# On equivalency of zero-divisor codes via classifying their idempotent generator

**Designs, Codes and Cryptography manuscript No.**
(will be inserted by the editor)

# On Equivalency of Zero-divisor Codes via Classifying Their Idempotent Generator

**Kai Lin Ong · Miin Huey Ang**

Received: date / Accepted: date

**Abstract** In 2009, Ted and Paul Hurley proposed a code construction method using group rings. These codes with single generator are termed *group ring codes* and in particular *zero-divisor codes* when using zero-divisors as generators. In this paper, we mainly study the equivalency of zero-divisor codes in $F_2G$ having generator from $I(G)$, the set of all idempotents in $F_2G$. For abelian $G$, our previous notion of *generated idempotents* completely classified $I(G)$ by serving as its basis. Here, we first extend the notion of generated idempotents to study and classify some elements in $I(G)$ for non-abelian $G$. Later, the study is generally done on equivalency of zero-divisor codes in $F_2G$, then concentrating on those with idempotent generator. In particular, we affirm the conjecture "Every group ring code in $F_2D_{2n}$ is equivalent to some in $F_2C_{2n}$" in the cases where the generators are our classified idempotents. We also show that the equivalency of zero-divisor codes in $F_2C_n$ with generated idempotent as generators can be established sufficiently on the generator property.

**Keywords** group ring code · zero-divisor code · idempotent · code equivalency

**Mathematics Subject Classification (2010)** 94B99 · 20C05 · 20D35

## 1 Introduction

The idea of defining codes as ideals in the group algebra $F_qG$ for finite group $G$ were introduced by Berman and MacWilliams independently [1,7]. These codes are termed *group codes*. In ring theory, a ring element whose square is itself is

Kai Lin Ong
School of Mathematical and Computer Sciences, Heriot-Watt University Malaysia, 62200 Putrajaya, W.P. Putrajaya, Malaysia
Tel.: +6016-7463529
E-mail: k.ong@hw.ac.uk

Miin Huey Ang (Corresponding author)
School of Mathematical Sciences, Universiti Sains Malaysia, 11800 Gelugor, Penang, Malaysia
Tel.:+6016-4221102
E-mail: mathamh@usm.my

an *idempotent*. For decades, group codes having idempotent generators remain at the forefront of research.This is due to the fact that any group code $C$ in $F_qG$ with $char(F_q)|G$ can be expressed as $\bigoplus_{i=1}^{l} F_qGe_i$ for some $l \in \mathbb{Z}^+$ where each $e_i$ is called a *primitive central idempotent generator* of $C$ [8]. These primitive central idempotent generators played a crucial role in extracting the parameters and algebraic properties of the group codes [3,12].

In 2009, Hurley and Hurley [4] presented a brand new construction method of codes which involved group rings $RG = \{ \sum_{g \in G} a_g g | a_g \in R\}$.

**Definition 1.1** *Let $RG$ be a group ring with $u \in RG$ and $W$ be an $R$ -submodule of $RG$. Define $f_{W,u} : W \to RG$ by $(w)f_{W,u} = wu$ for every $w \in W$. Then, $C = Im(f_{W,u})$ is called a group ring code in $RG$ and $u$ is called the generator of $C$.*

The resultant group ring code has the property of being an $R-$submodule of $RG$. For every $w \in W$, $w$ is known as a message word and $wu$ is a codeword in $C = Im(f_{W,u})$. Clearly, $C = Wu = \{wu : w \in W\}$. For every codeword $c = \sum_{g \in G} a_g g \in C$, define its *support* $supp(c) = \{g \in G | a_g \neq 0\}$ and weight $wt(c) = |supp(c)|$. Also, it can be easily verified that $f_{W,u}$ is an $R$-linear map and thus $C$ is an $R$-submodule of $RG$. Research work on group ring codes further led to the dichotomy of zero-divisor and unit-derived codes in $RG$, depending on the nature of their generator. From the point of zero-divisor codes, note that when $W = RG$, the resultant zero-divisor codes in $RG$ possess ideal structure, thus coinciding with the notion of group codes. Such codes in the form of $RGu$ are called ideal zero-divisor codes in $RG$. Various works on zero-divisor and unit-derived codes were established in the recent ten years, predominantly on the self-duality of codes and the construction of new convolutional codes [5,6].

