JP Journal of Algebra, Number Theory and Applications
© 2013 Pushpa Publishing House, Allahabad, India
Published Online: November 2013
Available online at http://pphmj.com/journals/jpanta.htm
Volume 30, Number 1, 2013, Pages 47-60

GROUP ALGEBRA CODES DEFINED OVER EXTRA SPECIAL *p*-GROUP OF ORDER p^{2r+1}

Denis C. K. Wong and Ang Miin Huey

Department of Applied Mathematics and Actuarial Science
Faculty of Engineering and Science
Universiti Tunku Abdul Rahman
UTAR Setapak, Off Jalan Genting Kelang
53300 Kuala Lumpur, Malaysia
e-mail: deniswong@utar.edu.my

School of Mathematical Sciences
Universiti Sains Malaysia
11800, Pulau Pinang, Malaysia
e-mail: mathamh@cs.usm.my

Abstract

Idempotents in the group algebra defined over an extra special *p*-group of order p^{2r+1} provide useful information to determine the minimum distance for this family of group algebra code. Our primary task is to identify all such idempotents and thus construct a family of MDS group algebra code by choosing a suitable set consisting of certain idempotents in order to maximize the minimum distance.

1. Introduction

Coding theory is important in modern digital communication; however,

---

Received: December 28, 2012; Accepted: March 12, 2013
2010 Mathematics Subject Classification: 05E20.
Keywords and phrases: group algebra, code, idempotent, extra special, minimum distance.
The work is partially supported by FRGS Grant 203/PMATHS/6711176 and UTARRF.

noises might occur during the transmission of digital data across a communication channel. This may cause the received data to differ from the transmitted data. Therefore, error correcting and detecting codes are used in modern digital communication system. The study of group codes as an ideal in a group algebra FG has been developed long time ago, refer [5] and [6].

Let $\mathcal{F}_q$ denote a finite field with q elements such that q is a prime. Given a finite group G of order n, the group algebra $\mathcal{F}_qG$ is a vector space over $\mathcal{F}_q$, with basis G and so, is isomorphic to $\mathcal{F}_q^n$ as a vector space. A group algebra code is defined as an ideal of the group algebra $\mathcal{F}_qG$. In particular, if G is a cyclic group, then the ideal in $\mathcal{F}_qG$ is a cyclic code, and if G is an abelian group, then the ideal in $\mathcal{F}_qG$ is an abelian code.

It is well known that if $q \nmid n$, then Maschke's Theorem (Theorem 1.9 in [2]) stated that the group algebra $\mathcal{F}_qG$ is semisimple and hence $\mathcal{F}_qG$ is a direct sum of minimal ideals, $\mathcal{F}_qG = I_1 \oplus I_2 \oplus \cdots \oplus I_s$, where $I_j = \mathcal{F}_qGe_j$ is the principal ideal of $\mathcal{F}_qG$ generated by e_j, where e_j is an idempotent in $\mathcal{F}_qG$ for $j = 1, 2, ..., s$. Let $M = \{e_j\}_{j=1}^{s}$ be the set of all pairwise orthogonal idempotents.

Every ideal I of $\mathcal{F}_qG$ is a direct sum $I = I_{i_1} \oplus I_{i_2} \oplus \cdots \oplus I_{i_t}$, where $t \le s$. Now, write $\mathcal{F}_qG = I \oplus J$, where $J = I_{j_1} \oplus I_{j_2} \oplus \cdots \oplus I_{j_{s-t}}$ is the direct sum of minimal ideals such that $I_{i_l} \neq I_{j_m}$ for all $1 \le l \le t$ and $1 \le m \le s - t$.

Lemma 1.1. *Let* $\mu = \{e_{j_1}, e_{j_2}, ..., e_{j_{s-t}}\}$. *Then* $I = I_\mu$, *where* $I_\mu = \{u \in \mathcal{F}_qG \mid ue_{j_m} = 0, \forall e_{j_m} \in \mu\}$.

