Bijective Equivalence mapping from $F_2[D_{2n}]$-Code to $F_2[C_{2n}]$-Code for integer n=3,4,5,…,n

[1]Dr.N.K.Agrawal, Professor
[2]Dhananjay Kumar Mishra
[3]Ram Naresh Das
Math. Dept. L.N.M.U. Darbhanga

Abstract

A group ring code is a kind of code which is made up of group ring structure. Every group ring code over a dihedral group for given sub-module becomes equivalent to some of group ring code over cyclic group for a given suitable other sub-module for integer n=3, 4, 5,…,n. But an $F_2[C_4]$-code cannot be an $F_2[D_4]$-code. Every cyclic code has spanning set. Due to this reason every dihedral group ring code is equivalent to some of cyclic group ring code up to adjustable permutations. Thus it is a bijective equivalent mapping, this means there is a bijective mapping from $F_2[D_{2n}]$-codes to $F_2[C_{2n}]$-code. If f_u be the require mapping, and hence $f_u(C_{D_{2n}}(z, N)) \rightarrow C_{C_{2n}}(z, M)$ for n=3,4,5,….,n. Such type of coding concept is utilized in communication areas to transmit information and to maintain secrecy.

Keywords: Group rings, cyclic group, dihedral group, group ring codes, bijective mapping, spanning set, sub-module.

1. INTRODUCTION

Let us suppose that G be a finite group and R be a ring. Then a group ring R[G] is a set of all collection of linear combination as, R[G]={ $\sum_{g \in G} a_g$|a_g∈R}. It has a ring structure as well as a free module structure. When we construct a code with the help of group ring structure R[G] then it is termed as a group ring code. We have observed that a famous code G_{24} is a group ring code over dihedral group D_{24} as well as a group ring code over a cyclic group C_{24}.Based on a condition, it is found that each binary group ring code over a dihedral group becomes equivalent to binary group ring code over a cyclic group. In this research paper we have taken a binary group ring codes which is also denoted as $F_2[G]$-code. Here F_2 is a finite field of order 2 and G is a group. Let us suppose that W be a sub-module of $F_2[G]$ and z ∈$F_2[G]$.Then a mapping f_u: W→$F_2[G]$ such that $f_z(x)$=zx is termed as group ring coding function which is given by Hyrley,2009. The image f_z will be denoted by $C_G(z, W)$ and will be called $F_2[G]$-code with generator z relative to the sub-module W. Thus we have $C_G(z, W)$ is a set as {zx|x∈W}.

2. A BRIEF HISTORY

In 1967 first of all group ring codes were discussed by Berman. He associated every cyclic code to a group algebra R[G] over a cyclic group as well as every Reed-Muller code to a group algebra R[G] over an elementary abelian 2-group. After that Mac William in 1969 had worked on the class of codes which are associated to group rings R[G] over dihedral groups. In 1983 Charpin found that every extended Reed-Solomon code can be taken as an ideal of some modular group algebras. In 1992 Landrock and Manz as well as in 2008 Mc-Loughlin and Hurley had shown the extended Golay code, as to be group ring codes. In 2000, Hughes had defined a group ring code as an ideal in a group ring. Fu and Feng. 2009; Jitman et al.,2010; Wong and Ang,2013; Hurley, 2014 had studied on group ring codes, such as self-orthogonal group ring codes, checkable group ring codes. In 2006 Hurley invented the isomorphism between a group ring and a ring of matrices. He by doing so upgrades the encoding method of group ring for codes in 2009. The group ring codes which were found by Hurley are of two types. **(1).** Sub-modules of their corresponding group rings **(2).** Ideals of given group rings. In this paper we have discussed on group ring encoding method which was suggested by Hurley. In 2008, Mc-Loughlin and Hurley in a paper had shown, the extended binary Golay code G_{24} as a group ring code over the dihedral group D_{24}. But in this paper we have found that the famous code G_{24} can be regarded as a group ring codes in two ways. (a). Golay code G_{24} is a group ring codes over a dihedral group D_{24} (b). Golay code G_{24} is a group ring codes over a cyclic group C_{24}. We have found that every binary group ring code over a dihedral group D_6 is equivalent to a binary group ring code over a cyclic group C_8.

3. Some basic definitions used in this paper:

a) If z = $\sum_{g_i \in G} a_{g_i} g_i$ ∈ $F_2[G]$ is the $F_2[G]$-matrix as $[a_{g_{n-1}, g_n}]_{nxn}$. Then the rank of z will be the rank of the $F_2[G]$-matrix for z.

b) Let us suppose that z∈ $F_2[G]$, then the support of z will be defined as the set, supp(b)={g ∈ G|$a_g \neq 0$.

c) The weight of z will be defined as wt(z)= |supp(z)|.

d) If z ∈ $F_2[G]$. Then every element of the form zx ∈ $F_2[G]$, x ∈ G has the same rank as z.

e) Every i^{th} row in $F_2[G]$-matrix of z will be understood with element $g_iz \in F_2[G]$ and the rank of z will be the maximum number of linearly independent elements in $\{g_1z, g_2z, g_3z, \ldots\ldots, g_nz\}$.

