Group Ring Codes over a Dihedral Group

*Zi Shyuan Tan, Miin Huey Ang and Wen Chean The

Pusat Pengajian Sains Matematik, Universiti Sains Malaysia,
Minden 11800, Penang, Malaysia

E-mail: tzs13_mah007@student.usm.my

*Corresponding author

ABSTRACT

A group ring code is a code that can be constructed using group rings. Linear codes have been associated to group rings since 1967. Many existing codes such as cyclic codes and abelian codes are specific examples of group ring codes. This study aims to answer whether there exists a group ring code that can never be a group ring code over a cyclic group. It is conceivable that it has a positive answer. However, our results on group ring codes over the dihedral group \( D_6 \) and \( D_8 \) do not support our belief. We found that every binary group ring code over \( D_6 \) (\( D_8 \) respectively) is equivalent to some binary group ring code over the cyclic group \( C_6 \) (\( C_8 \) respectively).

1. INTRODUCTION

Suppose \( G \) is a finite group and \( R \) is a ring. Then \( RG = \{ \sum_{g \in G} a_g g \mid a_g \in R \} \) is called a group ring over \( G \), which has a ring structure as well as a free module structure. Codes that can be constructed using group rings are known as group ring codes. Group ring codes were first discussed by Berman, 1967 by associating every cyclic code to a group algebra over a cyclic group and by associating every Reed-Muller code to a group algebra over an elementary abelian 2-group. Two years later, MacWilliams, 1969, examined the class of codes associated to group rings over dihedral groups. Charpin, 1983, discovered that every extended Reed-Solomon code can be considered as an ideal of some modular group algebras. Well-known classical codes, such as the extended binary Golay code, have been shown to be group ring codes (Landrock and Manz, 1992; McLoughlin and Hurley, 2008).
In 2000, Hughes defined a group ring code as an ideal in a group ring. Since then, various studies on group ring codes, such as self-orthogonal group ring codes, checkable group ring codes and etcetera, have also been done in the literature (Fu and Feng, 2009; Jitman et al., 2010; Wong and Ang, 2013; Hurley, 2014). Hurley, 2006, discovered the isomorphism between a group ring and a ring of matrices. This result leads to a group ring encoding method for codes which was introduced by Hurley, 2009. The group ring codes introduced by Hurley are generally submodules of their corresponding group rings and are only ideals in certain restrictive cases. Throughout this paper, when we say group ring codes, we mean codes that are constructed using group ring encoding method that was introduced by Hurley.

In the paper written by McLoughlin and Hurley, 2008, the extended binary Golay code $G_{24}$ was shown to be a group ring code over the dihedral group $D_{24}$. However, we observe that this famous code $G_{24}$ is not only a group ring code over the dihedral group $D_{24}$ but can also be realised as a group ring code over the cyclic group $C_{24}$ as well. This trigger our curiosity on the relation between the group ring codes over dihedral groups and the group ring codes over cyclic groups. We observe that every group ring code over a cyclic group has a shift spanning set. Based on this observation, we propose a sufficient condition for a group ring code to be equivalent to a group ring code over a cyclic group. Particularly, we found that each binary group ring code over the dihedral group $D_{6}$ is always equivalent to a binary group ring code over the cyclic group $C_{6}$. Similarly, each binary group ring code over $D_{8}$ is always equivalent to a binary group ring code over the cyclic group $C_{8}$. This paper is organised as follows. We give some basic definitions in the preliminary section. Next section contains our main results and some conclusions are provided in the last section.

2. PRELIMINARY

In this paper, our focus is on binary group ring codes, that is, $F_{2}G$-codes, where $F_{2}$ is the finite field of order 2 and $G$ is a group. Therefore, all the definitions and results given are restricted to the finite field $F_{2}$, although some of them are applicable for an arbitrary ring $R$.

Let $W$ be a submodule of $F_{2}G$ and $u \in F_{2}G$. A function $f_{u}: W \rightarrow F_{2}G$ such that $f_{u}(x) = ux$ is called a group ring encoding function (Hurley, 2009). The image of $f_{u}$, denoted as $C_{G}(u, W)$, is called an $F_{2}G$-code with generator $u$ relative to the submodule $W$. Thus $C_{G}(u, W)$ is the set $\{ux | x \in W\}$. 
It is pointed out by Hurley, 2009, that if a submodule of $F_2G$ has a basis that consists of only group elements, then the corresponding generating matrix and parity check matrix can be constructed easily. Hence, following Hurley’s approach, we concern only on $F_2G$-codes such that the corresponding submodule $W$ are generated by a subset $N$ of $G$, that is $W = L_{F_2}(N)$. It is easy to verify that the code $C_G(u, W) = L_{F_2}(uN)$ and thus $uN$ is a spanning set for $C_G(u, W)$. By abuse of notation, we denote the group ring code by $C_G(u, N)$ instead of $C_G(u, W)$. Clearly the group ring code $C_G(u, G)$ is of the greatest dimension among the group ring codes generated by $u$.

