Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 17, Number 2 (2024) pp. 103-112

https://dx.doi.org/10.37622/ACST/17.2.2024.103-112

Application of Group algebra R[G] in Communication (Coding Theory)

Dr. Hiteshwar Singh[1] and Dhananjay Kumar Mishra[2,*]

[1](Ex-Faculty, M. L. S. M. College, Darbhanga)
[2],(Dept. of Mathematics L. N. M. U. Darbhanga)*

Abstract

In this research paper we have tried to show that the group algebra is very prominent in theory of error correcting codes. We have studied codes which are constructed from ideals in group algebra. We have established the use of Hamming distance, dimension as well as weight of codes, which are derived from a group algebra. Here we have presented a special type of idempotent of group algebra E[G]. If H is a sub group of G then, $\widehat{H}$=1/|H|$\sum_{h\in H} h$ will be an idempotent of E[G]. By taking an idea from such type of idempotent we have introduced some special type of idempotent and studied the ideal which are generated from them. We have tried to show that the codes which are generated by abelian non-cyclic groups, are more convenient and useful than the codes from the cyclic group. We have also discussed about non-abelian codes and their utility.

Keywords: Non-abelian group, codes, ideals, cyclic group, weight, hamming distance, group code, abelian group.

1. Introduction

Group algebra is very important for the theory of error-correcting codes. In this paper we have focused on relationship between weight and dimension of group codes. Such type of codes have been the object of active research in [6],[14],[16],[18],[20],[22],[24],[26],[28],[21],[19],[11], and [5]. In this paper we shall not discussed upon the theory such as encoding and decoding because these are not directly related to our objectives.

2. A brief and short history

At the early days a method was made to prevent a computer from working with wrong data. Computer gets information which was composed of a series of digits equal to either 0 or 1. If we choose such a word that could be 10100110011.Then we add an extra digit at the end of each such word. It is termed as parity-check digit, which would be equal to 0 or 1 depending upon whether the number of bits equal to 1 in the given word were even or odd. In case of our example the parity check would be 0 and the extended word would be 101001100110. Thus every extended word sent to the computer would have 12 digits and an even number of bits equal to 1. After receiving each word the computer would check the number of digits equal to 1 and in case this number were odd it would know that there was a mistake in this word and stop to work. Of course this method has some difficulties. First one is if two mistakes were found the error would not be detected. Further also if the existence of a mistake is detected, it not possible to determine, which is the wrong bit in the word. This method was used very first in 1947 at the Bell Telephone Laboratories, where the engineer Richard W. Hamming was working. During those days computer were much slower than as these days. It had taken weekend to proceed its job. The computer might have worked on each job and if an error was detected it might have just stopped and started to the next job. To overcome such type of problem Richard W. Hamming had got an idea of error correcting codes. He started to work on the idea of error correcting codes. He thought to add to each word not just one parity-check digits but more digits, those he had termed redundancy. It might have allowed to locate the errors and corrected them. In 1947 at Bell Telephone Company he developed a code in which information to be transmitted was made up of a word of four bits. Then he added four bits of redundancy. Let us suppose that a_1, a_2, a_3, a_4 be a word to be transmitted. Now it can be written as a matrix of size 2x2,

$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$. Now we extend it to a matrix of size 3×3 in such a way that each row and column has an even number of digits equal to 1. $\begin{pmatrix} a_1 & a_2 & b_1 \\ a_3 & a_4 & b_2 \\ c_1 & c_2 & \end{pmatrix}$

Thus the matrix can be written as a word a_1, a_2, b_1, a_3, a_4, b_2, c_1, c_2. Let us take a word 1101 in matrix of the form $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and the extended matrix so formed, $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ & 1 & 0 \end{pmatrix}$

Thus word that has sent to the computer would be 11001110, and computer would produce 3x3 matrix as well as would check parity of rows and columns along with it is possible to detect the existence of the error and its position so that it can be corrected. Let us choose another word to be sent to computer a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9 in matrix

form $\begin{pmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{pmatrix}$. Word will be 111011010. After extension word will be sent to computer 1111011001011. Matrix in extended form is

$$\begin{pmatrix} a_1 & a_2 & a_3 & b_1 \\ a_4 & a_5 & a_6 & b_2 \\ a_7 & a_8 & a_9 & \\ c_1 & c_2 & & \end{pmatrix}$$

Corresponding coding matrix is, $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & \\ 1 & 1 & & \end{pmatrix}$

3. Some Basic Facts about the codes: A code is a language which is derived to communicate with a machine. There are some fundamental elements which are used to produce a code;

(1) A finite set $A^{\#}$ is termed as an alphabet, and its elements are known as letters. We write q=|A| the number of elements in $A^{\#}$ and we say that code is q-ary.

