambda_j \neq 0$ with $g_i \neq g_j \in D_8$, then $u \in I_{\{e5\}}$ if and only if $g_i, g_j \in H$.

Theorem 3.5. Let $\mu = \{e, e_5\}$ where e is any one of the linear idempotents and e_5 is the nonlinear idempotent in FD_8, then $d(I_\mu) = 4$ and so I_μ is a $(8,3,4)-$group code.

Proof. Without loss of generality, we only prove for the case $\mu = \{e_1, e_5\}$. By Lemma 2.7 and Lemma 3.3, we know that $d(I_\mu) \geq 2$. By the second statement in Lemma 3.4, if $u = \lambda_i g_i + \lambda_j g_j, \lambda_i \neq 0$ and $\lambda_j \neq 0$, then either g_i, g_j in H or g_i, g_j in sH or one in H and the other in sH will not produce a codeword in I_μ. This follows from equations (4) and (8) in which always gives the solution $\lambda_i = \lambda_j = 0$. Next, for $u = \lambda_i g_i + \lambda_j g_j + \lambda_k g_k, \lambda_i \neq 0$ and $\lambda_j \neq 0$ and $\lambda_k \neq 0$, we have either g_i, g_j, g_k all lies in H (resp. sH) or g_i, g_j lies in H (resp. sH) but g_k lies in sH (resp. H). For both cases, by using equations (4) and (8), u is not contained in I_μ. Finally, if $u = \lambda_1 + \lambda_2 r + \lambda_3 r^2 + \lambda_4 r^3, \lambda_1 \neq 0, \lambda_2 \neq 0, \lambda_3 \neq 0$ and $\lambda_4 \neq 0$, then $ue_1 = (\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4)e_1$ and $ue_5 = (\lambda_1 - \lambda_3)e_5 + (\lambda_2 - \lambda_4)re_5$.

Thus, $ue_1 = ue_5 = 0$ if and only if $\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = 0$ and $\lambda_1 - \lambda_3 = 0$ and $\lambda_2 - \lambda_4 = 0$. The only solution for the above is $\lambda_1 = \lambda_3 \neq 0$ and $\lambda_2 = \lambda_4 \neq 0$, So, $\lambda_1 + \lambda_2 + \lambda_1 + \lambda_2 = 0$ implies that $2\lambda_1 + 2\lambda_2 = 0$ and so $\lambda_1 = -\lambda_2 \neq 0$. Thus, we obtain a set of nonzero solution and so $u \in u \in I_\mu$. In other word, $d\left(I_\mu\right) = 4$. **Q.E.D.**

Theorem 3.6. Let e_1, e_2, e_3, e_4, e_5 be the idempotents in FD_8, then $d\left(I_{\{e_i, e_j, e_5\}}\right) = 4$ and $\dim\left(I_{\{e_i, e_j, e_5\}}\right) = 2$, where $i, j = 1,2,3,4, i \neq j$.

Proof. By Lemma 2.7 and Theorem 3.5, we only need to show that there exists a codeword of weight 4 in $I_{\{e_i, e_j, e_5\}}$, where $i, j = 1,2,3,4, i \neq j$. Since most calculations are routined, then we only state a codeword of weight 4 in each group code.

(i) $u = \lambda_1 + \lambda_2 r + \lambda_3 r^2 + \lambda_4 r^3 \in I_{\{e_1, e_2, e_5\}}$.
(ii) $u = \lambda_1 + \lambda_3 r^2 + \lambda_5 s + \lambda_7 r^2 s \in I_{\{e_1, e_3, e_5\}}$.
(iii) $u = \lambda_1 + \lambda_3 r^2 + \lambda_6 rs + \lambda_8 r^3 s \in I_{\{e_1, e_4, e_5\}}$.
(iv) $u = \lambda_1 + \lambda_3 r^2 + \lambda_6 rs + \lambda_8 r^3 s \in I_{\{e_2, e_3, e_5\}}$.
(v) $u = \lambda_1 + \lambda_3 r^2 + \lambda_6 rs + \lambda_7 r^2 s \in I_{\{e_2, e_4, e_5\}}$.
(vi) $u = \lambda_1 + \lambda_2 r + \lambda_3 r^2 + \lambda_4 r^3 \in I_{\{e_3, e_4, e_5\}}$.

Q.E.D.

