BULLETIN of the MALAYSIAN MATHEMATICAL SCIENCES SOCIETY

Bull. Malays. Math. Sci. Soc. (2) **27** (2004), 185–205

Group Codes Defined Using Extra-Special *p*-Group of Order p^3

[1]HOW GUAN AUN AND [2]DENIS WONG CHEE KEONG
School of Mathematical Sciences, Universiti Sains Malaysia, 11800 USM Pulau Pinang, Malaysia
e-mail: [1]gahow@cs.usm.my and [2]deniswck@hotmail.com

Abstract. The study of group code as an ideal in a group algebra has been developed long time ago. If $\mathrm{char}(F) \nmid |G|$, then FG is semisimple, and therefore, decomposes into a direct sum $FG = \underset{i}{\oplus} FGe_i$ where FGe_i are minimal ideals generated by the idempotent e_i. The idempotent e_i provides useful information about the minimum distance of group codes. In this paper, we consider group code generated by extra-special *p*-group of order p^3, and construct two families of group codes, one defined using linear idempotents, and the other defined using nonlinear idempotents. Our primary task is to determine the parameters of these two families of group codes.

2000 Mathematics Subject Classification: 94B60

1. Introduction

Throughout this paper, p is a prime number, G denotes a finite group, F denotes a finite field whose characteristic is a primitive root modulo p and $\mathrm{char}(F) \nmid |G|$. A group code is defined as an ideal I in a group algebra FG and we often say I is defined by G. If $\mathrm{char}(F) \nmid |G|$, then FG is semisimple and is a direct sum of some minimal ideals, say $FG = \overset{s}{\underset{j=1}{\oplus}} I_j$. Each I_j is generated by an idempotent e_j, i.e., $I_j = FGe_j$. Let $M = \{e_j\}_{j=1}^{s}$. Any ideal I of FG is a direct sum of some of the I_j, say $I = \overset{t}{\underset{k=1}{\oplus}} I_{j_k}$, $t \le s$. We say that I is generated by $\{e_{j_k}\}_{k=1}^{t}$. Let $\mu = M \setminus \{e_{j_k}\}_{k=1}^{t}$. Then $I = \{u \in FG \mid ue_{j_r}, = 0 \,\forall\, e_{j_r} \in \mu\}$. 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. Let us recall some notations 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 $\left|\{\lambda_g \mid \lambda_g \neq 0\}\right|$ and is denoted by $\mathrm{wt}(u)$. If I_μ has dimension K (as a vector space over F) and minimum distance $d(= \min\{\mathrm{wt}(u) \mid 0 \neq u \in I_\mu\})$, then I_μ is called an $[N, K, d]$ group code. In this paper, we consider group codes defined by extra-special p-group of order p^3, and construct two families of group codes. We determine dimension K of I_μ in Section 3 and its minimum distance in Section 4 and 5. Note that the basic theories in Section 2 and 3 can be found in [3, 5, 6].

2. Extra-special *p*-group of order p^3

In this paper, we follow the notation in [3, 5]. A finite p-group G is extra-special if $G' = Z(G)$, $|G'| = p$ and G/G' is elementary abelian. From now onward, G always denotes a p-group of order p^3, which is always extra-special. Let $G' = \langle g \rangle$ and $n = p^2 = |G/G'|$. We fixed a set of transversal T of G' in G, i.e., $T = \{t_0 = 1, t_1, t_2, \cdots, t_{n-1}\}$, and so $G = \bigcup_{i=0}^{n-1} G't_i$. We now state the following properties of extra-special p-group. For the proof we refer to $[3, 5]$.

P1. G has $p^2 + p - 1$ conjugacy classes; p of these has size 1 and the other $p^2 - 1$ each has size p.

P2. $|\mathrm{Irr}(G)| = p^2 + p - 1$.

P3. G has $p - 1$ nonlinear irreducible characters of degree p and p^2 linear characters.

P4. All nonlinear irreducible characters are faithful.

P5. Assume $\mathrm{char}(F) \neq p$, then $FG = \bigoplus_i FGe_i \cdot e_i$ can be computed using the formula

$$\frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1})g \quad \text{where} \quad \mathrm{Irr}(G) = \{\chi_i\}_{i=1}^{p^2+p-1}.$$

From P5, we see that distinct irreducible character determines distinct idempotent and e_i are orthogonal to one another. e_i is called linear idempotent if χ_i is linear and e_i is called nonlinear idempotent if χ_i is nonlinear. To distinguish linear and nonlinear idempotent, we let e_i be linear for $1 \leq i \leq p^2$, and e_i' be nonlinear for $1 \leq i \leq p - 1$. Let $M_L = \{e_i \mid e_i$ linear idempotent$\}$ and $M_N = \{e_i' \mid e_i'$ nonlinear idempotent$\}$.

3. Group codes defined using extra-special p-group of order p^3

To study a group code, we need the following trivial result [2, Lemma 1.3].

Lemma 1. *Let H be a subgroup of K. If T is a set of right transversal of H in K, then every element $u \in FK$ can be written uniquely in the form $u = \sum_{t\in T} a_t t$, with $a_t = \sum_{h\in H} b_h h \in FH$.*

From P5 and by taking $H = G'$ in Lemma 1, every idempotent e_k in FG can be written as

$$e_k = \frac{\chi_k(1)}{p^3}\left[\sum_{j=0}^{n-1}\sum_{i=0}^{p-1}\left(\chi_k\left(t_j^{-1}g^{-i}\right)g^i t_j\right)\right] \tag{3.1}$$

e_k can also be written as $\sum_{j=0}^{n-1} e_{kj}$, $e_{kj} = \frac{\chi_k(1)}{p^3}\left[\sum_{i=0}^{p-1}\chi_k(t_j^{-1}g^{-i})g^i\right]t_j$ is a linear combination of elements in $G't_j$ and we simply say e_{kj} corresponds to $G't_j$ or the "j^{th}-component" of e_k. Similarly, by Lemma 1 any word $u = \sum_{g\in G}\lambda_g g \in FG$ can be written uniquely as

$$u = \sum_{j=0}^{n-1}\left(\sum_{i=0}^{p-1}\lambda_{ji}g^i\right)t_j,\ \lambda_{ji} \in F. \tag{3.2}$$

$u_j = \sum_{i=0}^{p-1}\lambda_{ji}g^i t_j$ that corresponds to $G't_j$ is called the "j^{th}- component" of $u = \sum_{j=0}^{n-1} u_j$. Multiplication between u and e_k is given by $ue_k = \sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1}u_j\right)e_{k_i}$, which is called the parity check equation of e_k.

Remark. The property $G' = Z(G)$ provides an easy way to do calculation because we can always concentrate in G', whose elements commute with all the other elements in G. Because of this, in (3.1) and (3.2) we decompose the words and idempotents of FG into distinct "component" where each "component" corresponds to a unique coset of G'.

To obtain the dimension of I_μ, we need the help from the following theorem [5, Theorem 3.2].