(2) The finite sequences of elements of $A^{\#}$ are words. The number of letters in a word is known as its length. Here we shall assume that all the words in the codes taken have the same length.

(3) A q-ary code C of length n, this means a code C is a subset of $(A^{\#})^n = A^{\#}.A^{\#}.A^{\#}.....A^{\#}$(n-times). This set is also known as the ambient space F^n_q of the code.

(4) Hamming distance: Let us supposed that there be two words $x=(x_1, x_2, \ldots\ldots, x_n)$ and $y=(y_1, y_2, \ldots.., y_n)$ in a code $C \subset (A^{\#})^n$. The Hamming distance from x to y is the number of coordinates in which these elements differ, which is as $d(x, y)=|\{i, 1\leq i \leq n| x_i \neq y_i \}|$. For given a code $C \subset (A^{\#})^n$ is the minimal distance of C is the number $d=\min \{d(x, y)|x, y \in C, x\neq y \}$. Let us take a rational number α as the greatest integer $[\alpha]$ such that any greatest integer $m \leq \alpha$. One of the important result in coding theory is the following.

Theorem: Let us suppose that C be a code with minimal distance d and let us put, K=[d-1/2]. Then it is possible to detect up to d-1 errors and correct up K errors. The number K is called error correcting capacity of the code.

(5) A q-ary code of length n, which contains M words and having minimal distance d is termed as (n, M, d)-code. When we design a code, we try to make its efficiency heavy and minimal distance large so that it can correct a big number of errors. But it is very hard to do so, because the ambient space $(A^{\#})^n$ is finite. The main problem of coding theory is that to maximize the one parameters (n, M, d) when the other two are given. We will construct a linear code, which is the most important class

of codes. We choose as an alphabet, a finite field F_q with q elements, here q is power of a prime p=*char* (F_q). The ambient space F_q^n will be a vector space of dimension n over F_q^n. A linear code C of length n over F_q is a proper linear sub space of F_q. If we have dimension dim(C) =m than, $m \leq n$. So we have found that the number of words in code C will be q^m, and we get a new cods in code as (n, m, d)-code. E. Prange [17] in 1957 had introduced a special class of linear codes. Such type of codes have efficient implementation. Let us take a word $(x_1, x_2, \ldots\ldots, x_n) \in C \Rightarrow (x_n, x_1, x_2, \ldots\ldots, x_{n-1}) \in C$. Thus if $(x_1, x_2, \ldots, x_n)$ is a code then all its permutations are also in codes. Now we choose a map $\emptyset$ such that, $\emptyset: F_q^n \rightarrow F_q[X]/(X^n-1)$ which will be presented as $\emptyset(a_0, a_1, \ldots, a_{n-1}, a_{n-2}) = a_0+a_1X+\ldots..+a_{n-1}X^{n-1}$ here [f] is the class of polynomials $f \in F_q[x]$ in R_n, which is the linear isomorphism. So it is clear to observe that a linear subspace C in F^n_q is a cyclic code if and only if $\emptyset(C)$ is an ideal of $F_q[X]/(X^n-1)$. Thus the study of cyclic codes of length n over F_q^n is the same as the study of ideals in the quotient ring $F_q[X]/(X^n-1)$. But we have observed that C_n is a cyclic group of order n and Fq[Cn] is its group algebra over Fq, then we have found that $Fq[X]/(Xn-1) \cong Fq[Cn]$. Therefore we will say that the study of cyclic codes of length n over the field F_q can be also regarded as the study of ideals in the group algebra $F_q[C_n]$.