f) Let us take $z \in F_2[G]$ and rank(z)=k, then dimension of any $F_2[G]$-code generated by z will be at most up to k, also the dimension of $C_G(z, G)$ will be equal to k.

g) Let us choose Y as a sub-module of $F_2[G]$ and $z \in F_2[G]$. Now a function f_z: Y $\rightarrow F_2[G]$ such that $f_z(x)$=z x is termed as a group ring encoding function. The mapping of $\mathbf{f_z}$ will be denoted as $C_G(b, Y)$ is known as $F_2[G]$-code with generator b with respect to the sub-module Y. Hence we can say that $C_G(z, Y)$ will the set $\{zx|x \in Y\}$.

4. Important results related to this paper:

(a) **Group ring over a cyclic group C_n:** Group ring codes over a cyclic group are important, because they are easy to use for efficient error detection and correction. Let us suppose that there be a cyclic group $C_n = \{g|g^n=1\}$, and consider a shift mapping φ $(a_1, a_2, a_3, \ldots\ldots\ldots, a_n)=a_n, a_1, a_2, \ldots\ldots\ldots, a_{n-1}$ is also termed as shift cyclic mapping. **Definition:** Let there be a set $\{p_1, p_2, p_3, \ldots\ldots, p_k\} \subseteq F_2^m$ is called a shift set if each $p_i= \varphi_i^m(p_1)$for some positive integer m_i.

4(a).Proposition: Let us suppose that $G=\{g_1, g_2, \ldots.., g_n\}$, then $F_2[G]$-code is equivalent to a binary group ring code over a cyclic group of order n if only if the associated linear code has spanning set that is equivalent to a shift set. Proof: Let us suppose that $C_n=\{1, g, g^2, \ldots.., g^n\}$ be a cyclic group and $C_G(z, N)$ is $F_2[G]$-code. This is equivalent to group ring code $Cc_m(p, M)$ over a cyclic group C_n. $\overline{pM}$ is linear shift set which span the linear code $\overline{Cc_n(p, M)}$. As we have observed that $\overline{Cg(z, N)}$ is equivalent to $\overline{Ccn(p, M)}$. Thus we can say that the linear code $\bar{C}_G(z, N)$ has the spanning set equivalent to $\overline{pM}$. Let us suppose that $C_G(z, N)$ be an $F_2[G]$-code and $\overline{C_G(z, N)}$ is a spanning set which will be equivalent to a shift set $\bar{S}$ = $\{\overline{p_1}, \overline{p_2}, \ldots\ldots.., \overline{p_k}\}$ here each $\overline{p_1}$ = $a_1a_2\ldots\ldots a_n$ and we have for some positive integers m_i there exist $\overline{p_l}$ $=\pi^{m_i}(\overline{p_1})$.The set $\bar{S}$ can be regarded as the sets$\{p_1, p_2, \ldots\ldots\ldots.., p_k\}$ here each p_1= $a_1+a_2g+\ldots\ldots\ldots+a_ng^{n-1}$ $p_i = p_1g^{m_i}$, this spans the $F_2[C_n]$-code. Thus, we have seen that $C_G(z, N)$ is equivalent to a binary cyclic group ring code.

4(b).Proposition: Let $b \in F_2[G]$ and $x \in G$, for an arbitrary $N \subseteq G$ such that $C_G(zx, N')$ $=C_G(z, N)$. Then the code $C_G(zx, G)$ is same as the code $C_G(z, G)$. Proof: Let us take a set N= $\{g_{k_1}, g_{k_2}, \ldots\ldots\ldots, g_{k_t}\} \subseteq G$. Then the code over group G regarding field F_2, will be as $C_G(z, N)$= $\Gamma_{F_2}\{zg_{k_1}, zg_{k_2}, \ldots\ldots\ldots, zg_{k_t}\}$. Now for each i = 1, 2, 3,..,t there will be unique $g_{h_i} = g_{k_i}$. Therefore, $C_G(z, N)$ $=\Gamma_{F_2}\{z(xg_{h_1}), z(xg_{h_2}), \ldots\ldots\ldots, z(xg_{h_t})\}$ $=\Gamma_{F_2}\{zx(g_{h_1}), zx(g_{h_2}), \ldots\ldots, zx(g_{h_t})\}$ $= C_G(zx, N')$, here N'=$\{g_{h_1}, g_{h_2}, \ldots\ldots\ldots, g_{h_t}\} \subseteq$ G. Similarly we have, $C_G(zx, G)$= $\Gamma_{F_2}\{z(xg_1), z(xg_2), \ldots\ldots, z(xg_n)\}$= $\Gamma_{F_2}\{zg_1, zg_2, \ldots\ldots, zg_n\}$=$C_G(z, G)$.

4(c). Proposition: Let us suppose that $b \in F_2$and $x \in$ G. Now we choose any arbitrary $N \subseteq G$, such that there exists $N' \subseteq G$ so that we have $C_G(zx, N')$ $=C_G(z, G)$.