Corollary 3.7. $d\left(I_{\{e_i, e_j, e_k, e_5\}}\right) = 1$ and $d\left(I_{\{e_i, e_j, e_k, e_5\}}\right) = 8$, where $i, j, k \in \{1,2,3,4\}, i \neq j \neq k$.

Proof. The proof is similar to Theorem 3.6, and so without loss of geneality we consider only $\mu = \{e_1, e_2, e_3, e_5\}$, in the case of $\mu = \{e_1, e_2, e_5\}$, $d\left(I_{\{e_1, e_2, e_5\}}\right) = 4$, thus we may assume that the code generated by $\mu = \{e_1, e_2, e_3, e_5\}$ has minimum distance greater than or equal to 4.

By using equations (4), (5), (6) and (8), it can be shown that no codeword of weight 4, 5, 6, and 7 in $I_{\{e_1, e_2, e_5\}}$ and so we only exhibit there is an element of weight 8 in $I_{\{e_1, e_2, e_5\}}$.

If $u = \lambda_1 + \lambda_2 r + \lambda_3 r^2 + \lambda_4 r^3 + \lambda_5 s + \lambda_6 rs + \lambda_7 r^2 s + \lambda_8 r^3, \lambda_i \neq 0$ for $i = 1, 2, 3, ..., 8$, then

$$ue_1 = (\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 + \lambda_7 + \lambda_8) e_1,$$

$$ue_2 = (\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 - \lambda_5 - \lambda_6 - \lambda_7 - \lambda_8) e_2,$$

$$ue_3 = (\lambda_1 - \lambda_2 + \lambda_3 - \lambda_4 + \lambda_5 - \lambda_6 + \lambda_7 - \lambda_8) e_3 \text{ and}$$

$$\begin{aligned} ue_5 = \frac{1}{2}\big[& (\lambda_1 - \lambda_3) + (\lambda_2 - \lambda_4) r + (-\lambda_1 + \lambda_3) r^2 + (-\lambda_2 + \lambda_4) r^3 \\ & + (\lambda_5 - \lambda_7) s + (\lambda_6 - \lambda_8) rs + (-\lambda_5 + \lambda_7) r^2 s + (-\lambda_6 + \lambda_8) r^3 s \big] \end{aligned}.$$

Thus, $ue_1 = ue_2 = ue_3 = ue_5 = 0$ if and only if

$$\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 + \lambda_7 + \lambda_8 = 0,$$

$$\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 - \lambda_5 - \lambda_6 - \lambda_7 - \lambda_8 = 0,$$

$$\lambda_1 - \lambda_2 + \lambda_3 - \lambda_4 + \lambda_5 - \lambda_6 + \lambda_7 - \lambda_8 = 0,$$

$$\lambda_1 = \lambda_3, \lambda_2 = \lambda_4, \lambda_5 = \lambda_7 \text{ and } \lambda_6 = \lambda_8.$$

Hence, (i) $\lambda_1 + \lambda_2 + \lambda_5 + \lambda_6 = 0$
(ii) $\lambda_1 + \lambda_2 - \lambda_5 - \lambda_6 = 0$
(iii) $\lambda_1 - \lambda_2 + \lambda_5 - \lambda_6 = 0$

Upon solving (i) to (iii), we will obtain nonzero solution. Hence, $u \in I_{\{e_1, e_2, e_3, e_5\}}$ and so $d\left(I_{\{e_1, e_2, e_3, e_5\}}\right) = 8$.

3.3 Codes defined over FD_{10}

Let $H = \langle r \mid r^5 = 1 \rangle$ and so $D_{10} = H \cup sH$. From Lemma 2.6, we see that D_{10} consists of 4 irreducible characters, in which case, two of them are linear characters and the other two are nonlinear character. Each of this character will correspond to a unique idempotent as follows

(a) Idempotents correspond to linear characters:

$$\chi_1 \leftrightarrow e_1 = \frac{1}{10}\left(H + sH\right) \text{ and } \chi_2 \leftrightarrow e_2 = \frac{1}{10}\left(H - sH\right)$$

(b) Idempotents correspond to the nonlinear character χ_5 of degree 2:

$$\chi_3 \to e_3 = \frac{1}{10}\left(4 + \left(-1+\sqrt{5}\right)\left(r + r^4\right) + \left(-1-\sqrt{5}\right)\left(r^2 + r^3\right)\right) \text{ and}$$

$$\chi_4 \to e_4 = \frac{1}{10}\left(4 + \left(-1+\sqrt{5}\right)\left(r^2 + r^3\right) + \left(-1-\sqrt{5}\right)\left(r + r^4\right)\right)$$

We sumarize our results in the following theorem. Indeed most of them can be proved by using similar argument as for group codes in FD_6 and FD_8.