Proof. If $u \in I$, then $u = \sum_{e_i \in M \setminus \mu} a_i e_i$, $a_i \in \mathcal{F}_qG$. For all $e_j \in \mu$, $ue_j = \sum_{e_i \in M \setminus \mu} a_i(e_i e_j) = 0$. Thus, $u \in I_\mu$, and so $I \subseteq I_\mu$.

Conversely, for any $u \in \mathcal{F}_q G$, $u = \sum_{e_i \in M} a_i e_i$. If $u \in I_\mu$, then $ue_j = 0$ for all $e_j \in \mu$. Thus, $\left(\sum_{e_i \in M} a_i e_i\right) e_j = 0$ for all $e_j \in \mu$ if and only if $a_j e_j = 0$ for all $e_j \in \mu$ if and only if $a_j = 0$ for all *j*. Therefore, $u = \sum_{e_i \in M \setminus \mu} a_i e_i \in I$, and so $I_\mu \subseteq I$. □

Since I_μ is an ideal of $\mathcal{F}_q G$, I_μ is a subspace of $\mathcal{F}_q G$ which implies that I_μ is a linear code over $\mathcal{F}_q$. It is well known that a linear code can be defined by using a parity check matrix. In this paper, the usage of idempotents in $\mathcal{F}_q G$ as parity checks is equivalent to the definition of a linear code by its parity check matrix. As a parity check matrix of a linear code can tell us the minimum distance of the code, thus the set of idempotents μ should also provide some information to determine the minimum distance of I_μ.

In [1], we study the group algebra codes defined over extra special *p*-group of order p^3 by constructing two families of group algebra codes generated by linear idempotents and nonlinear idempotents separately. In this paper, we generalized our study to any extra special *p*-group of order p^{2r+1}.

We now give some basic definitions. Let I_μ as defined in Lemma 1.1. The element in I_μ is called a *codeword* and $N = dim(\mathcal{F}_q G) =$ length of codeword in I_μ. Furthermore, define the weight of *u* as $wt(u) = |\{a_g \mid a_g \neq 0\}|$ and the minimum distance of I_μ,

$$d(I_\mu) = min\{wt(u) \mid 0 \neq u \in I_\mu\}.$$

Therefore, I_μ with parameters N, $K = dim(I_\mu)$ and $d = d(I_\mu)$ is called an $[N, K, d]$-*group algebra code*. In this paper, our main task is to determine the parameters *N*, *K* and *d* for I_μ. The length and dimension of a code can be derived directly from the construction. However, to determine the minimum distance of a code, it may be a difficult task. The following lemma is needed later.

Lemma 1.2. *Let* μ_1, μ_2 *be the sets consisting of idempotents in* $\mathcal{F}_q G$ *such that* $\mu_1 \subseteq \mu_2$. *Then* $d(I_{\mu_2}) \geq d(I_{\mu_1})$.

Proof. For all $u \in I_{\mu_2}$, $ue = 0$ for all $e \in \mu_2$ and so $ue = 0$ for all $e \in \mu_1$. Thus, $u \in I_{\mu_1}$. Therefore, $I_{\mu_2} \subseteq I_{\mu_1}$. Next, let $u \in I_{\mu_1}$ with minimum weight, that is, $ue = 0$ for all $e \in \mu_1$. If $ue \neq 0$ for all $e \in \mu_2 \backslash \mu_1$, then $u \notin I_{\mu_2}$, so $d(I_{\mu_2}) > d(I_{\mu_1})$. On the other hand, if $ue = 0$ for all $e \in \mu_2 \backslash \mu_1$, then $u \in I_{\mu_2}$ and so the inequality holds. $\square$

2. Extra Special *p*-group and Characters

In this section, we will follow those notations used in [1] and [2]. Let p be a prime (distinct from q). A p-group G is called *extra special* if $G' = Z(G)$, $|G'| = p$ and G/G' is elementary abelian. From Theorem 2.17 in [4], there is an integer $r \geq 1$ such that $|G| = p^{2r+1}$ and G has normal subgroups $N_1, N_2, \ldots, N_r$ such that

(a) N_i is a nonabelian group of order p^3 for all i, $1 \leq i \leq r$.