From now on, for the remaining of this section, fix a group $G$. Suppose $\{g_1, g_2, ..., g_n\}$ is a fixed listing of the elements of $G$. Every $F_2G$-code $C_G(u, N)$ can be associated with a linear code, denoted $C_G(u, N)$, of length $n$ by identifying $x = \sum_{i=1}^{n} a_i g_i \in C_G(u, N)$ with the binary string $\bar{x} = a_1 a_2 ... a_n$. Note that if a linear code of length $n$ can be realised as a group ring code over some group, then the corresponding group must be of order $n$. Recall that two binary linear codes $C_1$ and $C_2$ are called equivalent if and only if there exist a permutation of coordinates which sends $C_1$ to $C_2$. Equivalently, there exist a pair of bases of $C_1$ and $C_2$ respectively that are equivalent. Two group ring codes are said to be equivalent if they are associated to two equivalent linear codes.

**Definition 2.1.** (Hurley, 2009). The $F_2G$-matrix of $u = \sum_{g_i \in G} a_i g_i \in F_2G$ is the matrix $[a^{-1}_{g_i} g_j]_{n \times n}$. The rank of $u$, denoted rank$(u)$, is the rank of the $F_2G$-matrix for $u$.

**Remark 2.2.**

(i) Every $i^{th}$ row in $F_2G$-matrix of $u$ can be identified with the element $g_i u \in F_2G$ and thus the rank of $u$ is equal to the maximum number of linearly independent elements in $\{g_1 u, g_2 u, ..., g_n u\}$.

(ii) Suppose $u \in F_2G$ with rank$(u) = k$. The dimension of any $F_2G$-code generated by $u$ is at most $k$; particularly, the dimension of $C_G(u, G)$ is equal to $k$.

(iii) Suppose $u \in F_2G$. Every element of the form $ux \in F_2G$ where $x \in G$ has the same rank as $u$.

For any element $u = \sum_{g \in G} a_g g \in F_2G$, the support of $u$ is defined to be the set

$$\text{supp}(u) = \{g \in G | a_g \neq 0\}$$
and the weight of \( u \) is defined by

\[
wt(u) = |\text{supp}(u)|.
\]

3. MAIN RESULTS

3.1. Group Ring Codes over Cyclic group up to Equivalent

It is well known that the cyclic codes are useful because they are convenient for efficient error detection and correction. In this section, we discuss on the group ring codes over cyclic group \( C_n = \langle g | g^n = 1 \rangle \), which can be treated as a generalisation of cyclic codes.

Recall that the map \( \pi: F_2^n \to F_2^n \) such that \( \pi(a_1 a_2 ... a_n) = a_n a_1 a_2 ... a_{n-1} \) is called a cyclic shift map. Using the cyclic shift map \( \pi \), we define a shift set as follows.

**Definition 3.1.1.** A set \( \{v_1, v_2, ..., v_k\} \subseteq F_2^n \) is called a shift set if each \( v_i = \pi^{m_i}(v_1) \) for some positive integer \( m_i \).

The following is a result for a group ring code to be equivalent to a group ring code over a cyclic group.

**Proposition 3.1.2.** Suppose \( \{g_1, g_2, ..., g_n\} \) is a fixed listing of the elements of \( G \). An \( F_2G \)-code is equivalent to a binary group ring code over a cyclic group of order \( n \) if and only if the associated linear code has a spanning set that is equivalent to a shift set.

**Proof.** Suppose \( \{1, g, g^2, ..., g^n\} \) is a fixed listing of elements in the cyclic group \( C_n \) and \( C_G(u, N) \) is an \( F_2G \)-code that is equivalent to \( C_{C_n}(v, M) \), a group ring code over \( C_n \). Note that the set \( \overrightarrow{vM} \) is a shift set that span the code \( C_{C_n}(v, M) \). Since \( \overrightarrow{C_G(u, N)} \) is equivalent to \( \overrightarrow{C_{C_n}(v, M)} \), the code \( C_G(u, N) \) has a spanning set that is equivalent to \( \overrightarrow{vM} \).

Let \( C_G(u, N) \) be an \( F_2G \)-code. Suppose \( \overrightarrow{C_G(u, N)} \) has a spanning set that is equivalent to a shift set \( \overrightarrow{S} = \{\overrightarrow{v_1}, \overrightarrow{v_2}, ..., \overrightarrow{v_k}\} \) where \( \overrightarrow{v_1} = a_1 a_2 ... a_n \) and \( \overrightarrow{v_i} = \pi^{m_i}(\overrightarrow{v_1}) \) for some positive integers \( m_i \). The set \( \overrightarrow{S} \) can be identified with the set \( \{v_1, v_2, ..., v_k\} \) where \( v_1 = a_1 + a_2 g + ... + a_n g^{n-1} \) and \( v_i = v_1 g^{m_i} \), which span an \( F_2C_n \)-code. Hence, \( C_G(u, N) \) is equivalent to a binary cyclic group ring code.

Before going on, we prove the following result that will be used to facilitate our discussion afterwards.
Proposition 3.1.3. Suppose $u \in F_2G$ and $x \in G$. For arbitrary $N \subseteq G$, there exists $N' \subseteq G$ such that $C_G(ux, N') = C_G(u, N)$. Particularly, the code $C_G(ux, G)$ is the same as the code $C_G(u, G)$.

Proof. Suppose $N = \{g_{k_1}, g_{k_2}, \ldots, g_{k_t}\} \subseteq G$. Then the code

$$C_G(u, N) = \langle L_1 \rangle = \{ \langle u \rangle \}.$$

For each $i = 1, 2, \ldots, t$, there exists unique $g_{h_i} \in G$ such that $xg_{h_i} = g_{k_i}$. Hence,

$$C_G(u, N) = \langle L_1 \rangle = \{ \langle u \rangle \}.$$

Particularly, we have $C_G(ux, G) = \langle L_1 \rangle = \{ \langle u \rangle \}$.