Theorem 3.8. Let $\mu_L = \{e_1, e_2\}$ and $\mu_N = \{e_3, e_4\}$ be all idempotents in FD_{10} which is defined as above.

(i) If $\beta \subseteq \mu_L$ such that $|\beta| = 1$, then $d\left(I_\beta\right) = 2$ and $\dim\left(I_\beta\right) = 9$.

(ii) If $\beta \subseteq \mu_N$ such that $|\beta| = 1$, then $d\left(I_\beta\right) = 3$ and $\dim\left(I_\beta\right) = 6$. Furthermore, if $v \in I_\beta$ with $wt(v) = 3$ then $\mathrm{supp}(v) \subset D_{10}'$ or $\mathrm{supp}(v) \subset sD_{10}'$.

(iii) If $\beta = \{e_i, e_j\}$ for $i = 1,2$ and $j = 3,4$, then $d\left(I_\beta\right) = 4$ and $\dim\left(I_\beta\right) = 5$. Furthermore, if $v \in I_\beta$ with $wt(v) = 4$ then $\mathrm{supp}(v) \subset D_{10}'$ or $\mathrm{supp}(v) \subset sD_{10}'$.

(iv) If $\beta = \mu_N$, then $d\left(I_\beta\right) = 10$ and $\dim\left(I_\beta\right) = 8$. Furthermore, if $v \in I_\beta$ with $wt(v) = 10$ then $\mathrm{supp}(v) = D_{10}' \cup sD_{10}'$.

(v) If $\beta = \{e_1, e_2, e_j\}$ for $j = 3,4$, then $d\left(I_\beta\right) = 4$ and $\dim\left(I_\beta\right) = 4$. Furthermore, if $v \in I_\beta$ with $wt(v) = 4$ then $\mathrm{supp}(v) \subset D_{10}'$ or $\mathrm{supp}(v) \subset sD_{10}'$.

(vi) If $\beta = \{e_i, e_3, e_4\}$ for $i = 1,2$, then $d\left(I_\beta\right) = 10$ and $\dim\left(I_\beta\right) = 1$. Furthermore, if $v \in I_\beta$ with $wt(v) = 10$ then $\mathrm{supp}(v) = D_{10}' \cup sD_{10}'$.

3.4 Codes defined over FD_{12}

D_{12} consists of six irreducible characters, four are linear characters and two are nonlinear characters. Each of this character will correspond to a distinct idempotent in the following way.

(a) Idempotents correspond to linear characters:

$$\chi_1 \leftrightarrow e_1 = \frac{1}{12}\left(\sum_{i=0}^{5} r^i (1+s)\right), \chi_2 \leftrightarrow e_2 = \frac{1}{12}\left(\sum_{i=0}^{5} r^i (1-s)\right),$$

$$\chi_3 \leftrightarrow e_3 = \frac{1}{12}\left(\sum_{i=0}^{5} (-r)^i (1+s)\right) \text{ and } \chi_4 \leftrightarrow e_4 = \frac{1}{12}\left(\sum_{i=0}^{5} (-r)^i (1-s)\right)$$

(b) Idempotents correspond to nonlinear characters:

$$\chi_5 \leftrightarrow e_5 = \frac{1}{6}\left(2-r-r^2\right)(1+r^3) \text{ and } \chi_6 \leftrightarrow e_6 = \frac{1}{6}(2-r-r^2)(1-r^3)$$

Let $u = \sum_{i=1}^{6} \lambda_i r^{i-1} + \sum_{j=7}^{12} \lambda_j r^{j-7} s$ be any elements in FD_{12} such that $\lambda_i \in F \forall 1 \leq i \leq 12$, then

$$ue_1 = \left(\sum_{i=1}^{12} \lambda_i\right) e_1 \tag{9}$$

$$ue_2 = \left(\sum_{i=1}^{6} \lambda_i + \sum_{j=7}^{12}\left(-\lambda_j\right)\right) e_2 \tag{10}$$

$$ue_3 = \left(\sum_{i=1,3,5,7,9,11} \lambda_i + \sum_{j=2,4,6,8,10,12}\left(-\lambda_j\right)\right) e_3 \tag{11}$$