Theorem 2. *Let K be a finite group of order n, and F be an algebraically closed field with* $\text{char}(F) \nmid n$. *Then* $FK \approx Mat_{n_1}(F) \oplus \cdots \oplus Mat_{n_s}(F)$, *where* $n = n_1^2 + \cdots + n_s^2$. *FK has exactly s nonisomorphic irreducible modules, of dimensions* $n_1, \cdots, n_s$, *and s is the number of conjugacy classes of K.*

FG can be written as $FG = \left(\overset{p^2}{\underset{i=1}{\oplus}} FGe_i\right) \oplus \left(\overset{p-1}{\underset{j=1}{\oplus}} FGe_j{}'\right)$ where $e_i \in M_L$, $\forall\, i$ and $e_i' \in M_N$, $\forall\, j$. It follows from Theorem 2 that $FGe_i \approx Mat_1(F)$, $\forall\, e_i \in M_L$, and $FGe_i' \approx Mat_p(F)$, $\forall\, e_i' \in M_N$. Thus, if $e_i \in M_L$, then $\dim(FGe_i) = 1$, and if $e_i' \in M_N$, then $\dim(FGe_i') = p^2$. We can immediately construct the following 2 families of group codes:

(1) If $\mu \subseteq M_L$ then $\dim(I_\mu) = \dim(FG) - |\mu| \dim(FGe_i) = p^3 - |\mu|$, and so I_μ is a $[p^3, p^3 - |\mu|, d_1]$ group code where $d_1 = d(I_\mu)$. We call I_μ the Type 1 Group Code.

(2) If $\mu \subseteq M_N$, then $\dim(I_\mu) = \dim(FG) - |\mu| \dim(FGe_i) = p^3 - p^2\,|\mu|$, and so I_μ is a $[p^3, p^3 - |\mu|\, p^2, d_2]$ group code where $d_2 = d(I_\mu)$. We call I_μ the Type 2 Group Code.

In Section 4 and Section 5, we will determine d_1 and d_2.

4. $d_1 = d(I_\mu)$, minimum distance of the type 1 group code

Assume F contains a primitive p^{th} root of unity such that $\text{char}(F) \neq p$ and K be the base field of F. For example, if $p = 3$, then we can take F to be the algebraic closure of F_{2^3} where F_{2^3} denotes the finite field of size 2^3. We now determined the minimum distance of Type 1 group codes defined by G over F. The idempotent corresponds to the principal character is called the principal idempotent and is denoted by $e_{principal}$. Let $\mu_0 = \{e_{principal}\}$. I_{μ_0} has length p^3 and $\dim(I_{\mu_0}) = p^3 - |\mu_0| = p^3 - 1$. To proceed further, we need the following results:

(i) By (3.1) and the definition of principal character, $e_{principal}$ can be written as:

$$e_{principal} = \frac{1}{p^3}\left(\sum_{g \in G} g\right) \tag{4.1}$$

(ii) By direct calculation, $\forall\ h \in G$, $he_{principal} = e_{principal}$ (4.2)

(iii) $\forall\ u = \sum_{i=0}^{p-1} \lambda_{0i} g^i + \left(\sum_{i=0}^{p-1} \lambda_{1i} g^i \right) t_1 + \cdots + \left(\sum_{i=0}^{p-1} \lambda_{(n-1)i} g^i \right) t_{n-1} \in FG$ where $\lambda_{ji} \in F$, by using (4.1) and (4.2), the parity check equation of $e_{principal}$ is as follows:

$$ue_{principal} = \left(\sum_{i=0}^{p-1} \lambda_{0i} + \sum_{i=0}^{p-1} \lambda_{1i} + \cdots + \sum_{i=0}^{p-1} \lambda_{(n-1)i} \right) e_{principal} \tag{4.3}$$

With (4.3), we can now show $\mathrm{d}(I_{\mu_0}) = 2$. Take any word in FG of weight 1, i.e., $u = \lambda g$ for $g \in G$. Assume $u \in I_{\mu_0}$, so $ue_{principal} = \lambda e_{principal} = 0$ which implies $\lambda = 0$. This contradicts $\mathrm{wt}(u) = 1$. Therefore, $u = \lambda g \notin I_{\mu_0}$. So $\mathrm{d}(I_{\mu_0}) > 1$. We next consider $u = \lambda g - \lambda h \in FG$ with $\mathrm{wt}(u) = 2$. $ue_{principal} = (\lambda + (-\lambda))\, e_{principal} = 0$ and so $u \in I_{\mu_0}$. This implies $d(I_{\mu_0}) = 2$. We conclude that I_{μ_0} is a $[\, p^3, p^3 - 1, 2\,]$ group code.

Now, we consider any $\mu \subseteq M_L$, $1 \le |\mu| \le p^2$. It is clear that I_μ have length p^3 and $\dim(I_\mu) = p^3 - |\mu|$. Before pressing on, we list a few useful results:

i. By (3.1) and $\chi_k(g) = 1\ \forall\ g \in G'$ where χ_k is linear, every linear idempotent can be written as:

$$e_k = \frac{1}{p^3} \left(\sum_{i=0}^{p-1} g^i \right) \left(\sum_{j=0}^{n-1} \chi_k(t_j^{-1})\, t_j \right) \tag{4.4}$$

ii. Let $A = \sum_{i=0}^{p-1} g^i$ and $e_k' = \sum_{j=0}^{n-1} \chi_k(t_j^{-1})\, t_j$, then

$$e_k = \frac{1}{p^3} A e_k' \tag{4.5}$$

iii. A is the sum of distinct element in G'. Thus, $\forall\ g \in G'$,

$$gA = A \tag{4.6}$$

iv. By (4.6), for $\sum_{i=0}^{p-1} \lambda_i g^i \in FG'$, we see that

$$\left(\sum_{i=0}^{p-1} \lambda_i g^i \right) A = \left(\sum_{i=0}^{p-1} \lambda_i \right) A \tag{4.7}$$

For any $u = \left(\sum_{i=0}^{p-1} \lambda_{0i} \, g^i \right) + \left(\sum_{i=0}^{p-1} \lambda_{1i} \, g^i \right) t_1 + \cdots + \left(\sum_{i=0}^{p-1} \lambda_{(n-1)i} \, g^i \right) t_{n-1} \in FG$ we denote $u_j = \left(\sum_{i=0}^{p-1} \lambda_{ji} \, g^i \right) t_j$ for $j = 0, 1, 2, \cdots, n-1$. The parity check equation is as follows:

$$ue_k = u_0 e_k + u_1 e_k + u_2 e_k + \cdots + u_{n-1} e_k \, . \tag{4.8}$$

Consider the j^{th}-component $u_j \, e_k$ of ue_k.

$$\begin{aligned} u_j e_k &= \left(\sum_{i=0}^{p-1} \lambda_{ji} g^i \right) t_j \, \frac{1}{p^3} A e'_k \\ &= \frac{1}{p^3} \left(\sum_{i=0}^{p-1} \lambda_{ji} g^i \right) A t_j \, e'_k \\ &= \frac{1}{p^3} \left(\sum_{i=0}^{p-1} \lambda_{ji} \right) A t_j \, e'_k && \text{(By (4.7))} \\ &= \left(\sum_{i=0}^{p-1} \lambda_{ji} \right) t_j e_k && (4.9) \end{aligned}$$

By substituting (4.9) into (4.8) for $j = 0, 1, 2, \cdots, n-1$, we obtain

$$ue_k = \left[\left(\sum_{i=0}^{p-1} \lambda_{0i} \right) + \left(\sum_{i=0}^{p-1} \lambda_{1i} \right) t_1 + \left(\sum_{i=0}^{p-1} \lambda_{2i} \right) t_2 + \cdots + \left(\sum_{i=0}^{p-1} \lambda_{(n-1)i} \right) t_{n-1} \right] e_k \tag{4.10}$$

We now show that the products of any element in the set of right transversal T of G' in G with any linear idempotent e_k are nonzero.

$$\forall \; t_i \in T, e_k \in M_L, t_i e_k = t_i \left(\frac{1}{p^3} A e'_k \right) = \frac{1}{p^3} \left(A, t_i \, e'_k \right) = \frac{1}{p^3} A \left(\sum_{j=0}^{n-1} \chi_k (t_j^{-1}) \, t_i \, t_j \right).$$

Let $s_j = t_i t_j$ for $j = 0, 1, \cdots, n-1$ and so $t_i e_k = \frac{1}{p^3} A\left(\sum_{j=0}^{n-1} \chi_k (t_j^{-1}) s_j\right)$. Since $\{s_0, \cdots, s_{n-1}\}$ is also a set of right transversal of G' in G, then $t_i e_k = \frac{1}{p^3}\left(\sum_{j=0}^{n-1} \chi_k (t_j^{-1}) As_j\right)$ is a sum of linear combination of distinct elements in G. Therefore,

$$t_i e_k \neq 0. \tag{4.11}$$

Lemma 3. *Let* $u = \sum_{i=0}^{n-1} u_i$. *If one of the* u_i *has weight* 1, *then* $u \notin I_\mu$.