We have settle down the basic layout that is needed and now we are ready to move on to discuss on the relation between the group ring codes over dihedral groups and the group ring codes over cyclic groups.

From now on, let $D_{2n} = \langle a, b | a^n = b^2 = 1, ba = a^{-1}b \rangle$ be the dihedral group of order $2n$ and $C_{2n} = \langle g | g^{2n} = 1 \rangle$ be the cyclic group of order $2n$. Throughout our discussion, we shall consider $\{1, a, a^2, \ldots, a^{n-1}, b, ba, ba^2, \ldots, ba^{n-1}\}$ and $\{1, g, g^2, \ldots, g^{2n-1}\}$ as the fixed listing of elements in $D_{2n}$ and $C_{2n}$ respectively.

Given an $F_2D_{2n}$-code $C_{D_{2n}}(u, N)$ where $N \subseteq D_{2n}$, our aim is to look for a suitable $\sigma$ and $\tau$ such that the $F_2C_{2n}$-code $C_{C_{2n}}(u, M)$ is equivalent to $C_{D_{2n}}(u, N)$. By Proposition 3.1.2, an $F_2D_{2n}$-code $C_{D_{2n}}(u, N)$ is equivalent to an $F_2C_{2n}$-code if there exist a permutation of coordinates such that the set $\bar{u}N$ is a shift set.

In our work, we need another technical result. Fix an element $u = \sum_{i=0}^{n-1} a_i a^i + \beta_i ba^i \in F_2D_{2n}$ and $N = \{a^{i_1}, a^{i_2}, \ldots, a^{i_{t}}, ba^{j_1}, ba^{j_2}, \ldots, ba^{j_k}\}$. Let $u' = \sum_{i=0}^{n-1} a_i a^i + (\beta_i ba^i)a^t$ and $N' = \{a^{i_1}, a^{i_2}, \ldots, a^{i_{t}}, ba^{j_1+t}, ba^{j_2+t}, \ldots \}$.
\[
\ldots, bα^i k^t \}\) for some integer \( t \). Under the permutation on coordinates that fixed \( i \in \{1,2, \ldots, n\} \) and map \( n + k \to n + (t + k) \mod n \) for \( k \in \{1,2, \ldots, n\} \), that is \( \frac{1}{2^2-1} n \to n + (t + 2) \mod n \to n + (t + (n+1)) \mod n \) \), the linear code \( L_{D_2n}(u', N') \) is identical with \( L_{D_2n}(u, N) \). Hence the code \( L_{D_2n}(u', N') \) is equivalent to \( L_{D_2n}(u, N) \). This gives part (i) of the following result. Note that part (ii) of the following proposition is true by Proposition 3.1.3.

**Proposition 3.1.4.** Suppose \( u = \sum_{i=0}^{n-1} α_i a^i + β_i bα^i \in F_2 D_{2n} \) and \( u' = \sum_{i=0}^{n-1} α_i a^i + (β_i bα^i) a^t \) for some integers \( t \). Then

(i) Every group ring code generated by \( u' \) is equivalent to some group ring code generated by \( u \).

(ii) Every group ring code generated by \( u' x \), where \( x \in D_{2n} \), is equivalent to some group ring code generated by \( u \).

In the next two sections, we shall discuss the equivalence between \( F_2 D_{2n} \)-codes and \( F_2 C_{2n} \)-codes for \( n = 3 \) and 4. For each \( F_2 D_{2n} \)-code \( L_{D_2n}(u, N) \), we search for an equivalent \( F_2 C_{2n} \)-code \( L_{D_2n}(u, N) \). Says \( u \) is of weight \( w \) and rank \( k \). For the sake of comparison, we choose an \( F_2 C_{2n} \) element of weight \( w \) and rank \( k \) as our \( v \). In fact, any \( F_2 C_{2n} \) element of weight \( w \) and of rank greater than or equal to \( k \) may act as \( v \). Nevertheless, \( v \) with smaller rank may not work; this is due partially to the fact that every group ring code with generator of rank \( k \) has dimension at most \( k \) (Hurley, 2009).

As shown in the following examples, a code \( L_{D_2n}(u, N) \) can be equivalent to \( L_{C_{2n}}(v, M) \) although \( u \) and \( v \) are of different rank or weight.

**Example 3.1.5.** The element \( 1 + a + b + ba \in F_2 D_6 \) is of rank 2 and \( 1 + g + g^2 + g^4 \in F_2 C_6 \) is of rank 5. The code \( L_{D_6}(1 + a + b + ba, \{1, a\}) = L_{F_2} \{1 + a + b + ba, a + a^2 + ba + ba^2\} \) can be identified with the code \( L_{D_6}(1 + a + b + ba, \{1, a\}) = L_{F_2} \{110110, 011011\} \) whereas the code \( L_{C_6}(1 + g + g^2 + g^4, \{1, g\}) = L_{F_2}(1 + g + g^2 + g^4, g + g^2 + g^3 + g^5) \) can be identified with the code \( L_{C_6}(1 + g + g^2 + g^4, \{1, g\}) = L_{F_2}(110101, 011101) \).