(b) $G = N_1 N_2 \ldots N_r$.

(c) $[N_i, N_j] = 1$ for all $i \neq j$.

(d) $N_i \cap N_1 \ldots N_{i-1} N_{i+1} \ldots N_r = Z(G)$ for all i.

Lemma 2.1. *Let* G *be the extra special* p*-group of order* p^{2r+1}. *Then each* N_i *is also an extra special* p*-group of order* p^3 *for* $i = 1, 2, \ldots, r$.

Proof. Since each N_i is a p-group, $Z(N_i) > 1$. Thus, $|N_i/Z(N_i)| \leq p^2$. As N_i is nonabelian, then $N_i/Z(N_i)$ is not cyclic and so $|N_i/Z(N_i)| = p^2$

which then implies $|Z(N_i)| = p$ and $N_i/Z(N_i) \cong Z_p \times Z_p$. Finally, as $N_i' \subseteq Z(N_i)$, then $Z(N_i) = N_i'$. □

Since $|G'| = |Z(G)| = p$, we may write $G' = \langle g \mid g^p = 1\rangle$. As $|G| = p^{2r+1}$, then $|G/G'| = p^{2r}$. Let $T = \{t_0 = 1, t_1, t_2, ..., t_{p^{2r}-1}\}$ be the set of all right transversal of G' in G. Then, the p^{2r} right cosets of G' in G are $G't_i = \{t_i, gt_i, g^2t_i, ..., g^{p-1}t_i\}$ for $i = 0, 1, 2, ..., p^{2r} - 1$ and so $G = \bigcup_{i=0}^{p^{2r}-1} G't_i$.

Proposition 2.1. *Let G be an extra special p-group of order* p^{2r+1}. *Then the following hold*:

(a) *G has* $p^{2r} + p - 1$ *conjugacy classes*; *p of these has size* 1 *and the other* $p^{2r} - 1$ *conjugacy classes has size p, which is exactly the right cosets* xG', $x \in G \setminus G'$.

(b) *The number of linear characters of G is* $|G/G'| = p^{2r}$.

(c) *The total number of irreducible characters of G is equal to the number of conjugacy classes of G, that is,* $|Irr(G)| = p^{2r} + p - 1$.

(d) *The total number of non-principal characters of G is equal to* $|Irr(G)| - |G/G'| = p - 1$.

Proof. Part (a) is a general result obtained from Section 2 in [1]. Part (b) follows from Corollary 2.23 in [2]. Part (c) follows from Corollary 2.7 in [2] together with part (a). Finally, part (d) is just a direct consequence from (b) and (c). □

Proposition 2.2. *Let G be an extra special p-group of order* p^{2r+1}. *If* χ *is a linear character of G, then the following hold*:

(a) *For all* $g \in G$, $\chi(g) \neq 0$.

(b) *For all* $g \in G'$, $\chi(g) = 1$. *In particular*, $\chi(1) = 1$, *that is*, $deg(\chi) = 1$.

(c) *For any* $x, y \in gG'$, $\chi(x) = \chi(y)$.

Proof. Part (a) directly follows from the fact that χ is a homomorphism. For part (b), consider any $g \in G'$, $\chi(g) = \chi([x, y]) = \chi(x^{-1}y^{-1}xy) = 1$ for some $x, y \in G$. Finally, part (c) follows directly from (b). □

Proposition 2.3. *Let G be an extra special p-group of order* p^{2r+1}. *If* χ *is a nonlinear character of G, then the following hold*:

(a) $\chi(1) = p^r$.

(b) *For all* $g \in G'$, $\chi(g) \neq 0$.

(c) *For all* $g \notin G'$, $\chi(g) = 0$.

(d) *Fix a generator*, *g*, *of* G', *and let* ζ *be a primitive pth root of unity in F. Then* $\chi_i(g) = p^r\zeta^i$ *for some* $i \in \{1, 2, ..., p-1\}$.