4. Formation of codes in group algebra $F_q^n[G_n]$, when we have a cyclic group G_n: We can extend the concept of code in group rings R[G] of cyclic group G as ideals to other classes of groups. It was very first done by S. D. Berman [10], [12], in 1967 and separately by F.J. Mac Williams [17], in 1970. Let we suppose that there be a group algebra of finite group G over field R is a set of all formal linear combinations, as $\alpha = \sum_{g\in G} \alpha_g.g$ as well as $\beta = \sum_{g\in G} \beta_g.g$ then we have $\alpha = \beta \iff \alpha_g=\beta_g \; \forall \; g\in G$. We will define group algebra further as, $\sum_{g\in G} \alpha_g.g + \sum_{g\in G} \beta_g.g = \sum_{g\in G}(\alpha g + \beta g)g$,

$(\sum_{g\in G} \alpha_g.g) .(\sum_{h\in G} \beta_h.h)=\sum_{g\in G(} \alpha_g.\beta_h)gh$. Let there be any constant λ in field R then we have,

$\lambda.(\sum_{g\in G} \alpha_g.g) = \sum_{g\in G(\lambda} \alpha_g.)g$. Thus the set R[G], with above operations is known as group algebra of basis set $G = \{g_1, g_2, \ldots.., g_n\}$ and $(x_1, x_2, \ldots\ldots., x_n)$ in F_q^n then the corresponding element of $F_q^n[G]$ will be written as $\alpha = x_1g_1+x_2g_2+\ldots\ldots..x_ng_n$. Now we choose a group algebra corresponding to F_q^n as $F_q[G]$ and define a group code or a G-code over F_q as an ideal of group algebra $F_q[G]$. We find that the support of an element $\alpha = \sum_{g\in G} \alpha_g.g$ in group algebra $F_q[G]$ of a group G over a field F_q is the set as $\sup(\alpha) = \{g\in G \mid \alpha_g\neq 0\}$. Now the Hamming distance between two elements of group algebra $F_q[G]$ as $\alpha = \sum_{g\in G} \alpha_g.g$ and $\beta = \sum_{g\in G} \beta_g.g$ is $d(\alpha\beta) = |\{g| \; \alpha_g\neq \beta_g, g\in A\}|$, as well as the weight of an element α of this group algebra is $w(\alpha) = d(\alpha,0) = |\text{supp}(\alpha)|$, then $w(\alpha)=|g\in G \mid \alpha_g\neq 0\}|$. For linear codes, the minimum distance of a code corresponds to the minimum weight. Let us take an ideal $I \subset F_q[G]$, the weight distribution of I is the map which assigns to each possible weight t and the number of elements of I having weight t. It is clear that due to well-known Maschke's theorem [13, corollary 3.2.8], the structure of the group algebra $F_q[G]$ depends on whether q and

|G| are relatively prime or not relatively prime. In this research paper we have assume that gcd (q,|G|)=1. In such case the group algebra $F_q[G]$ will semi-simple . This means that every two-sided ideal is a direct summand and thus it is a principal ideal, generated by an idempotent element. Further we can show that,

(1) Group algebra $F_q[G]$ is a direct sum of finite number of two-sided ideals $\{A_i\}_1 \leq i \leq r$. It is called the simple components of $F_q[G]$, and each A_i forms a simple algebra.
(2) Any two- sided ideal of group algebra $F_q[G]$ is a direct sum of some of the members of the family $\{B_i\}_1 \leq i \leq r$.
(3) Each simple component A_i will be isomorphic to a full matrix ring of the form $M_{ni}(E_i)$, here E_i is a field containing an isomorphic copy of F_q in its center**.**

As every simple component of ideal is generated by an idempotent element, so the above results can be transformed in following way.

Let us suppose that G be a finite group and F_q be a field such that char(F_q) does not divide |G| and $E[G]=\bigoplus_{i=1}^{s} A_i$ be the decomposition of group algebra as a direct sum of minimal two-sided ideals. Then there will be a family $\{e_1, e_2, \ldots\ldots, e_s\}$ of elements of E[G] such that,

(1.) $e_i \neq 0$ is a central idempotent, $1 \leq i \leq t$.
(2.) If we have $i \neq j$, then $e_i e_j = 0$
(3.) $e_1+e_2+e_3+\ldots\ldots\ldots+e_t = 1$
(4.) We cannot write e_i as $e_i = e' + e''$ here e', e'' are central idempotent provided that $e'.e'' \neq 0$ and $e'e''=0$, $1 \leq i \leq t$.
(5.) $A_i = A_{ei}$, , $1 \leq i \leq s$.