$$ue_4 = \left(\sum_{i=1,3,5,8,10,12} \lambda_i + \sum_{j=2,4,6,7,9,11}\left(-\lambda_j\right)\right) e_4 \tag{12}$$

$$\begin{aligned} ue_5 = \frac{1}{6}\Big[&\left(2\lambda_1 - \lambda_2 - \lambda_3 + 2\lambda_4 - \lambda_5 - \lambda_6\right) + \left(2\lambda_1 - \lambda_2 - \lambda_3 + 2\lambda_4 - \lambda_5 - \lambda_6\right) r^3 \\ &+ \left(-\lambda_1 + 2\lambda_2 - \lambda_3 - \lambda_4 + 2\lambda_5 - \lambda_6\right) r + \left(-\lambda_1 = 2\lambda_2 - \lambda_3 - \lambda_4 + 2\lambda_5 - \lambda_6\right) r^4 \\ &+ \left(-\lambda_1 - \lambda_2 + 2\lambda_3 - \lambda_4 - \lambda_5 + 2\lambda_6\right) r^2 + \left(-\lambda_1 - \lambda_2 + 2\lambda_3 - \lambda_4 - \lambda_5 + 2\lambda_6\right) r^5 \\ &+ \left(2\lambda_7 - \lambda_8 - \lambda_9 + 2\lambda_{10} - \lambda_{11} - \lambda_{12}\right) s + \left(2\lambda_7 - \lambda_8 - \lambda_9 + 2\lambda_{10} - \lambda_{11} - \lambda_{12}\right) r^3 s \\ &+ \left(-\lambda_7 - \lambda_8 + 2\lambda_9 - \lambda_{10} - \lambda_{11} + 2\lambda_{12}\right) r^2 s + \left(-\lambda_7 - \lambda_8 + 2\lambda_9 - \lambda_{10} - \lambda_{11} + 2\lambda_{12}\right) r^5 s\Big] \end{aligned} \tag{13}$$

$$\begin{aligned} ue_6 = \frac{1}{6}\Big[&\left(2\lambda_1 + \lambda_2 - \lambda_3 - 2\lambda_4 - \lambda_5 + \lambda_6\right) - \left(2\lambda_1 + \lambda_2 - \lambda_3 - 2\lambda_4 - \lambda_5 + \lambda_6\right) r^3 \\ &+ \left(\lambda_1 + 2\lambda_2 + \lambda_3 - \lambda_4 - 2\lambda_5 - \lambda_6\right) r - \left(\lambda_1 + 2\lambda_2 + \lambda_3 - \lambda_4 - 2\lambda_5 - \lambda_6\right) r^4 \\ &+ \left(-\lambda_1 + \lambda_2 + 2\lambda_3 + \lambda_4 - \lambda_5 - 2\lambda_6\right) r^2 - \left(-\lambda_1 + \lambda_2 + 2\lambda_3 + \lambda_4 - \lambda_5 - 2\lambda_6\right) r^5 \\ &+ \left(2\lambda_7 + \lambda_8 - \lambda_9 - 2\lambda_{10} - \lambda_{11} + \lambda_{12}\right) s - \left(2\lambda_7 + \lambda_8 - \lambda_9 - 2\lambda_{10} - \lambda_{11} + \lambda_{12}\right) r^3 s \\ &+ \left(\lambda_7 + 2\lambda_8 + \lambda_9 - \lambda_{10} - 2\lambda_{11} - \lambda_{12}\right) rs - \left(\lambda_7 + 2\lambda_8 + \lambda_9 - \lambda_{10} - 2\lambda_{11} - \lambda_{12}\right) r^4 s \\ &+ \left(-\lambda_7 + \lambda_8 + 2\lambda_9 + \lambda_{10} - \lambda_{11} - 2\lambda_{12}\right) r^2 s - \left(-\lambda_7 + \lambda_8 + 2\lambda_9 + \lambda_{10} - \lambda_{11} - 2\lambda_{12}\right) r^5 s\Big] \end{aligned} \tag{14}$$

Theorem 3.9. Let $\mu_L = \{e_1, e_2, e_3, e_4\}$ and $\mu_N = \{e_5, e_6\}$ be all idempotents in FD_{12} which is defined as above.