Proof: Let us take N= $\{g_{k_1,}\ g_{k_2}, \ldots\ldots\ldots\ g_{k_t}\}$ then code so formed will be, $C_G(z, N)$=$\Gamma_{F_2}(zg_{k_1}, zg_{k_2,}, \ldots\ldots.., zg_{k_t}\}$.

Thus for each i=1, 2, 3…t, there exists unique $zg_{h_i} = g_{k_i}$ Therefore, we have, $C_G(z, N) = \Gamma_{F_2}\{z(xg_{h_1}), z\left(xg_{h_2}\right), z(xg_{h_3}), \ldots\ldots, z(xg_{h_t})\}.=$ $\Gamma_{F_2}\{zx(g_{h_1}), \ldots, zx(g_{h_t})\}$=$C_G(zx, N')$. Here, N'= $\{g_{h_1}, g_{h_2}, \ldots\ldots, g_{h_t}\} \subseteq G$. Similarly we have,$C_G(\Gamma_{F_2}(z(xg_1)$, $z(xg_2)$, ….,$z(xg_n$))=$C_G(z, G)$.

5. Discussion on the relation between the group ring codes over dihedral groups D_{2n} as well as the group rings codes over cyclic groups C_{2n}:

Let us suppose that D_{2n} be a dihedral group and C_{2n} be a cyclic group of order 2 as D_{2n}= $\{a, b|a^n=b^2=1, ba=a^{-1}b\}$and C_{2n}=$\{g|g^{2n}=1\}$. In this paper we take the listing of D_{2n} as $\{1,a,a^2,\ldots.,a^{n-1},b,ba,ba^2,\ldots.,ba^{n-1}\}$ and the listing of C_{2n} as $\{1,g,g^2,g^3,\ldots\ldots..,g^{2n-1}\}$.

Our main aim in this paper is for $F_2[D_{2n}]$-code $C_{D_{2n}}(q, N)$, to find suitable $p \in F_2[C_{2n}]$ such that the $F_2[C_{2n}]$-code $C_{C_{2n}}(p, M)$ become equivalent to $C_{D_{2n}}(q, N)$. As we have found that an F_2D_{2n}-code $C_{D_{2n}}(q, M)$ is equivalent to an F_2C_{2n}-code if there exists a permutation of such type that the set $\overline{qN}$ is a shift set.

There is a requirement of a technical result to proceed further in this paper. We fix an element $z = \sum_{i=0}^{n-1} \alpha_i a^i + \beta_i ba^i \in F_2[D_{2n}]$, as well as N=$\{a^{i_1}, a^{i_2}, \ldots., a^{i_l}, ba^{j_1}, ba^{j_2}, \ldots.., ba^{j_k}\}$.Let us suppose that z'=$\sum_{i=0}^{n-1} \alpha_i a^i$+$(\beta_i ba^i)a^t$ and N'=$\{a^{i_1}, a^{i_2}, \ldots.., a^{i_l}, ba^{j_1+t}, ba^{j_2+t}, \ldots., ba^{j_k+t}\}$ for some integer t. We will do permutation on coordinates that will fix $i \in \{1,2,3,\ldots,n\}$ and we will map n+k→n+(t+k)mod n for $k \in \{1,2,3,\ldots n\}$. Now we have,

$$\begin{pmatrix} 1 & 2\ldots..n & n+1 & n+2 & \ldots\ldots.2n \\ 1 & 2\ \ldots.n & n+(t+1)\bmod n & n+(t+2)\bmod n\ldots & n+(t+n)\bmod n \end{pmatrix}$$

As we observe that the linear code $\overline{C_{D_{2n}}(z', N')}$ is same that of $\overline{C_{D_{2n}}(z, N)}$.Thus it is clear that, $C_{D_{2n}}(z', N')$ will be equivalent to code $C_{D_{2n}}(z, N)$.

5(a) Let us suppose that z=$\sum_{i=0}^{n-1} \alpha_i a^i + \beta_i ba^i \in F_2[D_{2n}]$ and z'=$\sum_{i=0}^{n-1} \alpha_i a^i + (\beta_i ba^i)a^t$ for some integers t. Then we have, (1). Every group ring code which is generated by z' will be equivalent to some group ring code generated by z. (2). Every group ring code generated by z'x here $x \in D_{2n}$ will be equivalent to some group ring codes, which are generated by z.

6. Equivalence between $F_2[D_{2n}]$ and $F_2[C_{2n}]$ for n=3, 4:

If we take group ring code $C_{D_{2n}}(z, N)$ of $F_2[D_{2n}]$ which has z as an element with wt(z)=w as well as rank(z)=k and try to make it equivalent to $F_2[C_{2n}]$. So we choose an element $p \in F_2[C_{2n}]$ such that the wt(p)=w and rank of p equal to or greater than k, then $C_{D_{2n}}(z, N)$ will be equivalent to $C_{C_{2n}}(p, M)$ as $N \subseteq D_{2n}$ and $M \subseteq C_{2n}$.