Proof. Suppose $u = u_1 + u_2 + \cdots + u_{n-1}$ and $\mathrm{wt}(u_s) = 1$ for some s. Thus, $u_s = \lambda_s g^j t_s$. By (4.10), $ue_k = \left[\left(\sum_i \lambda_{0i}\right) + \cdots + \lambda_s t_s + \cdots + \left(\sum_i \lambda_{(n-1)i}\right) t_{n-1}\right] e_k$. By using (4.11), $ue_k = 0$ implies $\lambda_s = 0$ and this contradicts $\mathrm{wt}(u_s) = 1$. So $u \notin I_\mu$.

An immediate consequence of Lemma 3 is that any nonzero u in I_μ has weight at least 2, i.e., $\mathrm{d}(I_\mu) \geq 2$. The next theorem shows $\mathrm{d}(I_\mu) = 2$.

Theorem 4. $\forall\, \mu \subseteq M_L, \mathrm{d}(I_\mu) = 2$.

Proof. Lemma 3 shows $\mathrm{d}(I_\mu) \geq 2$. So we try to find a codeword of weight 2 in I_μ. Choose $u = 1 - g \in FG$ for $g \in G'$. By (4.10), $ue_k = (1 + (-1)) e_k = 0 \,\forall\, e_k \in \mu$ which implies $u = 1 - g \in I_\mu$ and so $\mathrm{d}(I_\mu) = 2$.

We next show a general result for the group codes I_μ in FG where G is the extra-special 2-group.

Theorem 5. *For the extra-special 2-group G,* $\forall\, \mu \subseteq M_L, I_\mu \lhd FG$ *is an even weight group code.*

Proof. Let G be an extra-special 2-group. By definition of G, we know that $|G'| = 2$. And so $G' = \langle g \rangle = \{1, g\}$ where $g^2 = 1$. Let $u \in I_\mu$ be written as $u = u_0 + u_1 + u_2 + \cdots + u_{n-1}$. Since each cosets of G' has size 2, each component u_i has either weight 0 or weight 2. Evidently, the element $u_i = \alpha_i (1 - g) t_i$ where $\alpha_i = 0$

or 1, is in I_μ. Thus $u = \sum_{i=0}^{n-1} u_i$ is in I_μ and so I_μ contains elements of weight $2, 4, 6, \cdots, 2n$. This clearly shows that u has even weight. Therefore, I_μ is an even weight group code.

Theorem 6. *Let G be an extra-special p-group G of order* p^3 *where p is an odd prime.* $\forall\ \mu \subseteq M_L$, I_μ *contains codeword of weight* h *for* $2 \le h \le |G|$, $h \in N$.

Proof. By definition of *G*, $|G'| = p$. And so $G' = \langle g \rangle$ where $g^p = 1$. For any integer *k*, $2 \le k \le p$. Let $u = u_1 + u_2 + \cdots + u_{n-1}$ and $u_i = \left[\left(\sum_{j=0}^{k-2} g^j \right) - (k-1) g^{k-1} \right] t_i$ with $\mathrm{wt}(u_i) = k$, then $u_i e = [(k-1) - (k-1)] t_i e = 0\ \forall\ e \in \mu$. This implies $u_i \in I_\mu$. Consequently $ue = u_1 e + u_2 e + \cdots + u_{n-1} e = 0$ and so $u \in I_\mu$. We see that they may happen that $u = u_i$ for $u_i \ne 0$, then $2 \le \mathrm{wt}(u) \le p$. If $u = u_i + u_j$ where u_i, u_j are distinct and nonzero, then $4 \le \mathrm{wt}(u) = \mathrm{wt}(u_i) + \mathrm{wt}(u_j) \le 2p$. Thus, if $u = \sum_{i=0}^{r-1} u_i$ where all u_i are nonzero and distinct, then $2r \le \mathrm{wt}(u) \le rp$. Since *G* has $n = p^2$ right cosets of G', so *u* has at most *n* components. Thus, for $u = \sum_{i=0}^{n-1} u_i$ where some u_i may be zeros, we have $2 \le \mathrm{wt}(u) \le np = |G|$. That is, I_μ contains elements of weight $2, 3, \cdots, p, p+1, \cdots, 2p-1, 2p, \cdots, p^3$.

Example 1. Consider *FG* where $G = Z_9 \times_\theta Z_3$ is the extra-special 3-group of order 27. By arbitrariness in the choice of linear idempotents of *FG*, we obtain 9 different families of group codes all with minimum distance 2. Theorem 6 ensures that we can find codeword of weight *h* for $2 \le h \le 27$, $h \in \boldsymbol{N}$. We now try to find some codeword of weight 3 in I_μ for arbitrary choice of μ. $\forall\ \mu \subseteq M_L$, from (4.5) we know that $e_i \in \mu$ has the form $e_i = \frac{1}{p^3} A e_i'$. Knowing $G' = \{1, b^3, b^6\}$, then $A = 1 + b^3 + b^6$. Thus, $e_i = \frac{1}{27}(1 + b^3 + b^6) e_i'$ for $i = 1, 2, \cdots, 9$. Take $F = F_{2^2}$ and let ε be a primitive 3^{th} root of unity in *F*. We see that $u = b + b^4 \varepsilon + b^7 \varepsilon^2 \in I_\mu$ because $\forall\, e_i \in \mu$, $ue_i = \frac{1}{27}(b + b^4 + b^7)(1 + \varepsilon + \varepsilon^2) e_i' = 0$. Similarly, $u = 1 + b^3 \varepsilon + b^6 \varepsilon^2 \in I_\mu$, $u = ba^2 + b^4 a^2 \varepsilon + b^7 a^2 \varepsilon^2 \in I_\mu$ and so on.

5. $d_2 = \mathrm{d}(I_\mu)$, minimum distance of the type 2 group code

We shall now determine the minimum distance of the Type 2 Group Codes. The following results are essential.

i. For all χ_k that are nonlinear, $\chi_k(g) = 0$, $\forall\ g \notin G'$. Thus, $\forall\ e_k \in M_N$,

$$e_k = \frac{1}{p}\left(\sum_{i=0}^{p-1} \varepsilon^{-ki} g^i\right), 1 \geq k \leq p-1, \tag{4.12}$$

where ε is a primitive p^{th} root of unity in F.

ii. $\forall\, e_k \in M_N$ and $t \in T$,

$$te_k \neq 0 \tag{4.13}$$

iii. Let $u = u_0 + u_1 + \cdots + u_{n-1}$ where $u_j = \left(\sum_{i=0}^{p-1} \lambda_{ji} g^i\right) t_j$ for $j = 0, 1, 2, \cdots, n-1$. For $e_k \in M_N$, the parity check equation of e_k is given by

$$ue_k = \left[\left(\sum_{i=0}^{p-1} \lambda_{0i}\, \varepsilon^{ki}\right) + \left(\sum_{i=0}^{p-1} \lambda_{1i} \varepsilon^{ki}\right) t_1 + \left(\sum_{i=0}^{p-1} \lambda_{2i}\, \varepsilon^{ki}\right) t_2 + \cdots + \left(\sum_{i=0}^{p-1} \lambda_{(n-1)i} \varepsilon^{ki}\right) t_{n-1}\right] e_k \tag{4.14}$$

From (4.13), we know that $t_i e_k$ is a linear combination of elements in $G't_i$ and since G', $G't_1, \cdots, G'_{t_{n-1}}$ are all disjoint cosets, we see that $ue_k = 0$ if and only if all coefficients are zeros, that is,

$$\sum_{i=0}^{p-1} \lambda_{0i}\, \varepsilon^{ki} = 0,\ \sum_{i=0}^{p-1} \lambda_{1i}\, \varepsilon^{ki} = 0,\ \sum_{i=0}^{p-1} \lambda_{2i}\, \varepsilon^{ki} = 0, \cdots \text{ and } \sum_{i=0}^{p-1} \lambda_{(n-1)i}\, \varepsilon^{ki} = 0.$$

Let us now demonstrate the fact that the nonlinear idempotent in M_N is an idempotent of FG'.