Such above idempotent are termed as the primitive central idempotent of $F_q[G]$. We can also construct idempotent in group algebra in rather standard way. If we have H is a subgroup of G then, $\widehat{H}=1/|H|\sum_{h\in H} h$ will be an idempotent of group algebra E[G] and $\widehat{H}$ will central in G if and only if H is normal subgroup in G. We have a well-known isomorphism [13] $E[G].\widehat{H} \cong E[G/H]$, and hence $\dim_E\{E[G].\widehat{H}\} = [G:H]$. Thus it is easy to find that if τ is a transversal of H in G that is a complete set of cosets of H in group G, than we have $\{t\widehat{H} | t \in r\}$ is a basis of $(E[G]).\widehat{H}$ over E. But such type of ideal is not useful in coding, because it allows repetition of codes. We will write such type of ideal as $\alpha = \sum_{t\in r} a\, t\widehat{H}$ with basis from G. Here we have seen that the same coefficient along all the elements of the idempotent, in the form of t-th for a fixed $t \in \tau$ arbitrary $h \in H$.

Therefore, we will search another kind of idempotent, which will generate more effective codes:

Now we will get the help of some theorems, which will allows us to make another idempotent that will not permit any kind of repetition in codes.

Theorem [28]: Let us suppose that G be a finite group and E be a field such that char (E) does not divide |G|. Let us choose H and H* as normal subgroups of G such that $H \subset H^*$ and set $e=H-H^*$. Then $\dim_E(E[G]) = |G/H| - |G/H^*|$ and $w\{(E[G])e\} = 2|H|$.

Let us take B as a transversal of H* in G and τ be a transversal of H in H* containing 1. Than it seen that B'= {a(1-t)$\widehat{H}$|a∈B, t∈ τ/{1} is a basis of (E[G])e over E. In such case if G is an abelian group, it is possible to consider when all primitive central idempotent can be formed in this way. Let us take an abelian p-group A^0. For each subgroup H of A^0, such that A/H≠{1} is cyclic, and we will form an idempotent of group algebra E[A^0]. As A^0/H is a cyclic subgroup of order a power of p, there exists a unique subgroup H* of A^0, containing H, such that |H*/H|=p. We put $e_H = \widehat{H} - \widehat{H*}$ and also $e_G = 1/|G| \sum_{g \in G} g$.

Theorem [28]: Let us suppose that p be an odd prime and A^0 be an abelian p-group of exponent p^r. Then the set of idempotent above is the set of primitive idempotent of $F_q[A^0]$ and only if one of the following holds good,

(1) $p^r = 2$ and q is odd
(2) $p^r = 4$ and $q \equiv 3 (mod 4)$
(3) o(q)= $\emptyset(p^n)$ in U(Z_pn), here $\emptyset$ is Euler's Totient function. In special case when G is a cyclic group of order p^n, with gcd(p,q)=1 then the above theorem gives the following result.

Corollary [28], [7]. Let E be a field with q elements and A^0 is a cyclic group of order p^n such that o(q)=$\emptyset(p^n)$ in U(Z_p^n) and also let A0=A_0 ⊃A_1⊃A_2⊃……⊃A_n ={1} be the descending chain of all subgroups of A; Then we have the set of primitive idempotent of E[A] will be given by,

$e_0 = 1/p^n \sum_{a \in A0} a$, and e_i= A_i-A_{i-1}, $1 \leq i \leq n$. We can get a similar result for cyclic group of order $2p^n$ [4], [28]. Since the idea of abelian codes was given by Berman and Mac Wiliams. These codes were constructed, were defined from minimal ideals. These codes were no longer used for the purpose, as we have needed. Let us suppose that G_1 and G_2 are two finite groups of same order. E be a finite and takes $\gamma: G_1 \rightarrow G_2$ as a bijective mapping. We write, $\overline{\gamma}$: E[G_1]→ $E[G_2]$ as its linear extension to the corresponding group algebras. Thus it is clear that $\bar{\gamma}$ is a hamming isometry, this means elements corresponding under this map have the same hamming weight. If we have two ideals I_1⊂E [G_1] and I_2⊂E[G_2] such that $\overline{\gamma}$: (I_1)=I_2 are hence equivalent. This means that they have same dimension and same weight distribution. Thus codes I_1 and I_2 are said to be permutational equivalent as well as combinational equivalent [3].

Theorem: [16] Every minimal ideal in the semi-simple group algebra $F_q[A^0]$ of a finite abelian group A^0 is permutational equivalent to a minimal ideal in the group algebra F_q[C] of a cyclic group C of the same order.