Let us take two elements b and p of $F_2[D_6]$ as well as $F_2[C_6]$ respectively. Let us choose z=1+a+b+ba of rank 2 while $p=1+g+g^2+g^4$ of rank 5. Then code $C_{D_6}(1 + a + b + ba, \{1, a\})$ $=\Gamma_{F_2}(1 + a + b + ba, a + a^2 + ba + ba^2)$ can be regarded as code $\Gamma_{F_2}(110110,011011)$. While the code $C_{C_6}(1 + g + g^2 + g^4,\{1,g\})=\Gamma_{F_2}$ $(1+g+g^2+g^4, g+g^2+g^3+g^5)$ will be regarded as Γ_{F_2} (111010,011101}. Thus we can show that above two codes can be made equivalent by making permutation of digits.

Let the elements $1+a+a^2+b \in F_2[D_6]$ and $1+g \in F_2[C_6]$ are of rank 5 but different weight. It can be shown that codes from both group rings can be made equivalent with all F_2^6 elements of even weight.

6(a). Dihedral code over field F_2 ($F_2[D_6]$-code) versus cyclic code over field F_2 ($F_2[C_6]$-code):

We will do partition of $F_2[D_6]$. We will use the proposition 4(c) and 4(d) for a fixed $z \in F_2[D_6]$, we collect all the elements z' of $F_2[D_6]$, such that every group ring code generated by z' will be equivalent to a code generated by z. It will be denoted by a set A_u. Therefore the set $A_u = \{[\sum_{i=0}^{2} \alpha_i a^i + \beta_i (ba^i)a^t]x | t \in \{0,1,2\}, x \in D_6\}$. Then we have partition $P = \{A_u | z \in U\}$, where $U = \{0,1,1+a, 1+b, 1+a+b, 1+a+a^2, 1+a+a^2+b, 1+a+b+ba, 1+a+a^2+b+ba, 1+a+a^2+b+ba+ba^2\}$ is all elements of each component in partition P. Here every non-zero element $z \in U$ has 1 in their support.

6(b).Table of Partition P of $F_2[D_6]$

$z \in F_2[D_6]$	A_u	$\lvert A_u \rvert$
0	$\{0\}$	1
1	$\{x \mid x \in D_6\}$	6
1+a	$\{(1+a)x \mid x \in D_6\}$	6
1+b	$\{(1+b)x,(1+ba)x,(1+ba^2)x \mid x=1,a,a^2\}$	9
1+a+b	$\{(1+a+b)x,(1+a+ba)x,(1+a+ba^2)x \mid x\ D_6\}$	18
$1+a+a^2$	$\{(1+a+a^2)x \mid x=1,b\}$	2
$1+a+a^2+b$	$\{(1+a+a^2+b)x \mid x \in D_6\}$	6
1+a+b+ba	$\{1+a+b+ba)x,(1+a+ba+ba^2)x,(1+a+b+ba^2)x \mid x=1,a.a^2\}$	9
$1+a+a^2+b+ba$	$\{(1+a+a^2+b+ba)x \mid x \in D_6\}$	6
$1+a+a^2+b+ba+ba^2$	$\{1+a+a^2+b+ba+ba^2\}$	1

64

Since, every code which is generated by an element in A_u is equivalent to some code that is generated by z. So we will have to prove that every $F_2[D_6]$-code generated by $z \in U/\{0\}$ will be equivalent to some $F_2[C_6]$-code. Therefore we have to put focus on those codes whose generator will be $z \in U/\{0\}$ and which are starting from this point.

Categorisation of all the elements u of U/ {0} according to their weight as well as rank.

6(c). Categorisation Table of Elements in U

Wt.	$z \in U\backslash\{0\}$	Rank
1	1	6
2	1+a	4
2	1+b	3
3	1+a+b	4
3	$1+a+b^2$	2
4	$1+a+a^2+b$	5
4	1+a+b+ba	2
5	$1+a+a^2+b+ba$	6
6	$1+a+a^2+b+ba+ba^2$	1

Now, we choose $z \in F_2[D_6]$ such that $p_z \in F_2[C_6]$, such that every group ring code with generator with generator z is equivalent to some other group ring code generated by p_z.

6(d). Comparison Table between $U \in F_2[D_6]$ and $V_u \in F_2[C_6]$ with Respect to Weight and Rank:

Wt	$z \in F_2[D_6]$	$P_z \in F_2[C_6]$	Rank
1	1	1	6
2	1+a	$1+g^2$	4
2	1+b	$1+g^3$	3
3	1+a+b	$1+g+g^2$	4
3	$1+a+a^2$	$1+g^2+g^4$	2
4	$1+a+a^2+b$	$1+g+g^2+g^4$	5
4	1+a+b+ba	$1+g+g^3+g^4$	2
5	$1+a+a^2+b+ba$	$1+g+g^2+g^3+g^4$	6
6	$1+a+a^2+b+ba+ba^2$	$1+g+g^2+g^3+g^4+g^5$	1

Now, we want to show that every $F_2[D_6]$-code with generator u will be an $F_2[C_6]$-code with generator p_z for equivalence condition. We will produce an example to clear comparison.