Proof. To prove part (a), from Corollary 3.11 in [3], as χ is nonlinear, then $G' \not\subseteq ker(\chi)$ and so $G' \cap ker(\chi) = \{1\}$. As $|G'| = p$, then $ker(\chi) = 1$ and together with part (e) of Lemma 2.27 in [2], we see that $Z(\chi) = Z(G)$. For all $z \in Z(G)$, $|\chi(z)| = \chi(1)$. Since χ is irreducible, from Corollary 2.17 in [2],

$$\begin{aligned}1 &= [\chi, \chi]\\ &= \frac{1}{|G|}\sum_{z \in Z(G)} \chi(z)\overline{\chi(z)}\\ &= \frac{1}{p^{2r+1}}\sum_{z \in Z(G)} |\chi(z)|^2\end{aligned}$$

$$= \frac{1}{p^{2r+1}} | Z(G) | \chi(1)^2$$

which implies $\chi(1) = p^r$.

For part (b), as $G' = Z(G) = Z(\chi)$, then part (c) of Lemma 2.27 in [2] implies $\chi_{G'} = \chi(1)\lambda$, where λ is some linear character of G'. Therefore,

$$\chi_{G'}(g) = \chi(1)\lambda(g) \neq 0, \quad \forall g \in G'.$$

Next, since G has p^{2r} linear characters, which are, $\chi_1, \chi_2, \ldots, \chi_{p^{2r}}$, and let $\beta_1, \beta_2, \ldots, \beta_{p-1}$ be those nonlinear characters of G. Thus, for all $g \in G'$,

$$\begin{aligned} p^{2r} &= | C_G(g) | \\ &= \sum_{i=1}^{p^{2r}} | \chi(g) |^2 + \sum_{i=1}^{p-1} | \beta_i(g) |^2 \\ &= p^{2r} + \sum_{i=1}^{p-1} | \beta_i(g) |^2 \end{aligned}$$

implies $\sum_{i=1}^{p-1} | \beta_i(g) |^2 = 0$ and so $\beta_i(g) = 0$ for all $g \in G'$ and $i = 1, 2, \ldots, p-1$.

To prove part (d), note that from (b), $\chi_{G'} = \chi(1)\lambda$. For all $g \in G'$, $\chi_{G'} = p^r\lambda(g)$. Furthermore, $\chi_{G'}(g) = \chi(g)$ for $\chi \in G^*$ and for all $g \in G'$. Since $g^p = 1$, $\chi(g^p) = \chi(1) = p^r$, and so $p^r\lambda(g^p) = \chi(g^p) = p^r$ implies $\lambda(g)^p = 1$ and so $\lambda(g) = \zeta$, where ζ is a primitive *p*th root of unity and so (d) will follow directly. □

3. Idempotents

Since $d(I_\mu)$ depends on those idempotents in μ. We start by deriving a formula for all idempotents in $\mathcal{F}_q G,$ where G is the extra special p-group of order p^{2r+1}. From Theorem 2.12 in [2], any idempotent e_i in $\mathcal{F}_q G$ can be written uniquely as

$$e_i = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1}) g.$$

As $G = \bigcup_{i=0}^{p^{2r}-1} G' t_0$ and $G' = \langle g \mid g^p = 1 \rangle,$ then

$$e_i = \frac{\chi_i(1)}{p^{2r+1}} \sum_{j=0}^{p^{2r}-1} \sum_{i=0}^{p-1} \chi_i(g^{-i} t_j^{-1}) t_j g^i.$$

If χ_i is the principal character of G, that is, $\chi_i(g) = 1$ for all $g \in G,$ then χ_i will define e_i the principal idempotent which is usually denoted by $e_{principal}$ and

$$e_{principal} = \frac{1}{p^{2r+1}} \sum_{j=0}^{p^{2r}-1} \sum_{i=0}^{p-1} t_j g^i$$

$$= \frac{G}{|G|}.$$

Note that for all $g \in G,$ $e_{principal}\, g = \frac{G}{|G|} g = \frac{G}{|G|} = e_{principal}.$