From (4.12), $M_N = \left\{ e_k = \frac{1}{p}\left(\sum_{i=0}^{p-1} \varepsilon^{-ki} g^i\right) \mid k = 1, 2, \cdots, p-1 \right\}$. $G' = \langle g \rangle$ has p linear characters, and each linear character χ_i of G' corresponds to a linear idempotent of FG'. We denote the linear idempotent of FG' by $e_{i_{G'}}$ and the set consisting of all $e_{i_{G'}}$ is denoted by $M_{N_{G'}}$.

$$\forall\, e_i \in M_{N_{G'}},\ e_{i_{G'}} \frac{1}{|G'|} \sum_{j=0}^{p-1} \chi_i(1)\, \chi_i(g^{-j})\, g^j = \frac{1}{p} \sum_{j=0}^{p-1} \chi_i(g^{-1})^{g^j}.$$

Since $g^p = 1$, then $\chi(g)^p = \chi(g^p) = \chi(1) = 1$. If χ is not the principal character, then $\chi(g) = \varepsilon$ where ε is a primitive p^{th} root of unity in F. So $\chi(g^j) = \varepsilon^j$ for $1 \le j \le p-1$. In general, $\chi_i(g^{-j}) = \varepsilon^{-ij}$ for $1 \le i \le p$. Therefore,

$$e_{i_{G'}} = \frac{1}{p} \sum_{j=0}^{p-1} \varepsilon^{-ij} g^j = \frac{1}{p} \sum_{j=0}^{p-1} (\varepsilon^{-i} g)^j \quad \text{for} \quad i = 1, 2, \cdots, p-1.$$

From (4.12), we see that $M_N = M_{N_{G'}} -$ {principal idempotent in FG'}. We collect this fact in the following lemma.

Lemma 7. $M_N = M_{N_{G'}} -$ {*principal idempotent in* FG'}.

Example 2. Consider $G = Z_3 \times_\theta Z_9$. It can be found from the character table of G that $e_1 = \frac{1}{3}(1 + \theta^2 b^3 + \theta b^6)$ and $e_2 = \frac{1}{3}(1 + \theta^2 b^6 + \theta b^3)$ are nonlinear idempotents of FG. Let $G' = \langle b^3 \rangle = \{1, b^3, b^6\}$ where $b^9 = 1$ and $1 \ne \theta \in F$, $\theta^3 = 1$. FG' consists of 3 linear idempotents, i.e., $e_{1_{G'}}\ \frac{1}{3}(1 + b^3 + b^6)$ the principal idempotent, $e_{2_{G'}} = \frac{1}{3}(1 + \theta^2 b^3 + \theta b^6)$ and $e_{3_{G'}} = \frac{1}{3}(1 + \theta b^3 + \theta^2 b^6)$. We see that $e_1 = e_{2_{G'}}$ and $e_2 = e_{3_{G'}}$.

Recall that $M_N = \{e_1, e_2, \cdots, e_{p-1}\}$. If $\mu \subseteq M_N$ and $\mu = \{e_j, e_{j+1}, \cdots, e_{j+k}\}$ then we say μ is a consecutive set. In Section 5.1, we shall show that if μ is a consecutive set then $\mathrm{d}(I_\mu) = |\mu| + 1$. In Section 5.2, we shall show that the result still holds if we carefully choose a suitable field.

5.1. Group codes defined using consecutive set that consists of nonlinear idempotents

We now find the minimum distance of I_μ if μ happens to be a consecutive set. We first state some definitions and notation. Let ε be a primitive p^{th} root of unity in F. $M(\varepsilon^{i_1}, \varepsilon^{i_2}, \cdots, \varepsilon^{i_l})$ is a $l \times p$ matrix that has $1, \varepsilon^{i_k}, \varepsilon^{2i_k}, \cdots, \varepsilon^{(p-1)i_k}$ as its k^{th} row for

$k = 1, 2, \cdots, l$, that is, $$M(\varepsilon^{i_1}, \varepsilon^{i_2}, \cdots, \varepsilon^{i_l}) = \begin{pmatrix} 1 & \varepsilon^{i_1} & \varepsilon^{2i_1} & \cdots & \varepsilon^{(p-1)i_1} \\ 1 & \varepsilon^{i_2} & \varepsilon^{2i_2} & \cdots & \varepsilon^{(p-1)i_2} \\ . & . & . & \cdots & . \\ . & . & . & \cdots & . \\ 1 & \varepsilon^{i_l} & \varepsilon^{2i_l} & \cdots & \varepsilon^{(p-1)i_l} \end{pmatrix}.$$

For convenience, we write $M = M(\varepsilon^{i_1}, \varepsilon^{i_2}, \cdots, \varepsilon^{i_l})$. We now let $J \subseteq \{0, 1, 2, \cdots, p-1\}$, then M_J is the submatrix of M consists of the columns indexed by elements of J. A $p \times p$ matrix V of the form

$$\begin{pmatrix} 1 & 1 & . & . & 1 \\ \varepsilon_1 & \varepsilon_2 & . & . & \varepsilon_p \\ {\varepsilon_1}^2 & {\varepsilon_2}^2 & . & . & {\varepsilon_p}^2 \\ . & . & . & . & . \\ {\varepsilon_1}^{p-1} & {\varepsilon_2}^{p-1} & . & . & {\varepsilon_p}^{p-1} \end{pmatrix}$$

is called a Vandermonde matrix and $\det(V) = \prod_{1 \le i < j \le n} (\varepsilon_j - \varepsilon_i) \neq 0$ (refer [2]).

Lemma 8. *If ε is a primitive p^{th} root of unity in F and $|J| = t$ then $M_J = M(\varepsilon^i, \varepsilon^{i+1}, \cdots, \varepsilon^{i+t-1})_J$ has rank t.*

Proof. M has the form

$$\begin{pmatrix} 1 & \varepsilon^i & \varepsilon^{2i} & \cdots & \varepsilon^{(p-1)i} \\ 1 & \varepsilon^{i+1} & \varepsilon^{2(i+1)} & \cdots & \varepsilon^{(p-1)(i+1)} \\ . & . & . & \cdots & . \\ . & . & . & \cdots & . \\ 1 & \varepsilon^{i+t-1} & \varepsilon^{2(i+t-1)} & \cdots & \varepsilon^{(p-1)(i+t-1)} \end{pmatrix}_{t \times p}.$$