(i) If $\beta \subseteq \mu_L$, then $d(I_\beta) = 2$ and $\dim(I_\beta) = 12 - |\beta|$.

(ii) If $\beta \subseteq \mu_N$ and $|\beta| = 1$, then $d(I_\beta) = 2$ and $\dim(I_\beta) = 8$.

(iii) If $\beta = \{e_i, e_5\}$, then $d(I_{\{e_i,e_5\}}) = 2$ *only if* $i = 1$ *or* 2, and $d(I_{\{e_i,e_5\}}) = 4$ *only if* i = 3 *or* 4. Furthermore, $\dim(I_\beta) = 7$.

(iv) If $\beta = \{e_i, e_6\}$, then $d(I_{\{e_i,e_6\}}) = 4$ *only if* i = 1 *or* 2, and $d(I_{\{e_i,e_6\}}) = 2$*)* *only if* i = 3 *or* 4. Furthermore, $\dim(I_\beta) = 7$.

(v) $d(I_{\mu_N}) = 3$ and $\dim(I_\beta) = 4$.

(vi) $d(I_{\{e_1,e_2,e_5\}}) = d(I_{\{e_3,e_4,e_6\}}) = 2$ and $\dim(I_\beta) = 6$.

(vii) $d(I_{\{e_3,e_4,e_5\}}) = d(I_{\{e_1,e_2,e_6\}}) = 4$ and $\dim(I_\beta) = 6$.

(viii) $d(I_{\{e_1,e_3,e_5\}}) = d(I_{\{e_1,e_4,e_5\}}) = d(I_{\{e_2,e_3,e_5\}}) = d(I_{\{e_2,e_4,e_5\}}) = 6$ and $\dim(I_\beta) = 6$.

(ix) $d(I_{\{e_i,e_5,e_6\}}) = 6$ *for* $i = 1,2,3,4,$ and $\dim(I_\beta) = 3$.

(x) $d(I_{\{e_i,e_j,e_k,e_5\}}) = 6$, *where* $i, j, k = 1,2,3,4, i \neq j \neq k$, and $\dim(I_\beta) = 7$.

(xi) $d(I_{\{e_1,e_2\}\cup\mu_N}) = d(I_{\{e_3,e_4\}\cup\mu_N}) = 6$ and $\dim(I_\beta) = 2$.

(xii) $d(I_{\{e_1,e_3\}\cup\mu_N}) = d(I_{\{e_2,e_4\}\cup\mu_N}) = 12$ and $\dim(I_\beta) = 2$.

(xiii) If $\beta \subseteq \mu_N$ and $|\beta| = 1$, then $d(I_{\mu_L\cup\beta}) = 6$ and $\dim(I_\beta) = 4$.

REFERENCES

Berman, S. D. 1967. Semisimple Cyclic and Abelian Codes, II. *Kibernetika.* **3**: 21-30.

Berman, S. D. 1989. Parameter of Abelian Codes in the Group Algebra *KG* of $G = \langle a \rangle \times \langle b \rangle$, $a^p = b^p = 1$, p is prime, over a finite field K with a primitive p^{th} root of unity and related MDS-Codes. *Contempary Math.* **93**.

How Guan Aun and Denis Wong Chee Keong. 2004. Group Codes Defined Using Extra-Special p-Group of Order p^3. *Bull. Malays. Math. Sci. Soc*. **2**: 27: 185-205.

Hurley, P. and Hurley, T. 2007. Module codes in group rings. *Proc. IEEE Int. Symp. on Information Theory (ISIT).*

Hurley, P. and Hurley, T. 2007. Codes from Zero-divisors and units in group rings. *Int. J. Inform, and Coding Theory*. **1**: 57 – 87.

Isaacs, I. M. 1992. *Algebra, A Graduate Course*. California: Brooks/Cole Publishing. Pacific Grove.

James, G. D. and Liebeck, M. W. 1993. *Representations and Characters of groups*. Cambridge University Press.

Macwilliam, F. J. 1969. Codes and ideals in group algebras, in *Combinatorial Mathematics and its Applications*, R.C. Bose and T.A. Dowling, eds., Chapel Hill*:* Univ. North Carolina Press, 317-328.

Passman, D. S. 1977. *The Algebraic Structure of Group Rings*. New York: Wiley.

Sloane, N. J. A. and Macwilliam, F. J. 1978. *The Theory of Error Correcting Codes*. Amsterdam, Netherlands: North-Holland.