We can verify that the codes \( L_{D_6}(1 + a + b + ba, \{1, a\}) \) and \( L_{C_6}(1 + g + g^2 + g^4, \{1, g\}) \) are equivalent, by some permutation of the
digits, which implies that the code \( C_{D_6} (1 + a + b + ba, \{1, a\} \) is equivalent to the code \( C_{C_6} (1 + g + g^2 + g^4, \{1, g\}) \).

**Example 3.1.6.** Both the elements \( 1 + a + a^2 + b \in F_2D_6 \) and \( 1 + g \in F_2C_6 \) are of rank 5 but of different weight. It can be shown that \( C_{D_6} (1 + a + a^2 + b, D_6) \) and \( C_{C_6} (1 + g, C_6) \) are equivalent, which consist of all \( F_2^5 \) elements of even weight. Hence, the codes \( C_{D_6} (1 + a + a^2 + b, D_6) \) and \( C_{C_6} (1 + g, C_6) \) are equivalent.

### 3.2. \( F_2D_6 \)-code versus \( F_2C_6 \)-code

Recall that \( D_6 = \langle a, b \mid a^3 = b^2 = 1, ba = a^{-1}b \rangle \) is the dihedral group of order 6 and \( C_6 = \langle g \mid g^6 = 1 \rangle \) is the cyclic group of order 6. We start our discussion by considering a partition \( P \) of \( F_2D_6 \). Using Proposition 3.1.3 and 3.1.4, for a fixed \( u = \sum_{i=0}^{2} \alpha_i a^i + \beta_i ba^i \in F_2D_6 \), we group all the elements \( u' \) in \( F_2D_6 \) such that every group ring code generated by \( u' \) is equivalent to a code generated by \( u \) into a set denoted by \( A_u \), namely, \( A_u = \{ \sum_{i=0}^{2} \alpha_i a^i + \beta_i ba^i \mid t \in \{0,1,2\}, x \in D_6 \} \). Then we take \( P = \{ A_u \mid u \in U \} \), where \( U = \{ 0, 1, 1 + a, 1 + b, 1 + a + b, 1 + a + a^2, 1 + a + a^2 + b, 1 + a + b + ba, 1 + a + a^2 + b + ba, 1 + a + a^2 + b + ba^2 \} \) is a set of all distinct representative elements of each component in \( P \). Note that every nonzero element \( u \in U \) has 1 in their support. The Table 1 shows that \( P = \{ A_u \mid u \in U \} \) is a partition of \( F_2D_6 \).

| \( u \in F_2D_6 \) | \( A_u \) | \( |A_u| \) |
|------------------|--------------|--------|
| 0                | \{0\}        | 1      |
| 1                | \{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 \in 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 + a^2 + b + ba | \{(1 + a + a^2 + b + ba)x \mid x \in D_6\} | 9      |
| 1 + a + a^2 + b + ba | \{(1 + a + a^2 + b + ba)x \mid x \in D_6\} | 6      |
| 1 + a + a^2 + ba + ba^2 | \{1 + a + a^2 + b + ba + ba^2\} | 1      |

Since every code generated by an element in \( A_u \) is equivalent to some code generated by \( u \), if we manage to prove that every \( F_2D_6 \)-code generated by \( u \in U \setminus \{0\} \) is equivalent to some \( F_2C_6 \)-code, then we can conclude that
every $F_2D_6$-code is an $F_2C_6$-code up to equivalent. Hence, we only focus on those codes with generator $u \in U\setminus\{0\}$ starting from this point. Now, we categorise all the elements $u \in U\setminus\{0\}$ according to their weight and rank in the following table.

**TABLE 2: Categorisation of elements in $U$**

<table>
<thead>
<tr>
<th>Wt</th>
<th>$u \in U\setminus{0}$</th>
<th>rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$1$</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>$1 + a$</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>$1 + b$</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>$1 + a + b$</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>$1 + a + a^2$</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>$1 + a + a^2 + b$</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>$1 + a + b + ba$</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>$1 + a + a^2 + b + ba$</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>$1 + a + a^2 + b + ba + ba^2$</td>
<td>1</td>
</tr>
</tbody>
</table>

Next, for every $u \in U\setminus\{0\}$, we want to identify the possible element $v_u \in F_2C_6$ such that every group ring code with generator $u$ is equivalent to some group ring code generated by $v_u$. Suppose $u$ is of weight $w$ and rank $k$. For the sake of comparison, we would like to choose an $F_2C_6$ element of weight $w$ and rank $k$ that has 1 in the support as our $v_u$. As shown in the following table, for every $u \in U\setminus\{0\}$, such an element $v_u \in F_2C_6$ that we seek exists.

**TABLE 3: Element $v_u \in F_2C_6$ of same weight and rank with $u \in U\setminus\{0\}$**

<table>
<thead>
<tr>
<th>Wt</th>
<th>$u \in U\setminus{0}$</th>
<th>$v_u \in F_2C_6$</th>
<th>rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$1$</td>
<td>$1$</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>$1 + a$</td>
<td>$1 + g^2$</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>$1 + b$</td>
<td>$1 + g^4$</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>$1 + a + b$</td>
<td>$1 + g + g^2$</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>$1 + a + a^2$</td>
<td>$1 + g + g^2 + g^4$</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>$1 + a + a^2 + b$</td>
<td>$1 + g + g^2 + g^4 + g^5$</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>$1 + a + b + ba$</td>
<td>$1 + g + g^2 + g^4 + g^5$</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>$1 + a + a^2 + b + ba$</td>
<td>$1 + g + g^2 + g^4 + g^5 + g^6$</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>$1 + a + a^2 + b + ba + ba^2$</td>
<td>$1 + g + g^2 + g^4 + g^5 + g^6$</td>
<td>1</td>
</tr>
</tbody>
</table>

Now, we want to show that every $F_2D_6$-code with generator $u \in U\setminus\{0\}$ is an $F_2C_6$-code with generator $v_u$ up to equivalent. Our next example illustrates specifically for $u = 1 + a$.