Let us suppose that there be an $F_2[D_6]$-codes $C_{D_6}(1+a, N)$ here an arbitrary subset $N \subseteq D_6$. It is noted that wt(1+a)=2 and rank(1+a)=4. From above table 5(c) the element $1+g^2 \in F_2[D_6]$ has same weight and rank as 1+a.

We will remember a code word of the form $\sum_{i=0}^{2} \alpha_i a^i + \beta_i ba^i \in F_2[D_6]$ can traced as the binary code word $\alpha_0, \alpha_1, \alpha_2, \beta_0, \beta_1, \beta_2$ while the coed word of the form $\sum_{i=0}^{5} \omega_i g^i \in F_2[C_6]$ can traced as the binary code word $\omega_0, \omega_1, \omega_2, \omega_3, \omega_4, \omega_5$. Again we have a spanning set (1+a, N) of code $C_{D_6}(1+a, N)$ which similar to that of the cyclic code $C_{C_6}(1+g^2, M)$ with spanning set $(1+g^2)$ M Now we can choose M such that $C_{D_6}(1+a, N)$ and $C_{C_6}(1+g^{2,}, M)$ are equivalent.

6(e).Table for Binary Representation of $(1+a)D_6$ as well as $(1+g^2)C_6$:

$x \in D_6$	$(1+a)x$	$\overline{(1+a)x}$	$y \in C_6$	$(1+g^2)y$	$\overline{1+g^2)}$
1	1+a	110000	1	$1+g^2$	101000
a	$a+a^2$	011000	g^2	g^2+g^4	001010
a^2	$1+a^2$	101000	g^4	$1+g^4$	100010
b	$b+ba^2$	000101	g^5	$g+g^5$	010001
ba	b+ba	000101	g	$g+g^3$	010100
ba^2	$ba+ba^2$	000011	g^3	g^3+g^5	000101

As we know that the permutation group $\begin{pmatrix} 123456 \\ 135242 \end{pmatrix}$ can be written as (2354) also this shows that the two sets of binary code words are same.

Because these binary codes are same. Thus by permutation we can say that for every N subset of D_6, we can easily find a sub set M of C_6 such that $C_{D_6}(1+a, N)$ is equivalent to $C_{C_6}(1+g^2, M)$.

We can easily explain it by an example as, let us suppose that f be a bijective mapping. Then f(1)=1, f(a)= g^2 , f(a^2)= g^4, f(b)=g^5, f(ba)=g, f(ba^2)=g^3 . Thus we can say that, f(N)=M. Now we will show permutation arrangement of each element in $F_2[D_6]$ to the corresponding element of $F_2[C_6]$. Through this table we will be able to know that every element of $F_2]D_6]$ that is u∈ U/{0} will be written as equivalent to every corresponding element of p_z∈ $F_2[C_6]$, such that 1∈supp(p_z), wt(p_z)=wt(z), and rank(p_z)=rank(z).

6(f). Permutation Table from $C_{D_6}(z, D_6)$ to $C_{C_6}(p_{z,} C_6)$:

z∈U/{0}∈$F_2[C_6]$	P_z∈$F_2[C_6]$	Permutations
1	1	(2354)
1+a	$1+g^2$	(2354)
1+b	$1+g^3$	(2356)
$1+a+a^2$	$1+g^2+g^4$	(2354)
1+a+b	$1+g+g^2$	(2354)
$1+a+a^2+b$	$1+g+g^2+g^4$	(2354)
1+a+b+ba	$1+g^2+g^3+g^5$	(2354)
$1+a+a^2+b+ba$	1+g+g2+g3+g4	(2354)
$1+a+a^2+b+ba+ba^2$	$1+g+g^2+g^3+g^4+g^5$	(2354)

7. Theorem: every $F_2[D_6]$-Code is a $F_2[C_6]$-Code is Equivalent under Permutation:

Proof: Let us suppose that u' be a non-zero element of $F_2[D_6]$ and N' be a non-empty set of D_6. So the code formed $F_2[D_6]$-code as $C_{D_6}(z', N')$.The element z'∈A_u for some z∈ U/{0}. Therefore, from preposition 4(a) & 4(b) we have $C_{D_6}(z', N')$ is equivalent to some $F_2[C_6]$-code $C_{C_6}(z, N)$ for some N⊂D_6. Since $C_{D_6}(z, N)$ is equivalent to some $F_2[C_6]$-code $C_{C_6}(p, M)$. By transitivity the code $C_{D_6}(z', N')$ is equivalent to some $F_2[C_6]$-code $C_{C_6}(p, M)$.

8. $F_2[D_6]$-code versus $F_2[C_6]$-code:

Let us choose a dihedral group of order 8 as D_8= {a,b|a^4=b^2=1, ba=a^{-1}b} and cyclic group of order 8 will be written as, C_8 ={g|g^8=1}.