5. Construction of codes, defined from non-minimal ideals:

As we have discussed in previous section that the main problem in constructing codes to build codes with a good error correcting capacity and dimension as big as possible.

Since one of this numbers decreases as the other increases to compare the efficiency of codes with different weights and dimensions, Thus we have the following more natural concept, to overcome this challenges.

Let us choose a code C and we write convenience of code C, as in numeral way, Conv (C)=dim(C).w (C) If we a code with high convenience, this means one of the parameter is quit big and other is rather small. But such type of code is not useful. We choose a cyclic group o G= <a>, with a^{p^2}=1, which is acyclic code of order p^2 and we suppose F_q be any field as in the hypothesis of the theorem [16] above. Then from the corollary [28] [7] there exist only three principal idempotent in group algebra F[G] as

(1) $e_0=\widehat{G}$ **(2)** $e_1=\widehat{G}_1-\widehat{G}$ **(3)** $e_2=\widehat{G}_2-\widehat{G}_1$.

Therefore, the maximal ideals are , $I=I_0\oplus I_1$ and $J=I_1\oplus I_2$,with dim(I)=p, w(I)=p and dim(J)=p^2-1, w(J)=2 and hence conv(I)=p^2 as well as conv(J)=2(p^2-1). Again from theorem [16], it can be shown that if we choose A^0 =Cp . Cp then the principal idempotent of $F_q[A^0]$ are as $e_0=A^0$, $e_1=\hat{a}-\hat{A}^0$, $e_2=\hat{b}-\hat{A}^0$ as well as $f_j=\widehat{ab}^j-\hat{A}^0$, $1\leq i\leq p-1$, here a and b are generators of both direct factors. Now we have, $w(F_q[A^0])=p^2$ and dim($(F_q)e_0$)=1 and other minimal ideals $L_i=(F_q[A^0])e_0$, i=1,2 as well as $M_j=(F_q[A^0])f_i$, $1\leq i\leq p-1$.

Thus we get, $w(L_i)=2p$ $\dim(L_i)=p-1$,i=1,2,$w(M_j)=2p.\dim(M_j)=p-1$, $1\leq i\leq p-1$. If H=<h> and K=<k> are two subgroups of order p of $C_p.C_p$ the corresponding idempotent are, $e=\widehat{H}-\hat{A}^0$, $f=\widehat{K}-\hat{A}$, and we get N= $(E[A^0])e\oplus(E[A^0])f$.

Proposition: [15] The weight and dimension of $I=(E[G])e\oplus(E[G])f$ are w(N)=2p-2, so conv(N)=$4(p-1)^2$. Therefore, if prime p>3, we have conv (N) is greater than conv (I) for all proper ideal I of $F_q[C_p^2]$.

6. Codes in group algebra for non-abelian groups.

Lomonaco and Sabin [3] had studied meta-cyclic groups and they had found that central idempotent generate codes that are combinatorically equivalent to abelian codes. Recently C. Garca Pillado, S. Gonzalez, C. Martinez, V. Markov, as well as A. Nechaev, [29] found that for groups G=AB, here A and B are abelian is also valid in this case.

Therefore we should study on ideals those are generated by non-central idempotent.

Now, we try to understand the ideals, those are generated by non-central idempotent through suitable examples [6]

[1]. Let us choose a set of group G= {a, b|a^7=1=b^3, $bab^{-1}=a^2$} .

We can present the central primitive idempotent of $F_2[G]$ as

$f_1=\hat{b}\hat{a}$, $f_2=(1-\hat{b})\hat{a}$, $f_3=1/7(3+(\varepsilon+\varepsilon^2+\epsilon^4)\theta_a+(\varepsilon^3+\varepsilon^5+\varepsilon^6)\theta_a{}^3)$

$f_4=1/7(3+(\varepsilon 3+\varepsilon 5+\varepsilon 6)\theta_a+(\varepsilon+\varepsilon^2+\varepsilon^4)\theta^3$, here θ is a primitive 7^{th} root of unity.