The main study of equivalent codes is to identify the criteria that helps to classify codes that look different as a set but perform alike as codes from the theoretical and practical points. Theoretically, two codes are considered different if they exhibit different algebraic structures. Practically, two codes are considered different if they have different parameter sets.

In 1962, MacWilliams proved that two linear codes of the same length are equivalent if and only if there is a weight-preserving isomorphism between them [2]. A definition of equivalent zero-divisor codes in $F_2G$ is given by modifying MacWilliams' result into the following group ring version.

**Definition 1.2** *Let $G_1$ and $G_2$ be two finite groups with $|G_1| = |G_2|$. Let $W_1u_1$ and $W_2u_2$ be zero-divisor codes in $F_2G_1$ and $F_2G_2$ respectively. Then, $W_1u_1$ and $W_2u_2$ are said to be equivalent if there exists an $F_2$-linear isomorphism $\varphi : W_1u_1 \to W_2u_2$ such that for every codeword $c \in W_1u_1$, $wt(c) = wt((c)\varphi)$.*

In general, despite the exhibition of different algebraic properties of the non-isomorphic $G_1$ and $G_2$, there are 9 examples for which equivalency holds between zero-divisor codes in $F_2D_{2n}$ and those in $F_2C_{2n}$, where $D_{2n}$ and $C_{2n}$ are the dihedral and cyclic groups of order $2n$ respectively [13]. This lead to the conjecture "Every group ring code in $F_2D_{2n}$ is equivalent to some group ring codes in $F_2C_{2n}$" [13]. As any arbitrary idempotent in $F_2G$ can be chosen as a generator of a zero-divisor code $C = Wu$ in $F_2G$, the primary step to study equivalency is to

establish a way to classify and identify idempotents in $F_2G$. Let $I(G)$ be the set of all idempotents in $F_2G$. For abelian $G$, a new classification of idempotents that completely classified and identified all elements in $I(G)$ were introduced by Ong and Ang in 2017 [9,10]. This was done by first affirming the existence of a proper subset of $I(G)$ where the support of each of its element is generated by an element in $G$.

**Definition 1.3** *Let $G$ be an abelian group and let $e \in I(G)$ with $|supp(e)| = k$. If $e = \sum_{i=0}^{k-1} g^{2^i}$ for $g \in supp(e)$, then $e$ is said to be a generated idempotent in $F_2G$ with generator $g$ and is denoted by $\langle g \rangle_{Id}$.*

Throughout this paper, $I_{\langle Id \rangle}(G)$ denotes the set of all generated idempotents in $F_2G$. We have shown that apart from a subset of $I(G)$, $I_{\langle Id \rangle}(G)$ is precisely a basis for $I(G)$. The readers can refer to Corollary 3.6 in [9].

**Theorem 1.4** *Let $G$ be an abelian group. Then, $I_{\langle Id \rangle}(G)$ is a basis for $I(G)$.*

The identification of $I_{\langle Id \rangle}(G)$ for abelian $G$ began with the following theorem, which in fact holds generally for any $G$.

**Theorem 1.5** *Let $g \in G$. Then, $\langle g \rangle_{Id}$ is a non-trivial generated idempotent in $F_2G$ if and only if $ord(g)$ is odd with $ord(g) > 1$.*

Readers who are interested with the details of the complete identification of $I_{\langle Id \rangle}(G)$ for abelian $G$ are referred to [9,10]. We include a concise example to illustrate the identification of $I(G)$ for an abelian $G$. Note that, throughout this paper, $C_n$ denotes a cyclic group of order $n$ whereas $C_{\langle g \rangle}$ denotes a cyclic group with generator $g$.

**Example 1.6** *Consider $F_2C_{14}$ with $C_{14}$=$C_{\langle x \rangle}$. The set of all generated idempotents in $F_2C_{14}$ comprises three elements, that is $I_{\langle Id \rangle}(G) = \{1, \langle x^2 \rangle_{Id} = x^2 + x^4 + x^8, \langle x^6 \rangle_{Id} = x^6 + x^{10} + x^{12}\}$. Hence, by Theorem 1.4, we have $I(C_{14}) = L_{F_2}(I_{\langle Id \rangle}(C_{14}))$, the linear span of $I_{\langle Id \rangle}(C_{14})$ over $F_2$ with $|I(C_{14})| = 2^3 = 8$.*

From [9], it is instructive to note that we had shown for distinct $\langle g \rangle_{Id}, \langle h \rangle_{Id} \in I_{\langle Id \rangle}(G)$, $supp\langle g \rangle_{Id} \cap supp\langle h \rangle_{Id} = \emptyset$. This eventually led to the following classification of elements in $I(G)$ for abelian $G$.