Case 1. If $J \subseteq \{0,1,2,\cdots,p-1\}$ is consecutive, i.e., $J=\{k,k+1,\cdots,k+t-1\}$ with $k \geq 0$ and $t+k \leq p$, then

$$M_j = \begin{pmatrix} \varepsilon^{ik} & \varepsilon^{i(k+1)} & \cdots & \varepsilon^{i(k+t-1)} \\ \varepsilon^{(i+1)k} & \varepsilon^{(i+1)(k+1)} & \cdots & \varepsilon^{(i+1)(k+t-1)} \\ . & . & \cdots & . \\ \varepsilon^{(i+t-1)k} & \varepsilon^{(i+t-1)(k+1)} & \cdots & \varepsilon^{(i+t-1)(k+t-1)} \end{pmatrix}_{t\times t}.$$

Divide each entry in the m^{th} row of M_J with $\varepsilon^{(i+m-1)k}$ for $1 \leq m \leq t$, then we obtain

$$R = \begin{pmatrix} 1 & \varepsilon^{i} & \varepsilon^{2i} & . & \varepsilon^{(t-1)i} \\ 1 & \varepsilon^{i+1} & \varepsilon^{2(i+1)} & . & \varepsilon^{(t-1)(i+1)} \\ 1 & \varepsilon^{i+2} & \varepsilon^{2(i+2)} & . & \varepsilon^{(t-1)(i+2)} \\ . & . & . & . & . \\ 1 & \varepsilon^{i+t-1} & \varepsilon^{2(i+t-1)} & . & \varepsilon^{(t-1)(i+t-1)} \end{pmatrix}.$$

R^T is a Vandermonde matrix with $\det(R^T)=\det(R)\neq 0$. Since $\det(M_J)=h\det(R)$ for some $0 \neq h \in F$, then $\det(M_J)\neq 0$ and so rank(M_J) = t.

Case 2. If $J \subseteq \{0,1,2,\cdots,p-1\}$ is not consecutive, i.e., $J=\{k_1,k_2,\cdots,k_t\}$, then

$$M_J = \begin{pmatrix} \varepsilon^{ik_1} & \varepsilon^{ik_2} & \cdots & \varepsilon^{ik_t} \\ \varepsilon^{(i+1)k_1} & \varepsilon^{(i+1)k_2} & \cdots & \varepsilon^{(i+1)k_t} \\ . & . & \cdots & . \\ \varepsilon^{(i+t-1)k_1} & \varepsilon^{(i+t-1)k_2} & \cdots & \varepsilon^{(i+t-1)k_t} \end{pmatrix}_{t\times t}.$$

Divide each entry in the m^{th} column of M_J with ε^{ik_m} for $1 \leq m \leq t$, 1 then we obtain

$$S = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \varepsilon^{k_1} & \varepsilon^{k_2} & \cdots & \varepsilon^{k_t} \\ . & . & \cdots & . \\ \varepsilon^{(t-1)k_1} & \varepsilon^{(t-1)k_2} & \cdots & \varepsilon^{(t-1)k_t} \end{pmatrix}_{t\times t}.$$

S is again a Vandermonde matrix with $\det(S)\neq 0$ and hence $\det(M_J)$ is nonzero. Therefore, $\text{rank}(M_J)=t$.

Now, we determine $\mathrm{d}(I_\mu)$. If $u = \lambda g^i t \in I_{\{e_k\}}$ for $g^i \in G'$ and $t \in T$ then $ue_k = (\lambda\varepsilon^{ik}) te_k$. By (4.13), $te_k \neq 0$ and so $ue_k \neq 0$. This shows that $u \notin I_{\{e_k\}}$, and so $\mathrm{d}(I_{\{e_k\}}) > 1$. On the other hand, we can choose $u = (g^i - \varepsilon^{(i-j)k} g^j) t \in FG$ for $i \neq j$ so that $ue_k = (\varepsilon^{jk} - \varepsilon^{(i-j)k}\varepsilon^{jk}) te_k = 0$. Therefore, $u \in I_{\{e_k\}}$. This shows that $\mathrm{d}(I_{\{e_k\}}) = 2$.

Theorem 9. *If* $\mu \subseteq M_N$ *and* $\mu = \{e_{k+1}, e_{k+2}, \cdots, e_{k+t}\}$ *then* $\mathrm{d}(I_\mu) = t+1$.

Proof. We proceed by induction on $|\mu|$. For $|\mu| = 1$, we have showed above. Assume that the theorem is true if $u' = \{e_{k+1}, e_{k+2}, \cdots, e_{k+t-1}\}$. So $\mathrm{d}(I_{\mu'}) = |\mu'| + 1 = t$. Let $\mu = \mu' \cup \{e_{k+1}\}$. Since $\mu' \subseteq \mu$ then $\mathrm{d}(I_\mu) \geq \mathrm{d}(I_{\mu'}) = t$. We separate our proof into two parts. In Part (i), we show I_μ does not contains codeword of weight *t*, and then in Part (ii) we show I_μ contains at least one codeword of weight $t+1$, then our theorem is proved.

Part (i). To proof Part (i), we assume I_μ contains codeword of weight *t* and try to obtain a contradiction. Note that a word *u* of weight *t* in *FG* may be a sum of one or more components, that is , $u = u_0 + u_1 + \cdots + u_{n-1}$ where some u_i may be zeros.

First, we assume *u* has the form $u = u_j$ where u_j is the j^{th}-component of weight *t*.

Let $u = (\lambda_1 g^{i_1} + \lambda_2 g^{i_2} + \cdots + \lambda_t g^{i_t}) t_j$ where $1 \leq i_1 < i_2 < \cdots < i_t \leq p$.

By (4.14),
$$ue_{k+1} = \left(\lambda_1\varepsilon^{(k+1)i_1} + \lambda_2\varepsilon^{(k+1)i_2} + \cdots + \lambda_t\varepsilon^{(k+1)i_t}\right) t_j\, e_{k+1}$$
$$ue_{k+2} = \left(\lambda_1\varepsilon^{(k+2)i_1} + \lambda_2\varepsilon^{(k+2)i_2} + \cdots + \lambda_t\varepsilon^{(k+2)i_t}\right) t_j\, e_{k+2}$$
$$\cdots$$
$$ue_{k+t} = \left(\lambda_1\varepsilon^{(k+t)i_1} + \lambda_2\varepsilon^{(k+t)i_2} + \cdots + \lambda_t\varepsilon^{(k+t)i_t}\right) t_j\, e_{k+t}$$

$u \in I_\mu$ if and only if $ue_{k+1} = ue_{k+2} = \cdots = ue_{k+t} = 0$. Therefore, we obtain a homogenous system of linear equations that can be written in the form $H\lambda = \boldsymbol{0}$ as follows:

$$\begin{pmatrix} \varepsilon^{(k+1)i_1} & \varepsilon^{(k+1)i_2} & \varepsilon^{(k+1)i_3} & \cdots & \varepsilon^{(k+1)i_t} \\ \varepsilon^{(k+2)i_1} & \varepsilon^{(k+2)i_2} & \varepsilon^{(k+2)i_3} & \cdots & \varepsilon^{(k+2)i_t} \\ . & . & . & \cdots & . \\ \varepsilon^{(k+t)i_1} & \varepsilon^{(k+t)i_2} & \varepsilon^{(k+t)i_3} & \cdots & \varepsilon^{(k+t)i_t} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ . \\ \lambda_t \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ . \\ 0 \end{pmatrix}$$

where

$$H = \begin{pmatrix} \varepsilon^{(k+1)i_1} & \varepsilon^{(k+1)i_2} & \varepsilon^{(k+1)i_3} & \cdots & \varepsilon^{(k+1)i_t} \\ \varepsilon^{(k+2)i_1} & \varepsilon^{(k+2)i_2} & \varepsilon^{(k+2)i_3} & \cdots & \varepsilon^{(k+2)i_t} \\ . & . & . & \cdots & . \\ \varepsilon^{(k+t)i_1} & \varepsilon^{(k+t)i_2} & \varepsilon^{(k+t)i_3} & \cdots & \varepsilon^{(k+t)i_t} \end{pmatrix} \text{ is the } t \times t \text{ coefficient matrix,} \quad (4.15)$$

and $\lambda = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ . \\ \lambda_t \end{pmatrix}$.