Next, let M_L be the set consisting of all linear idempotents of $\mathcal{F}_q G,$ that is, all these idempotents correspond to the p^{2r} linear characters. Thus, $|M_L| = p^{2r}$. We know that from Proposition 2.2 for all $\chi_i \in G^*$ which is linear, we have $\chi_i(g) = 1$ for all $g \in G'$. Therefore,

$$e_i = \frac{1}{p^{2r+1}}\left(\sum_{i=0}^{p-1} g^i\right)\left(\sum_{j=0}^{p^{2r}-1} \chi_i(t_j^{-1})t_j\right)$$

$$= \frac{G'}{p^{2r+1}}\left(\sum_{j=0}^{p^{2r}-1} \chi_i(t_j^{-1})t_j\right).$$

It can be shown that for all $e \in M_L$, $ge = e$ for all $g \in G'$.

Finally, let M_N be the set consisting of all nonlinear idempotents of $\mathcal{F}_q G$, that is, all those idempotents corresponded to the nonlinear characters of G. Note that $|M_N| = p - 1$. For all $e_i \in M_N$, since

$$G = G't_0 \bigcup \left(\bigcup_{i=1}^{p^{2r}-1} G't_i\right)$$

and from Proposition 2.3, we have $\chi(G) = \chi(G') + \sum_{i=0}^{p^{2r}-1}\chi(G't_i) = \chi(G')$. Thus,

$$e_i = \frac{1}{p^{r+1}}\left[\sum_{g \in G'} \chi_i(g^{-1})g + \sum_{g \in G \setminus G'} \chi_i(g^{-1})g\right]$$

$$= \frac{1}{p^{r+1}} \sum_{g \in G'} \chi_i(g^{-1})g$$

$$= \frac{1}{p^{r+1}} \sum_{j=0}^{p-1} p^r \zeta^{-ij} g^j$$

$$= \frac{1}{p} \sum_{j=0}^{p-1} \zeta^{-ij} g^j.$$

Clearly, for all $g \in G'$, $ge_i = e_i'$, where $e_i, e_i' \in M_N$. We collect all facts above in the following proposition.

Proposition 3.1. *Let G be an extra special p-group of order* p^{2r+1}.

(a) *The principal idempotent of* $\mathcal{F}_q G$ *is* $e_{principal} = \frac{G}{|G|}$.

(b)

$$M_L \setminus \{e_{principal}\} = \left\{ e_i = \frac{G'}{p^{2r+1}} \left(\sum_{j=0}^{p^{2r}-1} \chi_i(t_j^{-1}) t_j \right) \middle| i = 1, 2, \ldots, p^{2r} - 1 \right\}.$$

(c) $M_N = \left\{ e_i = \frac{1}{p} \sum_{j=0}^{p-1} \zeta^{-ij} g^j \,|\, i = 1, 2, \ldots, p-1 \right\}$.

4. Dimension

In this section, we will determine the dimension for I_μ. We start by deriving two simple results.

Lemma 4.1. *For all* $e \in M_L$, $dim(\mathcal{F}_q Ge) = 1$.

Proof. For all $h \in G$,

$$\begin{aligned} he &= \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}h^{-1}) \chi(h) hg \\ &= \frac{\chi(h)}{|G|} \sum_{g \in G} \chi((hg)^{-1}) hg \\ &= \chi(h) e. \end{aligned}$$

Next, for all $u = \sum_{h \in G} a_h h \in \mathcal{F}_q G$,

$$\begin{aligned} ue &= \sum_{h \in G} a_h (he) \\ &= \sum_{h \in G} a_h (\chi(h) e) \\ &= \left(\sum_{h \in G} a_h \chi(h) \right) e \in \langle e \rangle. \end{aligned}$$

Therefore, for all $u \in \mathcal{F}_q G$, $\mathcal{F}_q Ge = \langle e \rangle$ and so $dim(\mathcal{F}_q Ge) = 1$ for all $e \in M_L$. □

Corollary 4.1. $dim(I_{M_N}) = p^{2r}$.