**Theorem 1.7** *Every non-zero $e \in I(G)$ is either a generated idempotent or a finite sum of some generated idempotents in $F_2G$.*

Unfortunately, for non-abelian $G$, the extension of this result fails to hold as shown by a counterexample in the dihedral group ring over $D_6 = \langle a, b | a^3 = b^2 = 1, aba = b^{-1} \rangle$; the element $a + ab + a^2b \in F_2D_6$ belongs to neither of the forms. However, we persist to focus on those idempotents in the form of Theorem 1.7 as Theorem 1.5 convincingly suggests that there is an abundance of $e \in I_{\langle Id \rangle}(G)$ for most of the groups $G$.

The paper is organized as follow. In Section 2, as for non-abelian $G$, $I(G)$ no longer possesses vector space structure, and so the study on $I(G)$ is then primarily focused on identifying and studying the properties of a subset of $I_{\langle Id \rangle}(G)$, called the set of joint idempotents, that is, $J(G) = \{\langle g \rangle_{Id} \in I_{\langle Id \rangle}(G) | \langle g \rangle_{Id} + \langle h \rangle_{Id} \in I(G)$, for every $\langle h \rangle_{Id} \in I_{\langle Id \rangle}(G)\}$. A complete classification of $J(G)$ for several

families of non-abelian $F_2G$ is given in Section 3. Section 4 consists of a comprehensive study on the conditions that affirms the equivalency between zero-divisor codes in $F_2G$. The results are then utilized in Section 5, in which we will show that every zero-divisor code in $F_2D_{2n}$ with idempotent generator in either form mentioned in Theorem 1.7 has an equivalent form in $F_2C_{2n}$. Also, we establish the equivalency of zero-divisor codes in $F_2C_n$ with generated idempotent as generator by solely looking at the generator property.

## 2 Idempotents in Non-abelian $F_2G$

Throughout this section, $G$ is fixed to be a non-abelian group. Consider distinct generated idempotents $\langle g\rangle_{Id}, \langle h\rangle_{Id} \in I_{\langle Id\rangle}(G)$. In general, Theorem 1.4 for general $G$ does not hold as $\langle g\rangle_{Id} + \langle h\rangle_{Id}$ is not necessarily in $I(G)$. This can be seen from the counterexample $G = A_4$, the alternating group on $\{1, 2, 3, 4\}$. It can be verified that $\langle(123)\rangle_{Id} = (123) + (132), \langle(124)\rangle_{Id} = (124) + (142) \in I_{\langle Id\rangle}(G)$ but $\langle(123)\rangle_{Id} + \langle(124)\rangle_{Id} \notin I(G)$. This triggers the introduction of the notion of joinability of generated idempotents.

**Definition 2.1** *For distinct $\langle g\rangle_{Id}, \langle h\rangle_{Id} \in I_{\langle Id\rangle}(G)$, $\langle g\rangle_{Id}$ is said to be joinable with $\langle h\rangle_{Id}$ if $\langle g\rangle_{Id} + \langle h\rangle_{Id} \in I(G)$.*

For distinct $\langle g\rangle_{Id}, \langle h\rangle_{Id} \in I_{\langle Id\rangle}(G)$, note that $(\langle g\rangle_{Id}+\langle h\rangle_{Id})^2 = \langle g\rangle_{Id}+\langle h\rangle_{Id}$ if and only if $\langle g\rangle_{Id}\langle h\rangle_{Id} + \langle h\rangle_{Id}\langle g\rangle_{Id} = 0$. This results in the following bi-condition, which will be frequently utilized subsequently in this section: $\langle g\rangle_{Id}$ is joinable with $\langle h\rangle_{Id}$ if and only if $\langle g\rangle_{Id}\langle h\rangle_{Id} = \langle h\rangle_{Id}\langle g\rangle_{Id}$. The next result ensures that if $\langle g\rangle_{Id}$ is joinable with $\langle h\rangle_{Id}$, then $C_{\langle g\rangle}$ must permute with $C_{\langle h\rangle}$.