Just like in $F_2[D_6]$-code we have, for fixed z=$\sum_{i=0}^{3} \alpha_i a^i + \beta_i ba^i \in F_2[D_8]$, we will group all elements z' in $F_2[D_8]$ such that every group ring code generated by z' will be equivalent to a code generated by z into a set denoted by A_z= {$[\sum_{i=0}^{3} \alpha_i a^i + \beta_i (ba^i) a^t x | t \in \{0,1,2,3), x \in D_8$ }. Let us suppose that there be a set P= {A_u |z∈ U} which makes a partition of $F_2[D_8]$. Here, U= {0, 1, 1+a, $1+a^2$, 1+b, $1+a+a^2$, $1+a^2+b$, 1+a+b, $1+a+a^2+a^3$, $1+a+a^2+b$, $1+a^2+b+ba^2$, 1+a+b+ba, $1+a+b+ba^2$, $1+a+a^2+a^3+b$, $1+a+a^2+b+ba^2$, $1+a+a^2+b+ba+ba^2$, $1+a+a^2+a^3+b+ba+ba^2$, $1+a+a^2+a^3+b+ba+ba^2+ba^3$}, it is noted that every element z∈U is the representative element of each component in partition set P.

9. Partition Set P of $F_2[D_8]$

z∈$F_2[D_8]$	**A_z**	**|A_z|**
0	{0}	1
1	{x|x∈D_8}	8
1+a	{(1+a)x|x∈D_8	8
$1+a^2$	{$(1+a^2)$x|x=1,a,b,ba}	4
1+b	{$(1+ba^i)$x|i∈{0,1,2,3},x=1,a,a^2,a^3}	16
$1+a+a^2$	{$(1+a+a^2)$x|x∈D_6}	8
$1+a^2+b$	{$(1+a2+ba^i)$x|i∈{0,1,2,3},x=1,a,b,ba}	16
1+a+b	{$(1+a+ba^i)$x|i∈{0,1,2,3},x∈D_8}	32
$1+a+a^2+a^3$	{$(1+a+a^2+a^3)$x|x=1,b}	2
$1+a+a^2+b$	{$(1+a+a^2+ba^i)$x|i∈{0,1,2,3},x∈D_8}	32
$1+a^2+b+ba^2$	{$[1+a2+(b+ba2)a^i]$x|i∈(0,1),x=1,a}	4
1+a+b+ba	{$[1+a+(b+ba)a^i]$x|i∈{0,1,2,3},x=1,a,a^2,a^3}	16
$1+a+b+ba^2$	{$[1+a+(b+ba^2)ai]$x|i∈{0,1},x∈D_8}	16
$1+a+a^2+a^3+b$	{$(1+a+a^2+a^3+ba^i)$x|i∈{0,1,2,3},x=1,b}	8
$1+a+a^2+b+ba$	{$[1+a+a^2+(b+ba^2)a^i]$x|i∈{0,1},x∈D_8}	16
$1+a+a^2+a^3+b+ba$	{$[1+a+a^2+(b+ba)a^i]$x|i∈{0,1,2,3},x∈D_8}	32
$1+a+a^2+a^3+b+ba^2$	{$[1+a+a^2+a^3+(b+ba)a_i]$x|i∈{0,1,2,3},x=1,b}	8
$1+a+a^2+b+ba+ba^2$	{$[1+a+a^2+(b+ba^2)a_i]]$x|i∈(0,1),x=1,b}	4
$1+a+a^2+a^3+b+ba+ba^2$	{$[1+a+a^2+(b+ba+ba^2)a_i]$x|i∈{0,1,2,3},x=1,a,a^2,a^3	16
$1+a+a^2+a^3+b+ba+ba^2+ba^3$	{$(1+a+a^2+a^3+b+ba+ba^2)$x|x∈D_8	8
$1+a+a^2+a^3+b+ba+ba^2+ba^3$	{$1+a+a^2+a^3+b+ba+ba^2+ba^3$}	1
		256

Now we categorize all the elements z∈ U/{0} according to their weight and rank. Now we choose p_z ∈ $F_2[C_8]$ such that

1∈supp(vu), wt(z)=wt(p_z), as well as rank(p_z)=rank(z). Under bijective mapping we seek for all non-zero z∈U except z=1+a+a^2+b there exist elements p_z∈ $F_2[C_8]$. Now we find the permutations that send $C_{D_8}(z, D_8)$ to $C_{C_8}(p_{z,} C_8)$, except z=1+a+a^2+b.