Let $\varepsilon^{i_j} = \alpha_j$ for $1 \le j \le t$ then

$$H = \begin{pmatrix} \alpha_1^{k+1} & \alpha_2^{k+1} & \alpha_3^{k+1} & \cdots & \alpha_t^{k+1} \\ \alpha_1^{k+2} & \alpha_2^{k+2} & \alpha_3^{k+2} & \cdots & \alpha_t^{k+2} \\ . & . & . & \cdots & . \\ \alpha_1^{k+t} & \alpha_2^{k+t} & \alpha_3^{k+t} & \cdots & \alpha_t^{k+t} \end{pmatrix}.$$

Divide each entry in the m^{th} column of H by α_m^{k+1} for $m = 1, 2, \cdots, t$ and obtain

$$A = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_t \\ . & . & . & \cdots & . \\ \alpha_1^{t-1} & \alpha_2^{t-1} & \alpha_3^{t-1} & \cdots & \alpha_t^{t-1} \end{pmatrix}$$

which is a Vandermonde matrix with $\det(A) \neq 0$. Hence $\det(H) \neq 0$ and so H^{-1} exists. Therefore, $\lambda = H^{-1}\boldsymbol{0} = \boldsymbol{0}$ and this contradicts the assumption that $\mathrm{wt}(u) = t$. Thus, we conclude that $u = (\lambda_1 g^{i_1} + \lambda_2 g^{i_2} + \cdots + \lambda_t g^{i_t})t_j \notin I_\mu$.

In general, we assume $\mathrm{wt}(u) = t$ and u has the form $u = u_1 + u_2 + \cdots + u_r \in FG$ where u_i are the nonzero i^{th}-component. Let $\mathrm{wt}(u_1) = t - s$ where $s = \mathrm{wt}(u_2) + \mathrm{wt}(u_3) + \cdots + \mathrm{wt}(u_r)$. Write $u = \left(\sum_{j=1}^{t-s} \lambda_j g^{i_j} \right) t_n + v$ where $v = u_2 + u_3 + \cdots + u_r$.

By (4.14),

$$\begin{aligned} ue_{k+1} &= \left[\left(\lambda_1 \varepsilon^{(k+1)i_1} + \cdots + \lambda_{t-s} \varepsilon^{(k+1)i_{t-s}} \right) t_n + \cdots \right] e_{k+1} \\ ue_{k+2} &= \left[\left(\lambda_1 \varepsilon^{(k+2)i_1} + \cdots + \lambda_{t-s} \varepsilon^{(k+2)i_{t-s}} \right) t_n + \cdots \right] e_{k+2} \\ &\ldots \\ ue_{k+t} &= \left[\left(\lambda_1 \varepsilon^{(k+t)i_1} + \cdots + \lambda_{t-s} \varepsilon^{(k+t)i_{t-s}} \right) t_n + \cdots \right] e_{k+t} \end{aligned}$$

$u \in I_\mu$ if and only if $ue_{k+1} = ue_{k+2} = \cdots = ue_{k+t} = 0$ and so we obtain r homogenous systems of linear equations. The homogenous system corresponds to the n^{th}-component is $H_1 \lambda = \boldsymbol{0}$ where

$$H_1 = \begin{pmatrix} \varepsilon^{(k+1)i_1} & \varepsilon^{(k+1)i_2} & . & . & \varepsilon^{(k+1)i_{t-s}} \\ \varepsilon^{(k+2)i_1} & \varepsilon^{(k+2)i_2} & . & . & \varepsilon^{(k+2)i_{t-s}} \\ . & . & . & . & . \\ \varepsilon^{(k+t)i_1} & \varepsilon^{(k+t)i_2} & . & . & \varepsilon^{(k+t)i_{t-s}} \end{pmatrix}_{t \times (t-s)} \quad \text{and} \quad \lambda = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ . \\ \lambda_{t-s} \end{pmatrix}.$$

Let $\alpha_j = \varepsilon^{i_j}$ for $1 \le j \le t - s$, then by applying suitable column operation to H_1, we obtain the following matrix:

$$C = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{t-s} \\ \alpha_1^{\ 2} & \alpha_2^{\ 2} & \alpha_3^{\ 2} & & \alpha_{t-s}^{\ \ 2} \\ . & . & . & \cdots & . \\ \alpha_1^{\ t-1} & \alpha_2^{\ t-1} & \alpha_3^{\ t-1} & \cdots & \alpha_{t-s}^{\ \ t-1} \end{pmatrix}_{t \times (t-s)} .$$

By Lemma 8, any $t - s$ columns of C^T is linearly independent and so any $t - s$ rows of C is linearly independent. Hence, any $t - s$ rows of H_1 is linearly independent. Therefore, $\mathrm{rank}(H_1) = t - s$. Let $T_{H_1} : F^{t-s} \to F^t$ be the linear transformation whose matrix relative to the standard bases is H_1, then $\dim(\mathrm{Ker}(T_{H_1})) = \dim(F^{t-m})$

$-\dim(\mathrm{Im}(T_{H_1})) = t - s - \mathrm{rank}(H_1) = 0$. Thus, $\lambda_1 = \lambda_2 = \cdots = \lambda_{t-s} = 0$ which implies that $\mathrm{wt}(u) = s < t$ and this contradicts the assumption that $\mathrm{wt}(u) = t$. Therefore, $u \notin I_\mu$ and this proved Part (i).

Part (ii). Now, we consider $T_{M_1} : F^{t+1} \to F^t$, the linear transformation whose matrix relative to the standard base is M_1, where M_1 is a $t \times (t+1)$ matrix which obtain by adding one more column to the matrix H in (4.15). We may assume M_1 has the following form:

$$M_1 = \begin{pmatrix} \varepsilon^{(k+1)i_1} & \varepsilon^{(k+1)i_2} & \cdots & \varepsilon^{(k+1)i_t} & \varepsilon^{(k+1)i_{t+1}} \\ \varepsilon^{(k+2)i_1} & \varepsilon^{(k+2)i_2} & \cdots & \varepsilon^{(k+2)i_t} & \varepsilon^{(k+2)i_{t+1}} \\ . & . & . & . & . \\ \varepsilon^{(k+t)i_1} & \varepsilon^{(k+t)i_2} & \cdots & \varepsilon^{(k+t)i_t} & \varepsilon^{(k+t)i_{t+1}} \end{pmatrix}_{t\times(t+1)}.$$

We take any t columns of M_1, and obtain a $t \times t$ submatrix of M_1. By Lemma 8, this submatrix is a Vandermonde matrix with nonzero determinant. Therefore, any t columns of M_1 is linearly independent. Hence, $\mathrm{rank}(M_1) = t$. And so $\dim(\mathrm{Ker}(T_{M_1})) = \dim(F^{t+1}) - \dim(\mathrm{Im}(T_{M_1})) = 1$. This implies that there exists a set of nonzero solution for this homogenous system of linear equations. Thus, $u = (\lambda_1 g^{i_1} + \lambda_2 g^{i_2} + \cdots + \lambda_t g^{i_t} + \lambda_{t+1} g^{i_{t+1}}) t_j \in I_\mu$ and $\mathrm{wt}(u) = t + 1$.

Combining Part (i) and Part (ii), we obtain $\mathrm{d}(I_\mu) = t + 1 = |\mu| + 1$.