**Proposition 2.2** *For distinct $\langle g\rangle_{Id}, \langle h\rangle_{Id} \in I_{\langle Id\rangle}(G)$, if $\langle g\rangle_{Id}$ is joinable with $\langle h\rangle_{Id}$, then $C_{\langle g\rangle}C_{\langle h\rangle} = C_{\langle h\rangle}C_{\langle g\rangle}$.*

*Proof* Suppose that $\langle g\rangle_{Id}$ is joinable with $\langle h\rangle_{Id}$, then $\langle g\rangle_{Id}\langle h\rangle_{Id} = \langle h\rangle_{Id}\langle g\rangle_{Id}$. Then, for every $i \in \{0, 1, 2, ..., |supp\langle g\rangle_{Id}| - 1\}$ and $j \in \{0, 1, 2, ..., |supp\langle h\rangle_{Id}| - 1\}$, there exist $l \in \{0, 1, 2, ..., |supp\langle h\rangle_{Id}| - 1\}$ and $m \in \{0, 1, 2, ..., |supp\langle g\rangle_{Id}| - 1\}$ such that

$$g^{2^i}h^{2^j} = h^{2^l}g^{2^m}. \tag{2.1}$$

Note that for each $s \in \mathbb{Z}_n^+$, there exists unique $\{x_{i_1}, x_{i_2}, ..., x_{i_r}\} \subset \mathbb{N}$, such that $s = 2^{x_{i_1}} + 2^{x_{i_2}} + \cdot + 2^{x_{i_r}}$. Let $g^\alpha h^\beta \in C_{\langle g\rangle}C_{\langle h\rangle}$, this implies that there exists unique $\{i_1, i_2, ..., i_r\}, \{j_1, j_2, ..., j_s\} \subset \mathbb{N}$ such that $g^\alpha h^\beta = g^{\sum_{k=1}^{r} 2^{i_k}} h^{\sum_{k=1}^{s} 2^{j_k}} = \prod_{k=1}^{r} g^{2^{i_k}} \prod_{k=1}^{s} h^{2^{j_k}}$. Then, by (2.1), note that $\prod_{k=1}^{r} g^{2^{i_k}} \prod_{k=1}^{s} h^{2^{j_k}} = \prod_{k=1}^{s} h^{2^{l_k}} \prod_{k=1}^{r} g^{2^{m_k}} = h^{\sum_{k=1}^{s} 2^{l_k}} g^{\sum_{k=1}^{r} 2^{m_k}}$. Thus, $g^\alpha h^\beta = h^{\sum_{k=1}^{s} 2^{l_k}} g^{\sum_{k=1}^{r} 2^{m_k}} \in C_{\langle h\rangle}C_{\langle g\rangle}$ and this results in $C_{\langle g\rangle}C_{\langle h\rangle} \subseteq C_{\langle h\rangle}C_{\langle g\rangle}$. By a similar argument, it can be shown that $C_{\langle h\rangle}C_{\langle g\rangle} \subseteq C_{\langle g\rangle}C_{\langle h\rangle}$ and thus $C_{\langle g\rangle}C_{\langle h\rangle} = C_{\langle h\rangle}C_{\langle g\rangle}$. □

We term those $\langle g\rangle_{Id} \in I_{\langle Id\rangle}(G)$ which are joinable with every generated idempotent in $I_{\langle Id\rangle}(G)$ as follows.

**Definition 2.3** *Let $\langle g\rangle_{Id} \in I_{\langle Id\rangle}(G)$. Then, $\langle g\rangle_{Id}$ is termed a joint idempotent if for every $\langle h\rangle_{Id} \in I_{\langle Id\rangle}(G)$, $\langle g\rangle_{Id}$ is joinable with $\langle h\rangle_{Id}$.*

Throughout this paper, the set of all joint idempotents in $F_2G$ is denoted as $J(G)$. Then, $\langle g\rangle_{Id} \in J(G)$ if and only if for every $\langle h\rangle_{Id} \in I_{\langle Id\rangle}(G)$, $\langle g\rangle_{Id}\langle h\rangle_{Id} = \langle h\rangle_{Id}\langle g\rangle_{Id}$. For every $G$, $J(G)$ is always non-empty as the trivial generated idempotent $1 \in J(G)$. Moreover, we prove that $\{\langle g\rangle_{Id} \in I_{\langle Id\rangle}(G) | g \in Z(G)\} \subseteq J(G)$, where $Z(G)$ denotes the centre of $G$.