We can also show that, $F[G] \cong F_2 \oplus F_4 \oplus M_3[F_2] \oplus M_3[F_2]$. If we choose $e_1=1+\hat{a}$, which is not a central primitive idempotent, and calculate,

$F= (\hat{b}+\hat{b}a(1+\hat{b}))e_1 = (\hat{b}+\hat{b}a(1+\hat{b}))(1+\hat{a})$

$=1+b+b^2+a+a^2b+a^4b+a+ab+ab^2+a^2b+a^2b^2+a^2+a^4b^2+a^4+a^4b+\hat{G}$

Thus the weight of f as w(f)=12 as well as weight distribution of this ideal will be,

Weight	0	8	12
Word	1	21	42

It is clear that the code [21, 6, 8] has same weight as in code [21, 6]

[2]. Let us choose another dihedral group of order 6:

D_6= {a, b|$a^3=1=b^2$, bab=a^2}.

Let us suppose that F_q be a finite field with q elements such that $U(Z_3) =<\bar{q}>$ Thus from [11, theorem 3.3], central primitive idempotent of $F_q[D_6]$ will be,

$e_{11}=(1+b/2)\hat{A}$, $e_{22}=(1-b/2)\hat{A}$, $e_1=1-e_{11}-e_{22}$, as well as we write $f=e_{11}-e_{22}$ and the we will put $I=F_qD_6.f$. Since it is clear that |I|=2, and set {f, af} will be the basis over F_q, and an element $\alpha \in F_qD_6$ .f will be represented as $\alpha = \boldsymbol{\alpha_0}\mathbf{f}+\alpha_1 af=1/12[4\,\boldsymbol{\alpha_0} + \alpha_1)\mathbf{1} +(-5\,\boldsymbol{\alpha_0} +4\,\alpha_1)a+(\,\boldsymbol{\alpha_0} -5\,\alpha_1\,)a^2 + (4\,\boldsymbol{\alpha_0} -5\,\alpha_1)b+(\,\boldsymbol{\alpha_0} +4\,\alpha_1)ab+(-5\,\boldsymbol{\alpha_0} + \alpha_1)a^2b]$. If q=11, is a direct calculation then w(I)=5 is the weight of code [6,2] from [27]. When we have any field of characteristic different from 2, 3, 5, and 7 then such above condition also holds good.

Matrix algebra for idempotent as well as left ideals in the formation code:

It is very important to represent coding theory in matrix algebra. For this purpose we to convert the idempotent and ideals into matrix algebra. Matrix algebra is the building blocks of finite semi-simple group algebra over finite field. This can be required as follow,

Let us suppose that Y(n, k) be the set all matrices $D=(b_{ij}\}$ such that there exist k rows, at positions presented as $i_1, i_2, i_3, i_4, \ldots\ldots\ldots\ldots, i_k$ such that

(1) Every row of D, except these which is row of zeros.
(2) $b_{ij,ij}=1$ as well as $b_{ij,\,h}=0$ if $h<i_j$, $1 \leq j \leq k$.
(3) b_{ij}, h=0 for $h=i_s$, $j+1 \leq s \leq k$.
As the set of numbers $i_1, i_2, i_3, \ldots\ldots..,i_k$ will be called the pivotal position of D.
Now we try to produce an example, let Y(4, 3) be the set all matrices then its all forms will be presented as,

$$\begin{pmatrix} 1 & 0 & 0 & a_{14} \\ & 1 & 0 & a_{24} \\ & & 1 & a_{34} \\ & & & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & a_{13} & 0 \\ & 1 & a_{23} & 0 \\ & & 0 & 0 \\ & & & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & a_{12} & 0 & 0 \\ & 0 & 0 & 0 \\ & & 1 & 0 \\ & & & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ & 1 & 0 & 0 \\ & & 1 & 0 \\ & & & 1. \end{pmatrix}$$

Thus, each left ideal of rank k has $q^{(n-k)k}$ different idempotent generators. Or the elements of the set Y(n, k) are idempotent generators of the different left ideals of rank k of $M_n[F_q]$[30].

References

[1] Thompson T.M., From error –correcting codes sphere packing to simple groups, Carus Mathematical Monographs 21, Mathematical Association of America, Washigton,1983.

[2] Shannon C.E.,"A mathematical theory of communication", Bell System Tech. j. 27 (1948), 379-423.

[3] Sabin R.E. and Lomonaco S.J., Metacyclic Error-correcting Codes", Appl. Algebra Energy. Comm. comput. 6 (1995), No. 3, 191-210.