**Example 3.2.1.** Consider the $F_2D_6$-codes $C_{D_6}(1 + a, N)$ where $N$ is an arbitrary subset of $D_6$. Note that $wt(1 + a) = 2$ and $rank(1 + a) = 4$. From Table 3.2.3, the element $1 + g^2 \in F_2C_6$ is of the same weight and same rank as $1 + a$. 

*Malaysian Journal of Mathematical Sciences*
Recall that a codeword of the form $\sum_{i=0}^{2} \alpha_i a^i + \beta_i b a^i \in F_2 D_6$ is identified with the binary codeword $\alpha_0 \alpha_1 \alpha_2 \beta_0 \beta_1 \beta_2$, whereas a codeword of the form $\sum_{i=0}^{5} \omega_i g^i \in F_2 C_6$ is identified with the binary codeword $\omega_0 \omega_1 \omega_2 \omega_3 \omega_4 \omega_5$. Additionally, $C_{D_6}(1 + a, N)$ has a spanning set $(1 + a)N$. Similar is true for $C_{C_6}(1 + g^2, M)$.

By comparing the two sides of the table below, we can choose $M$ easily such that $C_{D_6}(1 + a, N)$ and $C_{C_6}(1 + g^2, M)$ are equivalent, to be described below.

**TABLE 4**: Binary representations for $(1 + a)D_6$ and $(1 + g^2)C_6$

<table>
<thead>
<tr>
<th>$x \in D_6$</th>
<th>$(1 + a)x$</th>
<th>$(1 + a)y$</th>
<th>$y \in C_6$</th>
<th>$(1 + g^2)y$</th>
<th>$(1 + g^2)y'$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 + a</td>
<td>110000</td>
<td>1</td>
<td>1 + g^2</td>
<td>101000</td>
</tr>
<tr>
<td>a</td>
<td>a + a^2</td>
<td>011000</td>
<td>g^2</td>
<td>g^2 + g^4</td>
<td>001010</td>
</tr>
<tr>
<td>a^2</td>
<td>1 + a^2</td>
<td>101000</td>
<td>g^4</td>
<td>1 + g^4</td>
<td>100010</td>
</tr>
<tr>
<td>b</td>
<td>b + ba^2</td>
<td>000110</td>
<td>g^5</td>
<td>g + g^5</td>
<td>010001</td>
</tr>
<tr>
<td>ba</td>
<td>b + ba</td>
<td>000110</td>
<td>g</td>
<td>g + g^3</td>
<td>010100</td>
</tr>
<tr>
<td>ba^2</td>
<td>ba + ba^2</td>
<td>000011</td>
<td>g^3</td>
<td>g^3 + g^5</td>
<td>001011</td>
</tr>
</tbody>
</table>

By the permutation $(1 2 3 4 5 6)$ abbreviated as $(2 3 5 4)$, notice that the two sets of binary codewords are the same. Hence, for any $N$ subset of $D_6$, we can easily find $M$ such that $C_{D_6}(1 + a, N)$ is equivalent to $C_{C_6}(1 + g^2, M)$. For example, let $\phi$ be the bijection defined by $\phi(1) = 1, \phi(a) = g^2, \phi(a^2) = g^4, \phi(b) = g^5, \phi(ba) = g, \phi(ba^2) = g^3$, then we can take $M$ to be $\phi(N)$.

Table 5 shows the corresponding permutation that works in the way as described in Example 3.2.1 for other representative elements $u \in U \setminus \{0\}$. Table 5 tells that every $F_2 D_6$-code generated by $u \in U \setminus \{0\}$ is equivalent to some $F_2 C_6$-code generated by $v_u$, an element in $F_2 C_6$ such that $1 \in supp(v_u)\), $wt(v_u) = wt(u)$ and $rank(v_u) = rank(u)$.

**TABLE 5**: Permutations that sends $C_{D_6}(u, D_6)$ to $C_{C_6}(v_u, C_6)$

<table>
<thead>
<tr>
<th>$u \in U \setminus {0}$</th>
<th>$v_u \in F_2 C_6$</th>
<th>Permutation on coordinates</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>$(2 3 5 4)$</td>
</tr>
<tr>
<td>1 + a</td>
<td>1 + g^2</td>
<td>$(2 3 5 4)$</td>
</tr>
<tr>
<td>1 + b</td>
<td>1 + g^4</td>
<td>$(2 3 5 4)$</td>
</tr>
<tr>
<td>1 + a + a^2</td>
<td>1 + g^4 + g^6</td>
<td>$(2 3 5 4)$</td>
</tr>
<tr>
<td>1 + a + b</td>
<td>1 + g + g^2</td>
<td>$(2 3 5 4)$</td>
</tr>
</tbody>
</table>

*Malaysian Journal of Mathematical Sciences* 45
TABLE 5 (continued): Permutations that sends $C_{D_6}(u, D_6)$ to $C_{C_6}(v, C_6)$