**Proposition 2.4** *Let $\langle g\rangle_{Id} \in I_{\langle Id\rangle}(G)$ with $g \in Z(G)$. Then, $\langle g\rangle_{Id} \in J(G)$.*

*Proof* Let $\langle h\rangle_{Id} \in I_{\langle Id\rangle}(G)$. Since $Z(G)$ is a subgroup of $G$, then $supp\langle g\rangle_{Id} \subseteq Z(G)$. This results in $\langle g\rangle_{Id}\langle h\rangle_{Id} = \langle h\rangle_{Id}\langle g\rangle_{Id}$. □

Recall that Proposition 2.2 reflects that joinability of $\langle g\rangle_{Id}, \langle h\rangle_{Id} \in I_{\langle Id\rangle}(G)$ results in their corresponding cyclic subgroups $C_{\langle g\rangle}$ and $C_{\langle h\rangle}$ of $G$ to be permuted. The next proposition gives a necessary condition for $\langle g\rangle_{Id} \in J(G)$.

**Proposition 2.5** *Let $\langle g\rangle_{Id} \in I_{\langle Id\rangle}(G)$. If $\langle g\rangle_{Id} \in J(G)$, then $C_{\langle g\rangle}$ permutes with every odd order subgroup of $G$.*

*Proof* It follows from Theorem 1.5 and Proposition 2.2 that $C_{\langle g\rangle}$ permutes with every odd order cyclic subgroup of $G$, that is $C_{\langle g\rangle}C_{\langle h\rangle} = C_{\langle h\rangle}C_{\langle g\rangle}$ for every odd order cyclic subgroup $C_{\langle h\rangle}$ of $G$. Let $K$ be an odd order subgroup of $G$. For every $g^ik \in C_{\langle g\rangle}K$, $C_{\langle g\rangle}C_{\langle k\rangle} = C_{\langle k\rangle}C_{\langle g\rangle}$ results in $g^ik = k^lg^j \in C_{\langle k\rangle}C_{\langle g\rangle} \subseteq KC_{\langle g\rangle}$ for some $k^l \in C_{\langle k\rangle}$ and $g^j \in C_{\langle g\rangle}$. Thus, $C_{\langle g\rangle}K \subseteq KC_{\langle g\rangle}$. Using a similar argument, it can be verified that $KC_{\langle g\rangle} \subseteq C_{\langle g\rangle}K$, hence $C_{\langle g\rangle}K = KC_{\langle g\rangle}$. □

Proposition 2.5 indicates the need of the notion of odd-permutable subgroups as defined next.

**Definition 2.6** *Let $H$ be an odd order subgroup of $G$. Then, $H$ is termed an odd-permutable subgroup of $G$ if $H$ permutes with every odd order subgroup of $G$.*

In group theory, the permutability of a subgroup always guarantee its subnormality [11]. In conjunction with the odd-permutability of a subgroup, we introduce the notion of odd-subnormality.

**Definition 2.7** *Let $H$ be an odd order subgroup of $G$. Then, $H$ is said to be an odd-subnormal subgroup of $G$ if there exists $1 = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_r$, a subnormal series where $|G_i|$ is odd for every $i \in \{1, 2, ..., r-1\}$ with $H = G_j$ for some $j \in \{0, 1, 2, ..., r-1\}$.*

Let $H$ and $K$ be distinct odd order subgroups of $G$. It follows easily that $HK$ and any conjugate of $H$ must have odd order. Then, with these assertions, the next theorem directly follows from the context in Section 13.2 in [11].

**Theorem 2.8** *Every odd-permutable subgroup of $G$ is an odd-subnormal subgroup of $G$.*

We thus obtain another necessary condition for $\langle g\rangle_{Id} \in J(G)$ as follows.

**Theorem 2.9** *Let $\langle g\rangle_{Id} \in I_{\langle Id\rangle}(G)$. If $\langle g\rangle_{Id} \in J(G)$, then $C_{\langle g\rangle}$ is odd-subnormal in $G$.*

*Proof* This follows from Proposition 2.5 and Theorem 2.8. □

## 3 Joint Idempotents in Some Non-abelian $F_2G$

In this section, $J(G)$ of three families of $F_2G$ are studied. The first two families involve groups which are semidirect product of their two cyclic subgroups.