[4] [1. Arora S.k., Pruthi M., "Minimal cyclic codes of length $2p^n$", Fields APPL. 5 (1999), No. 2, 177-187.

[5] Sabin R. E., "On determining all the codes in semi-simple group rings".in Lecture Notrs in Comput. Sci. Springer (1993), 279-290.

[6] Ferraz R., Polcino Milies C. and Taufer E., "Left ideals in matrix rings over finite field," preprint, arXiv:1711.09289.

[7] Pruthi M. and Arora S.K. , "Minimal codes of prime length", Finite Fields Appl. 3 (1997), No. 2, 99-113.

[8] Berlekamp E.R., Key papers in the development of coding theory, I.E.E.E. Press, New York, 1974.

[9] Prange E., Cyclic error-correcting codes in two symbols, AFCRC-TN-57-103, USAF, Cambridge Research Laboratories, New York, 1957.

[10] Berman S.D., "On the theory of group codes", Kibernetika 3 (1967), No. 1, 31-39.

[11] Poli A., "Codes dans les algebras de group abelienes (codes semisimple, et codes moduaries)", in Information Theory (Proc. Internat. CNRS Collq., Cachan 1977) Colloq. Internat. CNRS 276 (1978), 261-271.

[12] Berman S.D. "Semisimple cyclic and abelian codes 2", Kibernetika 3(1967), No. 3, 17-23.
[13] Polcino Milies C. and Sehgal S.K., An introduction to group rings, Algebras and Applications, Kluwer Academic Publishers, Dortrecht, 2002.
[14] Bernhardt F., Landrock P. and Manz O., "The extended Goly codes considered as ideals", J. Combin. Theory Ser. A 55 (1990), No. 2, 235-246.
[15] Polcino Milies C. and de Melo F., "On Cyclic and Abelian codes", IEEE Trans. Inform. Theory 59 (2013), No. 11, 7314-7319.
[16] Chalom G., Ferraz R. and Polcino Milies C.," Essential idempotents and simplex codes".J.Algebra Comb. Discrete struct. Appl. 4 (2017), No. 2, 181-188.
[17] MacWiliams F.J., "Binary codes which are ideals in group algebra of an abelian group",Bell System Tech. J.49 (1970),987-1011.
[18] Charpin P., "The Reed-Solomon code as ideals in a modular algebra", C.R. Acad. Sci. Paris, Ser. I. Math. 294 (1982), 597-600.
[19] Landrock P. and Manz O., " Classical codes as ideals in group algebras", Des. Codes Cryptogr. 2 (1992), No. 3, 273-285.
[20] Dougherty S., Gildea J., Taylor R. and Tylyshchak A., "Group rings, G-codes and constructions of self-dual and formally self-dual codes", Des. Codes Cryptogr. 86 (2018). No. 9, 2115-2138.
[21] Keralev A. and Sole P.,"Error-correcting codes as ideals in group rings", in Contemporarry Math. 273, Amer. Math. Soc. (2001), 11-18.
[22] Drensky V. and Lakatos P., "Monomial ideals, group algebras and error correcting codes", in Lect. Note in Compute. Sci. 257, Springer, Berlin (1989), 181-188.
[23] Hamming R.W., Interview, February 1977.
[24] Dutra F.S.Ferraz R.A., Polcino Milies C.," Semisimple group codes and dihedral codes", Algebra Discrete Math. (2009),No. 3, 28-48.
[25] Hamming R.W. "Error-detecting and error-correcting codes", Bell System Tech. J. 29(1950), 147-160.
[26] Ferraz R., Guerreiro M. and Polcino Milies C., "G-equivalence in group algebras and minimal abelian codes", IEEE Trans. on Inform. Theory 60 (2014), No. 1, 252-260.
[27] Grassl M., Bounds on the minimum distance linear codes and quantum codes. Online available at htt://www.codetables.de/BKLC/index.html [21 December 2018]
[28] Ferraz R., Polcino Milies C.,"Idempotents in group algebras and minimal abelian codes", Finite Fields Appl. 13 (2007), No.2, 382-393.
[29] Garcia Pillado C., Gonzalez S., Martinez C., Markov V. and Nechaev A.,"Group codes over non-abelian groups", J. Algebra Appl. 12(2013), No. 7, 20 pp.
[30] Ferraz R., Polcino Milies C., and Tufer E., "Left ideals in matrix rings over finite fields",preprint, arXiv:1711.09289.