<table>
<thead>
<tr>
<th>$u \in U\setminus{0}$</th>
<th>$v_u \in F_2C_6$</th>
<th>Permutation on coordinates</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1 + a + a^2 + b + ba$</td>
<td>$1 + g + g^2 + g^4$</td>
<td>(2 3 5 4)</td>
</tr>
<tr>
<td>$1 + a + b + ba$</td>
<td>$1 + g^2 + g^4 + g^5$</td>
<td>(2 3 5 6)</td>
</tr>
<tr>
<td>$1 + a + a^2 + b + ba$</td>
<td>$1 + g + g^2 + g^4$</td>
<td>(2 3 5 4)</td>
</tr>
<tr>
<td></td>
<td>$+ g^3$</td>
<td></td>
</tr>
<tr>
<td>$1 + a + a^2 + b + ba + ba^2$</td>
<td>$1 + g + g^2 + g^3$</td>
<td>(2 3 5 4)</td>
</tr>
<tr>
<td></td>
<td>$+ g^4 + g^5$</td>
<td></td>
</tr>
</tbody>
</table>

Theorem 3.2.2. Every $F_2D_6$-code is a $F_2C_6$-code up to equivalent.

**Proof.** Suppose $u'$ is a nonzero element in $F_2D_6$ and $N'$ is a non-empty subset in $D_6$. Consider the $F_2D_6$-code $C_{D_6}(u', N')$. The element $u'$ belongs to $A_u$ for some $u \in U\setminus\{0\}$. By Proposition 3.1.3 or Proposition 3.1.4, the code $C_{D_6}(u', N')$ is equivalent to some $F_2C_6$-code $C_{D_6}(u, N)$ for some $N \subseteq D_6$. Since $C_{D_6}(u, N)$ is equivalent to some $F_2C_6$-code $C_{C_6}(v_u, M)$, by transitivity, the code $C_{D_6}(u', N')$ is equivalent to some $F_2C_6$-code $C_{C_6}(v, M)$.

3.3. $F_2D_8$-code versus $F_2C_8$-code

The dihedral group and cyclic group of order 8 are denoted as $D_8 = \langle a, b | a^4 = b^2 = 1, ba = a^{-1}b \rangle$ and $C_8 = \langle g | g^8 = 1 \rangle$ respectively.

Similar to the works in section 3.2, for a fixed $u = \sum_{i=0}^{3} \alpha_i a^i + \beta_1 ba^i \in F_2D_8$, we group all the elements $u'$ in $F_2D_8$ such that every group ring code generated by $u'$ is equivalent to a code generated by $u$ into a set denoted by $A_u$, namely, $A_u = \{ [\sum_{i=0}^{3} \alpha_i a^i + \beta_1 (ba^i) a^i] x | x \in \{0,1,2,3\}, x \in D_8 \}$.

The $A_u$s are either identical or disjoint and there are altogether 21 distinct $A_u$. The set $P = \{A_u | u \in U \}$ forms a partition of $F_2D_8$, where $U = \{0, 1 + a, 1 + a^2, 1 + b, 1 + a + a^2, 1 + a^2 + b, 1 + a + b, 1 + a + a^2 + a^3, 1 + a + a^2 + b, 1 + a^2 + b + ba^2, 1 + a + b + ba, 1 + a + b + ba^2, 1 + a + a^2 + a^3 + b, 1 + a + a^2 + b + ba^2, 1 + a + a^2 + b + ba, 1 + a + a^2 + a^3 + b + ba^2, 1 + a + a^2 + a^3 + b + ba + ba^2, 1 + a + a^2 + a^3 + b + ba + ba^2 + ba^3 \}$, as summarised in Table 6. Note that every $u \in U$ is the representative element of each component in $P$. 

46 Malaysian Journal of Mathematical Sciences
After that, we categorise all the elements \( u \in U \setminus \{0\} \) according to their weight and rank. Then, we search for possible candidate \( v_u \in F_2C_8 \) such that \( 1 \in \text{supp}(v_u) \), \( \text{wt}(v_u) = \text{wt}(u) \) and \( \text{rank}(v_u) = \text{rank}(u) \). It happens that such elements \( v_u \) that we seek exist for all nonzero \( u \in U \) except for \( u = 1 + a + a^2 + b \). Lastly, we determine the permutations on coordinates that sends \( C_{D_8}(u, D_8) \) to \( C_{C_8}(v_u, C_8) \) for all the 19 nonzero representative elements \( u \) (except for the case \( u = 1 + a + a^2 + b \)) as summarised in table 7. The codes generated by elements in \( A_{1+a+a^2+b} \) will be dealt separately.