Proof. From Lemma 1.1, we know that

$$I_{M_N} = \oplus_{e_i \in M \setminus M_N} FGe_i = \oplus_{e_i \in M_L} FGe_i.$$

Thus, $dim(I_{M_N}) = \sum_{e_i \in M_L} dim(FGe_i)$ and so the result will follow from Lemma 4.1. □

Lemma 4.2. *For all* $e \in M_N$, $dim(\mathcal{F}_q Ge) = p^{2r}$.

Proof. Since each $e \in M_N$ corresponds to χ such that $deg(\chi) = p^r$ and $\mathcal{F}_q Ge \cong M_{n_j}(F)$ (refer [2]) and so $dim(\mathcal{F}_q Ge_j) = n_j^2$, where $n_j = p^r = deg(\chi)$. Thus, $dim(\mathcal{F}_q Ge) = p^{2r}$. □

Corollary 4.2. $dim(I_{M_L}) = p^{2r}(p-1)$.

Proof. Follows from Lemma 1.1 and Lemma 4.2. □

Our main result on dimension of I_μ.

Theorem 4.1. *Let* $\mu = \mu_L \cup \mu_N$, *where* $\mu_L \subseteq M_L$ *and* $\mu_N \subseteq M_N$. *Then* $dim(I_\mu) = p^{2r+1} - |\mu_L| - |\mu_N| p^{2r}$.

Proof. By the property of semisimple, as $\mathcal{F}_q G = \oplus_i \mathcal{F}_q Ge_i$, then $|G| = dim(\mathcal{F}_q G) = \sum_i dim(FGe_i)$. Thus,

$$\begin{aligned} dim(I_\mu) &= dim(\bigoplus_{e_i \in M \setminus \mu} \mathcal{F}_q Ge_i) \\ &= (|M_L| - |\mu_L|) dim(\mathcal{F}_q Ge) + (|M_N| - |\mu_N|) dim(\mathcal{F}_q Gf) \end{aligned}$$

$$= (|M_L| - |\mu_L|) + (|M_N| - |\mu_N|)\, p^{2r}$$

$$= (p^{2r} - |\mu_L|) + (p - 1 - |\mu_N|)\, p^{2r}$$

$$= p^{2r+1} - |\mu_L| - |\mu_N|\, p^{2r},$$

where $e \in M_L$ and $f \in M_N$. □

5. Minimum Distance

Theorem 5.1. $d(I_{e_{principal}}) = 2.$

Proof. We first note that for all $u \in \mathcal{F}_q G,$ $u = \sum_{j=0}^{p^{2r}-1} \sum_{i=0}^{p-1} \lambda_{ji} g^i t_j.$ Then $ue_{principal} = \left(\sum_{j=0}^{p^{2r}-1} \sum_{i=0}^{p-1} \lambda_{ji} \right) e_{principal}.$ For all $u \in \mathcal{F}_q G$ with $wt(u) = 1,$ that is, $u = \lambda g$ for some $g \in G$ and $\lambda \neq 0.$ Then $ue_{principal} = \lambda e_{principal} \neq 0$ and so $u \notin I_{e_{principal}},$ that is, $d(I_{e_{principal}}) \geq 2.$ Next, for some $g, h \in G$ such that $g \neq h,$ clearly, $u = \lambda g + (-\lambda) h \in I_{e_{principal}}$ as $ue_{principal} = (\lambda - \lambda) e_{principal} = 0.$ Therefore, $d(I_{e_{principal}}) = 2.$ □

From Theorem 4.1 and Theorem 5.1, we see that $I_{e_{principal}}$ is a $[p^{2r+1},\ p^{2r+1} - 1,\ 2]$-group algebra code which is an MDS code. Recall from Section 2, any extra special *p*-group *G* of order p^{2r+1} has the form $G = N_1 N_2 \ldots N_r,$ where N_i is a normal subgroup of *G*.