5.2. Group codes defined using any set of nonlinear idempotents

We now show that by choosing a finite field F with the following properties, we can proof $\mathrm{d}(I_\mu) = |\mu| + 1 \ \forall \mu \subseteq M_N$.

- **G1.** K is a base field of F and $\mathrm{char}(F) = q$.
- **G2.** F contains a primitive p^{th} root of unity, $p \neq q$.
- **G3.** q is a primitive root modulo p, i.e., $q^{p-1} \equiv 1 \pmod{p}$.

For example, if we choose $K = F_2$ and $p = 5$, then $F = F_{2^4}$ is a finite field that satisfies G1 to G3. In the next paragraph, we show the existence of such a field.

Knowing that $Z_p = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{p-1}\}$ is a finite field, so its multiplicative group $Z_p^* = \{\overline{1}, \overline{2}, \cdots, \overline{p-1}\}$ is cyclic. Let this multiplicative group be generated by $\overline{q}$. Then $GCD(p,q) = 1$ and the order of $\overline{q}$ is $\phi(p) = p-1$. So q is a primitive root modulo p. Let $F = F_{q^{p-1}}$. The multiplicative group F^* of F has order $(q^{p-1} - 1)$ and is cyclic. Since $q^{p-1} \equiv 1 (\text{mod } p)$, p divides $|F^*|$ and so F^* has an element $\overline{a}$ of order p. This $\overline{a}$ is a primitive p^{th} root of unity in F.

Next, we proof the following lemma.

Lemma 10. *If* $\text{char}(F) = q$ *is a primitive root modulo p then* $1 + x + x^2 + \cdots + x^{p-1}$ *is irreducible over* F_q.

Proof. Denote $f(x) = 1 + x + x^2 + \cdots + x^{p-1}$. Let α be a primitive p^{th} root of unity in $F_{q^{p-1}}$. Since $(\alpha - 1) f(\alpha) = \alpha^p - 1 = 0$ and $\alpha \neq 1$, so $f(\alpha) = 0$. Thus, the minimal polynomial $m_\alpha(x)$ of α divides $f(x)$. If $k = \deg(m_\alpha(x)) < p-1$, then $\left| F_q(\alpha) : F_q \right| = k$ and so $F_q(\alpha) = F_{q^k}$. So we have $\alpha^{q^k - 1} = 1$ and so $p \left| (q^k - 1) \right.$, that is, $q^k \equiv 1 (\text{mod } p)$. This contradicts that q is a primitive root modulo p. So $\deg(m_\alpha(x)) = p-1$ and we conclude that $m_\alpha(x) = f(x)$. Thus, $f(x)$ is irreducible.

By assuming $\text{char}(F)$ is a primitive root modulo p, we see that $f(x) = 1 + x + x^2 + \cdots + x^{p-1}$ is the minimal polynomial of α over K. Therefore, $(1 + x + x^2 + \cdots + x^{p-1}) \left| g(x) \right.$ for $g(x) \in K[x]$ with $g(\beta) = 0$.

Lemma 11. *Let* $\mu \subseteq M_N$ *and* $0 < |\mu| = t \leq p-1$. *Assume char(F) is a primitive root modulo p. If* $u = u_j \in FG$ *where* u_j *is the* j^{th}*-component of weight t then* $u \notin I_\mu$.

Proof. Take $\mu = \{e_{k_1}, e_{k_2}, \cdots, e_{k_t}\}$. Since $u = u_j$ of weight t then we write u as $u = (\lambda_1 g^{i_1} + \lambda_2 g^{i_2} + \cdots + \lambda_t g^{i_t}) t_j$. By (4.14),

$$ue_{k_1} = \left[\left(\lambda_1 \varepsilon^{k_1 i_1} + \lambda_2 \varepsilon^{k_1 i_2} + \cdots + \lambda_t \varepsilon^{k_1 i_t} \right) t_j \right] e_{k_1}$$

$$ue_{k_2} = \left[\left(\lambda_1 \varepsilon^{k_2 i_1} + \lambda_2 \varepsilon^{k_2 i_2} + \cdots + \lambda_t \varepsilon^{k_2 i_t} \right) t_j \right] e_{k_2}$$

$$\cdots$$

$$ue_{k_1} = \left[\left(\lambda_1 \varepsilon^{k_t i_1} + \lambda_2 \varepsilon^{k_t i_2} + \cdots + \lambda_t \varepsilon^{k_2 i_t} \right) t_j \right] e_{k_t}$$

Assume $u \in I_\mu$ then $ue_{k_1} = ue_{k_2} = \cdots = ue_{k_t} = 0$. Therefore, we obtain the following homogenous system of linear equations:

$$\begin{pmatrix} \varepsilon^{k_1 i_1} & \varepsilon^{k_1 i_2} & \cdots & \varepsilon^{k_1 i_t} \\ \varepsilon^{k_2 i_1} & \varepsilon^{k_2 i_2} & \cdots & \varepsilon^{k_2 i_t} \\ . & . & \cdots & . \\ \varepsilon^{k_t i_1} & \varepsilon^{k_t i_2} & \cdots & \varepsilon^{k_t i_t} \end{pmatrix} = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ . \\ \lambda_t \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ . \\ 0 \end{pmatrix}.$$

where
$$H = \begin{pmatrix} \varepsilon^{k_1 i_1} & \varepsilon^{k_1 i_2} & \cdots & \varepsilon^{k_1 i_t} \\ \varepsilon^{k_2 i_1} & \varepsilon^{k_2 i_2} & \cdots & \varepsilon^{k_2 i_t} \\ . & . & \cdots & . \\ \varepsilon^{k_t i_1} & \varepsilon^{k_t i_2} & \cdots & \varepsilon^{k_t i_t} \end{pmatrix}.$$

Let $\varepsilon^{i_s} = z_s$ for $1 \le s \le t$, then $H = \begin{pmatrix} z_1^{k_1} & z_2^{k_1} & \cdots & z_t^{k_1} \\ z_1^{k_2} & z_2^{k_2} & \cdots & z_t^{k_2} \\ . & . & \cdots & . \\ z_1^{k_t} & z_2^{k_t} & \cdots & z_t^{k_t} \end{pmatrix}$. If the rows of H are linearly dependent over F then there will exist $c_1, c_2, \cdots, c_t$ not all zero such that

$$c_1\left(z_1^{k_1}, z_2^{k_1}, \cdots, z_t^{k_1}\right) + c_2\left(z_1^{k_2}, z_2^{k_2}, \cdots, z_t^{k_2}\right) + \cdots + c_t\left(z_1^{k_t}, z_2^{k_t}, \cdots, z_t^{k_t}\right) = \boldsymbol{0},$$

and so
$$\left(\sum_{i=1}^{t} c_i z_1^{k_i}, \sum_{i=1}^{t} c_i z_2^{k_i}, \cdots, \sum_{i=1}^{t} c_i z_t^{k_i}\right) = \boldsymbol{0}.$$

Thus, $\sum_{i=1}^{t} c_i z_s^{k_i} = 0$ for $s = 1, 2, \cdots, t$. Denoted $f(x) = \sum_{i=1}^{t} c_i x^{k_i}$. We see that $z_1, z_2, \cdots, z_t$ are all distinct zeros of $f(x)$.

By Lemma 10, $(1 + x + x^2 + \cdots + x^{p-1}) \mid f(x)$. Since $\deg(f(x)) = t \le p - 1$, then either $f(x) \equiv 0 (\bmod 1 + x + x^2 + \cdots + x^{p-1})$ or $\deg(f(x)) = t = p - 1$. If $f(x) = 0$ then all $c_i = 0$ and this contradicts that all the rows of H are linearly dependent. Thus, the rows of H are linearly independent and so $\operatorname{rank}(H) = t$. Let $T : F^t \to F^t$ be the linear transformation whose matrix relative to the standard base is *H*. Thus $\dim(\operatorname{Ker}(T)) = t - \dim(\operatorname{Im}(T)) = t - t = 0$, and this contradicts $wt(u) = t$.