TABLE 7: Permutations that sends \( C_{D_8}(u, D_8) \) to \( C_{C_8}(v_u, C_8) \)

<table>
<thead>
<tr>
<th>Wt</th>
<th>( u \in F_2D_8 )</th>
<th>( v_u \in F_4C_8 )</th>
<th>rank</th>
<th>Permutation on coordinates</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>8</td>
<td>(2 3 5)(4 7 6)</td>
</tr>
<tr>
<td></td>
<td>( 1 + a )</td>
<td>( 1 + g^2 )</td>
<td>6</td>
<td>(2 3 5)(4 7 6)</td>
</tr>
<tr>
<td></td>
<td>( 1 + a^2 )</td>
<td>( 1 + g^4 )</td>
<td>4</td>
<td>(2 3 5)(4 7 6)</td>
</tr>
<tr>
<td></td>
<td>( 1 + b )</td>
<td>( 1 + g^4 )</td>
<td>4</td>
<td>( e )</td>
</tr>
</tbody>
</table>
TABLE 7 (continued): Permutations that sends $C_{D_8}(u, D_8)$ to $C_{C_8}(u, C_8)$

<table>
<thead>
<tr>
<th>Wt</th>
<th>$u \in F_2 D_8$</th>
<th>$v_u \in F_2 C_8$</th>
<th>rank</th>
<th>Permutation on coordinates</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>$1 + a + a^2$</td>
<td>$1 + g^2 + g^4$</td>
<td>8</td>
<td>(2 3 5) (4 7 6)</td>
</tr>
<tr>
<td></td>
<td>$1 + a + b$</td>
<td>$1 + g + g^2$</td>
<td>8</td>
<td>e</td>
</tr>
<tr>
<td>4</td>
<td>$1 + a + a^2 + a^3$</td>
<td>$1 + g^2 + g^4 + g^6$</td>
<td>2</td>
<td>(2 3 5) (4 7 6)</td>
</tr>
<tr>
<td></td>
<td>$1 + a^2 + b + ba^2$</td>
<td>$1 + g^2 + g^4 + g^6$</td>
<td>2</td>
<td>e</td>
</tr>
<tr>
<td></td>
<td>$1 + a + b + ba^2$</td>
<td>$1 + g + g^3 + g^5$</td>
<td>3</td>
<td>e</td>
</tr>
<tr>
<td>5</td>
<td>$1 + a + a^2 + a^3 + b$</td>
<td>$1 + g^2 + g^4 + g^6 + g$</td>
<td>8</td>
<td>(2 3 5) (4 7 6)</td>
</tr>
<tr>
<td></td>
<td>$1 + a^2 + b + ba^2$</td>
<td>$1 + g^2 + g^4 + g^6 + g$</td>
<td>8</td>
<td>e</td>
</tr>
<tr>
<td>6</td>
<td>$1 + a + a^2 + a^3 + b + ba$</td>
<td>$1 + g^2 + g^4 + g^6 + g + g^4$</td>
<td>6</td>
<td>(2 3 5) (4 7 6)</td>
</tr>
<tr>
<td></td>
<td>$1 + a^2 + a^3 + b + ba + ba^2$</td>
<td>$1 + g^2 + g^4 + g^6 + g + g^5$</td>
<td>4</td>
<td>(2 3 5) (4 7 6)</td>
</tr>
<tr>
<td>7</td>
<td>$1 + a + a^2 + a^3 + b + ba + ba^2$</td>
<td>$1 + g^2 + g^4 + g^6 + g + g^3 + g^3 + g^5 + g^5$</td>
<td>8</td>
<td>(2 3 5) (4 7 6)</td>
</tr>
<tr>
<td>8</td>
<td>$1 + a + a^2 + a^3 + b + ba + ba^2 + ba^3$</td>
<td>$1 + g^2 + g^4 + g^6 + g + g^3 + g^5 + g^7$</td>
<td>1</td>
<td>(2 3 5) (4 7 6)</td>
</tr>
</tbody>
</table>

Now, we discuss on the exceptional case, the $F_2D_8$-codes with generator in $A_w$ where $w = 1 + a + a^2 + b$. If we manage to show that all $F_2D_8$-codes generated by $w$ is equivalent to some $F_2C_8$-code, then every $F_2D_8$-codes generated by an element in $A_w$ is equivalent to some $F_2C_8$-code.

Consider a code $C_{D_8}(w, N')$ of dimension $k$. Recall that if $|N'| > k$ (implies that $wN'$ is a linearly dependent spanning set for $(w, N')$), then there exists a subset $N \subset N'$ with $|N| = k$ such that $wN$ is linearly independent and span the same code as $wN'$, that is, $C_{D_8}(w, N) = C_{D_8}(w, N')$. This means that, focus on those set $N$ with $|N| = k$ such that $wN$ is a basis for the code $C_{D_8}(w, N)$ is enough to cover all $F_2D_8$-codes of dimension $k$ with generator $w$.

Note that $w$ is of rank 4 and hence the dimensions of $F_2D_8$-codes with generator $w$ are at most 4 (Hurley, 2009).

(i) **Dimension = 4**: Recall that the code $C_{D_8}(w, D_8)$ is the code of largest size (hence of dimension = 4) among all the $F_2D_8$-codes generated by $w$. Any 4 linearly independent elements in the set $wD_8$ form a basis for the code $C_{D_8}(w, D_8)$.

Hence every dimension four $F_2D_8$-codes generated by $w$ is the same as the code $C_{D_8}(w, \{1, a, a^2, a^3\}) = L_{F_2}(w, wa, wa^2, wa^3)$ which can be identified with the code $C_{D_8}(w, \{1, a, a^2, a^3\}) = L_{F_2}(S)$, where $S = \{1110100, 01110100, 10110010, 11010001\}$. 

48  Malaysian Journal of Mathematical Sciences
Note that $C_{D_8}(w, \{1, a, a^2, a^3\})$ is equivalent to the code \( C = L_{F_2}\{11101000, 00111010, 10001110, 10100011\} \) that can be realised as the code $C_{C_8}(1 + g + g^2 + g^4, \{1, g^2, g^4, g^6\})$.