10. Table for Permutations that Sends $C_{D_8}(z, D_8)$ to $C_{C_8}(p_{z,} C_8)$

Wt.	z∈$F_2[D_8]$	P_z∈$F_2[C_8]$	Rank	Permutation on coordinates
1	1	1	8	(235)(476)
2	1+a	1+g^2	6	(235)(476)
2	1+a^2	1+g^4	4	(235)(476)
2	1+b	1+g^4	4	e
3	1+a+a^2	1+g^2+g^4	8	(235)(476)
3	1+a^2+b	1+g^2+g^4	8	(235)(476)
3	1+a+b	1+g+g^2	8	(235)(476)
4	1+a+a2+a3	1+g^2+g^4+g^6	2	(235)(476)
4	1+a2+b+ba2	1+g^2+g^4+g^6	2	e
4	1+a+b+ba	1+g+g^4+g^5	3	e
4	1+a+a^2+a^3+b	1+g^2+g+g^5	6	(235)(476)
5	1+a+a2+a3+b	1+g^2+g^4+g^6+g	8	(235)(476)
5	1+a+a2+b+ba2	1+g^2+g^4+g^6+g	8	e
5	1+a+a2+b+ba	1+g^2+g^4+g+g^3	8	(235)(476)
5	1+a+a2+b+ba	1+g^2+g^4+g+g^3	8	(235)(476)
6	1+a+a2+a3+b+ba	1+g^2+g^4+g^6+g+g^3	6	(235)(476)
6	1+a+a2+a3+b+ba2	1+g^2+g^4+g^6+g+g^5	4	(235)(476)
6	1+a+a2+b+ba+ba2	1+g^2+g^4+g^6+g+g^5	4	e
7	1+a+a^2+a^3+b+ba+ba^2	1+g^2+g^4+g^6+g+g^3+g^5	8	(235)(476)
8	1+a+a^2+a^3+b+ba+ba^2+ba^3	1+g^2+g^4+g^6+g+g^3+g^5+g^7	1	(235)(476)

Now we will discuss on the exceptional case, when the $F_2[D_8]$-codes which has generator in A_w here w=1+a+a^2+b. Let us consider a code $C_{D_8}(w, N')$ of dimension k. If |N'|>k, then there exists a subset N⊂N' with |N|=k such that wN is linearly independent and span the same code as wN', that is $C_{D_8}(w, N)$=$C_{D_8}(w, N')$. Thus we will say that with |N|=k and wN as basis for code $C_{D_8}(w, N)$ has dimension k with generator w. Since w is of rank 4 then the dimension of $F_2[D_8]$-codes with generator w will be at most 4 (Hurley, 2009).

11. Dimensions of $F_2[D_8]$-Code:

(a).When dimension of $F_2[D_8]$-code is 4:

The code of the largest size in $F_2[D_8]$ is of dimension 4 which is generated by w is $C_{D_8}(w, D_8)$. Any 4 linearly independent elements in the set wD_8 will be the basis of code $C_{D_8}(w, D_8)$. Hence every code of dimension 4 in F_2 [D_8] will be same as the code $C_{D_8}(w, \{1, a, a^2, a^3\}) \underline{= Ʊ_{F_2}\{w, wa, wa^2, wa^3\}}$ which will be recognized with code$\overline{C_{D_8}(w, \{1, a, a^2, a^3\})}$_=$Ʊ_{F_2}(S)$ here, S={$\underline{1110100,01110100}$,10110010,11010001}. It is noted that$\overline{C_{D_8}(w, \{1, a, a^2, a^3\}}$ will be equivalent to the code C=C_{F_2}\{11101000,00111010,10001110,10100011\} which can be denoted as the code $C_{C_8}(1 + g + g^2 + g^4, \{1, g^2, g^4, g^6\})$.

(b). When dimension of F_2 [D_8]-code is 3:

Les us suppose that N={x, y, z} ⊂ D_8 and wN is linearly independent. Very first we find the number of $F_2[D_8]$-codes of dimension 3 with generator w. In next table we describe the support of wx for all x∈D_8. From this table we can show that any three elements in wD_8 are linearly independent and so any three elements in D_8 can form such set N. Thus we will get $\mathbf{C_3^8}$**=56** combinations, which can be obtained from N.

(c).The support of (1+a+a^2+b) x for x∈D_8 Supp (wx):

x∈ D_8	**1**	**a**	**a^2**	**a^3**	**b**	**ba**	**ba^2**	**ba^3**
1	×	×	×		×			
ba^3				×		×	×	×
a		×	×	×		×		
b	×				×		×	×
a^2	×		×	×			×	
ba		×			×	×		×
a^3	×	×		×				×
ba^2			×		×	×	×	

From above table we have observed that |supp (a^i) ∩ supp (ba^{i-1})|=0 for i= {0, 1, 2, 3}. When we take an element z∈ D_8 here z≠ a^i as well as z≠ba^{i-1}then we have,|supp (a^i)⍰supp(z)|=supp(ba^{i-1}∩supp(z)|=2.

Case1: Let us suppose that x, y∈N such that **|supp(wx)∩**

supp(wy)|=0.In this case two elements of N are a^i as well as ba^{i-1} for i={0,1,2,3} and the third element is arbitrary $D_8\setminus\{a^i, bb^{i-1}\}$. There are total 4×6 =24 sets and N lies in this case. So every possible linear code $\overline{C_{D8}(w,N)}$ which are equivalent to C=$Ͳ_{F_2}$(11110000, 00001111, 00111100}, which will be regarded as code C_{C_8}(1+g+g^2+g^3,{1,g^2,g^4}).