On the other hand, if $t = p-1$, then the zeros of $f(x)$ are $z_1, z_2, \cdots, z_{p-1}$. Since the zeros of $1 + x + x^2 + \cdots + x^{p-1}$ are $\varepsilon, \varepsilon^2, \cdots, \varepsilon^{p-1}$ and $(1 + x + x^2 + \cdots + x^{p-1}) \mid f(x)$, these imply $z_i = \varepsilon^j$ for some i, j. There is no loss if we assume $z_1 = \varepsilon,\ z_2 = \varepsilon^2, \cdots,\ z_{p-1} = \varepsilon^{p-1}$ and so convert H into

$$\begin{pmatrix} \varepsilon^{k_1} & \varepsilon^{2k_1} & \cdots & \varepsilon^{(p-1)k_1} \\ \varepsilon^{k_2} & \varepsilon^{2k_2} & \cdots & \varepsilon^{(p-1)k_2} \\ . & . & \cdots & . \\ \varepsilon^{k_{p-1}} & \varepsilon^{2k_{p-1}} & \cdots & \varepsilon^{(p-1)k_{p-1}} \end{pmatrix}$$

which is a Vandermonde matrix with $\det(H) \neq 0$ and so H^{-1} exists. This implies

$$\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ . \\ \lambda_t \end{pmatrix} = H^{-1} \begin{pmatrix} 0 \\ 0 \\ . \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ . \\ 0 \end{pmatrix}$$

and again this contradicts $wt(u) = t$. We conclude that $u = (\lambda_1 g^{i_1} + \lambda_2 g^{i_2} + \cdots + \lambda_t g^{i_t}) t_j \notin I_\mu$.

Theorem 12. *$\forall \mu \subseteq M_N$, if char(F) is a primitive root modulo p and $0 < |\mu| = t \leq p-1$, then I_μ does not contains codeword of weight t.*

Proof. We use induction on *t*. If $t = 1$, then μ is a consecutive set. And so $d(I_\mu) = 2$ by Theorem 9. Hence, the theorem is proved. Assume the theorem is true for $t \leq m$. Let $u \in FG$ with $\mathrm{wt}(u) = m$. We separate the proof into 2 cases:

Case 1. If u is a sum of one component, i.e., $u = u_j$ for some *j*, then Lemma 11 proved this case.

Case 2. Let $u = \sum_{i=0}^{n-1} u_i$, is a sum of at least two components. Thus, $\mathrm{wt}(u_i) < m$ for each *i*. Without loss of generality, we may assume $\mathrm{wt}(u_i) = m_i$ and $m_i \leq m_j$ if $i < j$. Let $\mu = \{e'_0, e'_1, \cdots, e'_m\}$ and $\mu_i = \{e'_0, e'_1, \cdots, e'_{m_i}\}$ for $i = 0, 1, 2, \cdots, n-1$. Since $m_i \leq m_j$ for $i < j$, then we see that $\mu_0 \subseteq \mu_1 \subseteq \cdots \subseteq \mu_{n-1}$ where $\mu_0 \neq \varnothing$ and contains at least one idempotent, say e'_0. By induction, since $\mathrm{wt}(u_i) = m_i$ and

$|\mu_i| = m_i$ then $u_i \notin I_{\mu_i}$ $\forall\ i$. Therefore, $u_i e_0' \neq 0$. Thus, $ue_0' = \sum_{i=0}^{n-1} u_i\, e_0' \neq 0$ since $u\,e_0'$ is a linear combination of elements of $G', G't_1, \cdots, G't_{n-1}$. And so we conclude that $u \notin I_\mu$.

Armed with the above results, we are in a position to establish our main result:

Theorem 13. *$\forall\ \mu \subseteq M_N$ and $1 \leq |\mu| = t \leq p-1$. If the char(F) is a primitive root modulo p then $d(I_\mu) = t+1$.*

Proof. Let $u \in FG$ with $\mathrm{wt}(u) = t$. Since $|\mu| = t$ then $u \notin I_\mu$ by Theorem 12. We next assume $\mathrm{wt}(u) = r < t$ then we may choose $\mu_0 \subset \mu$ with $|\mu_0| = r$ and again Theorem 12 implies $u \notin I_{\mu_0}$. This implies $ue \neq 0\ \forall\ e \in \mu_0$ and so $ue \neq 0$ for some $e \in \mu$. Therefore, $u \notin I_\mu$. Thus, we have showed that $\mathrm{d}(I_\mu) \geq t+1$. Now, Lemma 7 states that $\mu = \mu_{G'}$ where $\mu_{G'}$ is the set of nonprincipal linear idempotents in FG'. Since G' is a cyclic group, then by [7, Lemma 1], $\mathrm{d}(I_{\mu_{G'}}) = |\mu_{G'}| + 1$ $= t+1$. Thus, there exist $u = \lambda_{i_1} g^{i_1} + \lambda_{i_2} g^{i_2} + \cdots + \lambda_{i_t} g^{i_t} + \lambda_{i_{t+1}} g^{i_{t+1}} \in FG'$ for $g^{i_1}, g^{i_2}, \cdots, g^{i_{t+1}} \in G'$ such that $u \in I_{\mu_{G'}}$ and so $ue = 0\ \forall\ e \in \mu_{G'}$. Since $\mu = \mu_{G'}$, then $ue = 0\ \forall\ e \in \mu$. We conclude that $u \in I_\mu$ and so $\mathrm{d}(I_\mu) \geq t+1$.

By Theorem 13, I_μ is a $[p^3, p^3 - p^2|\mu|, +1]$ group code with information rate $R = 1 - \frac{|\mu|}{p}$. We emphasize that I_μ is a nonabelian code and is not a MDS code.

6. Conclusions

We make a few remarks to conclude this paper. The following two families of group codes had been constructed:

(a) In Section 4, we found the Type 1 Group Codes I_μ, which is a $[p^3, p^3 - |\mu|, 2]$ – single error detecting code. We also proved that if $p = 2$, then I_μ is an even weight group code, and if $p > 2$, then I_μ contains codeword of weight h for $2 \leq h \leq |G|$, $h \in \boldsymbol{N}$.

(b) For the Type 2 Group Codes in Section 5, either by choosing $\mu \subseteq M_N$ to be a consecutive set or *F* with the property that char (*F*) is a primitive root modulo *p*, we obtained a $\frac{|\mu|}{2}$ – error correcting group code.

(c) Extra special *p*-group is a special case of a relative *M*-group with respect to all its subgroups. Results in this paper hold if we take *G* to be a relative *M*-group with respect to all its subgroups.

Acknowledgement. The first author is supported by the Fundamental Research Grant 304, PMATHS 670021.

References

1. D.S. Passman, *The Algebraic Structure of Group Rings*, New York: Wiley, 1977.
2. I.M. Isaacs, *Algebra, A Graduate Course*, Brooks/Cole Publishing. Pacific Grove, California, 1992.
3. I.M. Isaacs, *Character Theory of Finite Groups*, Academic Press, 1976.
4. J.H. Van Lint and R.M. Wilson, On the minimum distance of Cyclic code, *IEEE Trans. Inform. Theory* **32** (1986), 23–40.
5. L. DornHoff, *Group Representation Theory*, Part A. Marcel Dekker, inc., New York, 1971.
6. N.J.A. Sloane and F.J. Macwilliam, *The Theory of Error Correcting Codes*, Amsterdam, The Netherlands: North-Holland, 1978.
7. S.D. Berman, 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** (1989).