(ii) **Dimension = 3:** Let $N = \{x, y, z\} \subset D_8$ such that $wN$ is linearly independent.

First, we determine the number of possible $F_2D_8$-codes (up to equivalent) of dimension 3 with generator $w$. Table 8 as follows describe the support of $wx$ for all $x \in D_8$. From the table, we can see that any three elements in $wD_8$ are linearly independent and hence any three elements in $D_8$ can form such a set $N$. This implies that there are $C_3^8 = 56$ different combinations that can form $N$.

**TABLE 8:** The support of $(1 + a + a^2 + b)x$ for $x \in D_8$

<table>
<thead>
<tr>
<th>$x \in D_8$</th>
<th>1</th>
<th>$a^i$</th>
<th>$a^{-1}$</th>
<th>$b$</th>
<th>$ba$</th>
<th>$ba^{-1}$</th>
<th>$ba^i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>$ba^i$</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>$a$</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>$b$</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>$a^2$</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>$ba$</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>$a^3$</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>$ba^2$</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

From table 8, we also observe that $|\text{supp}(a^i) \cap \text{supp}(ba^{i-1})| = 0$ for $i \in \{0,1,2,3\}$. For an element $z \in D_8$ where $z \neq a^i$ and $z \neq ba^{i-1}$, we have $|\text{supp}(a^i) \cap \text{supp}(z)| = |\text{supp}(ba^{i-1}) \cap \text{supp}(z)| = 2$.

**Case 1:** Suppose there exist a pair of elements $x, y \in N$ such that $|\text{supp}(wx) \cap \text{supp}(wy)| = 0$.

In this case, two of the elements in $N$ are $a^i$ and $ba^{i-1}$ for some $i \in \{0,1,2,3\}$, whereas the third element can be chosen arbitrarily from the set $D_8 \setminus \{a^i, ba^{i-1}\}$. There are altogether $4 \times 6 = 24$ possible sets $N$ falling into this case. Every possible linear code $C_{D_8}(w, N)$ is equivalent to $C = L_{F_2}\{11110000, 00001111, 00111100\}$, which can be realised as the code $C_{C_8}(1 + g + g^2 + g^3, \{1, g^2, g^4\})$. 

*Group Ring Codes over a Dihedral Group*

*Malaysian Journal of Mathematical Sciences*
Case 2: Suppose the intersection of supports for each pair of element in \( wN \) is equal to 2. From Table 3.3.3, we observe that \( \bigcap_{x \in N} supp(wx) \bigcap 2 \). There are \( \frac{8 \times 6 \times 4}{3!} = 32 \) different sets \( N \) falling into this case. Each possible linear code \( C_{D_8}(w, N) \) is equivalent to \( C = L_{F_2}\{11101000, 00111010, 10001110\} \), which can be realised as the \( F_2C_8 \)-code \( C_{C_8}(1 + g + g^2 + g^4, \{1, g^2, g^4\}) \).

From the two cases, we conclude that every group ring code of dimension 3 with generator \( w \) is equivalent to some group ring code over \( C_8 \).

(iii) **Dimension = 2:** Let \( N = \{x, y\} \subset D_8 \) such that \( wN \) is linearly independent. As stated in previous case, \( |supp(wx) \bigcap supp( wy)| \) is either 0 or 2.

**Case 1:** Suppose \( |supp(wx) \bigcap supp( wy)| = 0 \). Then \( C_{D_8}(w, N) \) is equivalent to \( C = L_{F_2}\{11110000, 00001111\} \), which can be realised as the code \( C_{C_8}(1 + g + g^2 + g^3, \{1, g^4\}) \).

**Case 2:** Suppose \( |supp(wx) \bigcap supp( wy)| = 2 \). Then \( C_{D_8}(w, N) \) is equivalent to \( C = L_{F_2}\{11110000, 00111100\} \), which can be realised as the code \( C_{C_8}(1 + g + g^2 + g^3, \{1, g^2\}) \).

From the discussions, we see that every \( F_2D_8 \)-code with generator \( w \) is equivalent to some \( F_2C_8 \)-code.

Hence, similar to the Theorem 3.2.2, we can conclude that every \( F_2D_8 \)-code is a \( F_2C_8 \)-code up to equivalent.

**4. CONCLUSION**

In this paper, we see that every group ring code over a cyclic group has a shift spanning set. We have shown that every \( F_2D_6 \)-code (or \( F_2D_8 \)-code) can always be expressed as an \( F_2C_6 \)-code (or \( F_2C_8 \)-code) up to equivalent by using a suitable generator and an appropriate submodule. In fact, we also get similar result for \( F_2D_{10} \)-codes, that is, every \( F_2D_{10} \)-code is equivalent to some \( F_2C_{10} \)-codes. However we do not know yet whether the converse is true. We do know the existence of an \( F_2C_4 \)-code that can never be an \( F_2D_4 \)-code. The existence of a group ring code that can never be a group ring code over a cyclic group remains as an open problem. Our result on \( F_2D_{2n} \)-code
where \( n = 3, 4 \) and 5 led us to conjecture that, every group ring code over the dihedral group \( D_{2n} \) is equivalent to some group ring code over the cyclic group \( C_{2n} \).

**ACKNOWLEDGEMENT**

This work was supported in part by Universiti Sains Malaysia (USM) Research University (RU) Grant no. 1001/PMATHS/811286.

**REFERENCES**