Lemma 5.1. *Let e be an idempotent in* $\mathcal{F}_q N_i.$ *Then* $e \in \mathcal{F}_q G.$

Proof. Let $f = e_{principal}$ be the principal idempotent of $\mathcal{F}_q G$ and let $\chi \in N_i^*$ be the character defined *e*. Then

$$ef = \left(\frac{\chi(1)}{|N_i|}\sum_{g\in N_i}\chi(g^{-1})g\right)\frac{G}{|G|}$$

$$= \frac{\chi(1)}{|G||N_i|}G\sum_{g\in N_i}\chi(g^{-1}).$$

If e is the principal idempotent of $\mathcal{F}_q N_i$, then $ef = \frac{1}{|G||N_i|}G|N_i| = f \in \mathcal{F}_q G$ and so $e \in \mathcal{F}_q G$. If e is a linear idempotent of $\mathcal{F}_q N_i$, then $ef = \frac{1}{|G||N_i|}G\chi(N_i) = \frac{1}{|G||N_i|}G|N_i| = f \in \mathcal{F}_q G$ and so $e \in \mathcal{F}_q G$. Finally, if e is a nonlinear idempotent of $\mathcal{F}_q N_i$, then

$$ef = \frac{\chi(1)}{|G||N_i|}G\sum\nolimits_{g\in N_i}\chi(g^{-1}) \in FG$$

and so $e\mathcal{F}_q G \subseteq \mathcal{F}_q G$ implies $e \in \mathcal{F}_q G$. □

Theorem 5.2. *Let* $\mu \subseteq M$.

(a) *If* $\mu = \mu_L$, *then* I_μ *is a* $[p^{2r+1}, p^{2r+1} - |\mu_L|, 2]$*-group algebra code.*

(b) *If* $\mu = \mu_N$ *and q is a primitive root modulo p, then* I_μ *is a* $[p^{2r+1}, p^{2r+1} - |\mu_N|p^{2r}, |\rho_N| + 1]$*-group algebra code, where* ρ_N *is the set of all nonlinear idempotents in* N_i.

Proof. The dimension of I_μ follows directly from Theorem 4.1. Let ρ_L be all linear idempotents in $\mathcal{F}_q N_i$. From Lemma 5.1, since $\rho_L \subseteq \mu_L$, by Lemma 1.1, $d(I_{\mu_L}) \geq d(I_{\rho_L})$ and also $d(I_{\rho_L}) = 2$ follows from Theorem 4 in [1]. Finally, since $\mu_L \subset \mu$, by Lemma 1.1 against, $d(I_\mu) \geq d(I_{\mu_L}) \geq 2$.

Next, let ρ_N be the set of all nonlinear idempotents in $\mathcal{F}_q N_i$. From Theorem 13 in [1], since we assume q is a primitive root modulo p,

$d(I_{\rho_N}) = |\rho_N| + 1.$ From Lemma 5.1, since $\rho_N \subseteq \mu_N$, by Lemma 1.1, $d(I_{\mu_N}) \geq d(I_{\rho_N}) = |\rho_N| + 1.$ Also, since $\mu_N \subset \mu$, by Lemma 1.1, $d(I_\mu) \geq d(I_{\mu_N}) \geq |\rho_N| + 1.$ □

References

[1] G. A. How and Denis C. K. Wong, Group codes defined using extra special *p*-group of order p^3, Bull. Malays. Math. Sci. Soc. (2) 27 (2004), 185-205.

[2] I. M. Isaacs, Character Theory of Finite Groups, AMS Chelsea Publishing, Providence, RI, 2006.

[3] I. M. Isaacs, Algebra, A Graduate Course, Brooks/Cole Publishing, Pacific Grove, California, 1992.

[4] G. Karpilovsky, Group representations, Vol. 1. Part B: Introduction to Group Representations and Characters, Elsevier Science Publishers B.V., 1992.

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

[6] S. D. Berman and I. I. Grushko, Parameters of abelian codes in the group algebra *KG* of $G = \langle a \rangle \times \langle b \rangle$, $a^p = b^p = 1$, *p* prime, over a finite field *K* with primitive *p*th root of unity and related MDS-codes, Representation theory, group rings, and coding theory, 77-83, Contemp. Math., 93, Amer. Math. Soc., Providence, RI, 1989.