Case2: Now we take **|supp (wx)Ո supp (wy)|=2,** As we have observed that from above, $|⍰_{x\in N} supp(wx)| = 1.$ So there will be $\frac{8\times6\times4}{3!}$=32 different sets lying in this case. Hence it is clear that each linear code $\overline{C_{D8}(w,N)}$ that is C=C_{F_2}(11101000,001110010,10001110} will be regarded $F_2[C_8]$-code $C_{C_8}(1+g+g^2+g^4,\{1,g^2,g^4\})$.Thus we can say that every group ring code $F_2[D_8]$ will be equivalent to some of group ring code $F_2[C_8]$-code. Hence there is a bijective mapping from $F_2[D_8]$ to $F_2[C_8]$, when the dimension of this type of group ring is 3.

(d). When dimension of $F_2[D_8]$-code is 2:

Let us suppose that N={x, y}⊂D_8 such that wN will be linearly independent. As in previous case we have |supp (wx) Ո supp (wy)| will be either 0 or 2.

Case-1: If we take |supp (wx) Ո supp (wy)|=0, then will be equivalent to C= $Ͳ_{F_2}$\{11110000, 00001111\}, which is regarded as the code $C_{C_8}(1+g+g^2+g,^3\{1, g^4\})$.

Case-2: If we take |supp (wx) Ո supp (wy)|=2, then $\overline{C_{D8}(w,N)}$ will be equivalent to C=$C_{C_8}(1+g+g^2+g^{3,}\{1,g^2\})$. Thus we have found that every $F_2[D_8]$-code with generator w will be equivalent to some of $F_2[C_8]$-code Therefore, we can say that, there is a bijective mapping from $F_2[D_8]$-code to that of $F_2[C_8]$ –code when code is 2 in such group rings.

12. Conjecture:

every $F_2[D_{2n}]$-code will be equivalent to some of $F_2[C_{2n}]$-code for integer n=3,4,5…n.

13. Generalization:

First of all we have found that every $F_2[D_6]$-code is equivalent to some of $F_2[C_6]$-code. Similarly, we have got that every $F_2[D_8]$-code is equivalent to some of $F_2[D_8]$-code. In similar way, we can obtain that every $F_2[D_{10}]$-code is equivalent to some of $F_2[C_{10}]$-code. Thus, we will generalize that every $F_2[D_{2n}]$-code will be equivalent to some of $F_2[C_{2n}]$-code for integer n=3,4,5…n.

Hence, there is bijective mapping from $F_2[D_{2n}]$ to that of some $F_2[C_{2n}]$.

CONCLUSIONS

We found that every group ring code over a cyclic group has a spanning shift set. Thus under such spanning shift set and by choosing suitable generator and appropriate sub-module up to adjustable permutations, every $F_2[D_{2n}]$-code will be equivalent to some of $F_2[C_{2n}]$-code. But it is not clear whether the converse is true. We have also, there exist an $F_2[C_4]$-code which can never be an $F_2[D_4]$-code. There are some group ring code which are not a group ring code over a cyclic group.

REFERENCES:

[1] Mac-Wiliams. F.J. (1969). Codes and Ideals in Group Algebras. *Combinatorial Mathematics and its Applications*. 312-328.

[2] Jitman, S., Ling, S., Liu, H. and Xie, X. (2010) Chakable Codes from Group Rings. arXiv:1012.5498.

[3] Mc-Loughlin, I.and Hurley, T. (2008). A Group Ring Construction of the Extended Binary Golay Code. *IEEE Transactions in Information Theory*. 54(9): 4381-4383

[4] Wong, Denis C.K.and Ang. M.H. (2013). Group Algebra Codes Defined over Extra Special p-group. *JP Journal of Algebra, Number Theory and Applications.* 78(1): 19-27.

[5] Hurley. T. (2006). Group Rings and Rings of Matrices. *International Journal of Pure and Applied Mathematics*. 31(3):319-335

[6] Hurley. P. and Hurley T.2009. Codes from Zero-divisors and Units in Group Rings. *.Int. J. Information and Coding Theory*. Int 1(1): 57-87.

[7] Hurley, B. and Hurley, T. (2014). Paraunitary Marces and Group Rings. *International Journal of Theory*. 3(1):31-56.

[8] Berman, S.D.(1967). On the Theory of Group Codes. *Kibernetika*. 3(1):31-39.

[9] Charpin, P. (1983). The Extended Reed-Solomon Codes Considered as Ideals of a Modular Group Algebra. *Annals of Discrete Math*. 17: 171-176.

[10] Fu, W. and Feng, T. (2009). On Self-orthogonal Group Ring Codes. *Designs, Codes and Cryptography*. 50(2): 203-214.

[11] Huffman, W.C. and Pless, V.2003. *Fundamental of Error Correcting codes*. Cambridge: Cambridge University Press.

[12] Hughes, G. (2000). Consacyclic Codes, Cocycles and a u+v|u-v Construction. *IEEE Transaction in Information Theory*. 46(2): 674-680.