**Definition 3.1** *Let $C_m$ and $C_n$ be two non-trivial cyclic subgroups of $G$. Then, $G$ is said to be a semidirect product of $C_m$ by $C_n$, denote as $G = C_m \rtimes C_n$, if the following conditions are satisfied:*

1. $G = C_mC_n = \{xy|x \in C_m, y \in C_n\}$ *with $C_m$ is normal in $G$,*
2. $C_m \cap C_n = \{1\}$.

### 3.1 Non-abelian Groups of Order $pq$

Let $G$ be of order $pq$, where $p$ and $q$ are two distinct odd primes, with $p > q$. Note that $G = C_p \rtimes C_q$. Therefore, $G = \langle x, y|x^p = y^q = 1, xy = yx^\alpha\rangle$ for some $\alpha \in \mathbb{Z}_p^* \setminus \{1\}$. Each element in $G$ has a general form of $x^iy^j$, where $i \in \{0, 1, 2, \ldots, p-1\}$ and $j \in \{0, 1, 2, \ldots, q-1\}$. By Theorem 1.5, we have $I_{\langle Id\rangle}(G) = \{\langle x^iy^j\rangle_{Id}|i \in \{0, 1, 2, \ldots, p-1\}, j \in \{0, 1, 2, \ldots, q-1\}\}$. Then, $I_{\langle Id\rangle}(G)$ can be partitioned into $\{\langle x^iy^j\rangle_{Id}|j \neq 0\}$ and $\{\langle x^iy^j\rangle_{Id}|j = 0\}$. We first show that for the former set,$\{\langle x^iy^j\rangle_{Id}|j \neq 0\} \cap J(G) = \emptyset$.

**Proposition 3.2** *Let $p$ and $q$ be two distinct odd primes, with $p > q$ and $G = C_p \rtimes C_q = \langle x, y|x^p = y^q = 1, xy = yx^\alpha\rangle$ for some $\alpha \in \mathbb{Z}_p^* \setminus \{1\}$. Then, for any $\langle x^{k_1}y^{k_2}\rangle_{Id} \neq \langle x^iy^j\rangle_{Id}$ with $j \neq 0$ and $k_2 \neq 0$, $\langle x^{k_1}y^{k_2}\rangle_{Id}$ is not joinable with $\langle x^iy^j\rangle_{Id}$ if and only if $C_{\langle x^{k_1}y^{k_2}\rangle} \neq C_{\langle x^iy^j\rangle}$.*

*Proof* Note that every proper subgroup of $G$ is of order either $p$ or $q$. Clearly, $C_p$ is a Sylow $p$-subgroup of $G$. As $C_p$ is normal in $G$, $C_p$ is the unique Sylow $p$-subgroup of $G$. Thus, $C_{\langle x^iy^j\rangle}$ must be a cyclic subgroup of $G$ with order $q$ for every $j \neq 0$.

Suppose that $C_{\langle x^{k_1}y^{k_2}\rangle} = C_{\langle x^iy^j\rangle}$, then clearly $\langle x^{k_1}y^{k_2}\rangle_{Id}$ is joinable with $\langle x^iy^j\rangle_{Id}$ as they are both in $I_{\langle Id\rangle}(C_{\langle x^iy^j\rangle})$. Conversely, suppose that $C_{\langle x^{k_1}y^{k_2}\rangle} \neq C_{\langle x^iy^j\rangle}$. Then, both $C_{\langle x^{k_1}y^{k_2}\rangle}$ and $C_{\langle x^iy^j\rangle}$ are of order $q$ with $C_{\langle x^{k_1}y^{k_2}\rangle} \cap C_{\langle x^iy^j\rangle} = \{1\}$. If $C_{\langle x^{k_1}y^{k_2}\rangle}$ permutes with $C_{\langle x^iy^j\rangle}$, then it follows that $C_{\langle x^{k_1}y^{k_2}\rangle}C_{\langle x^iy^j\rangle}$ is a subgroup of $G$ with $|C_{\langle x^{k_1}y^{k_2}\rangle}C_{\langle x^iy^j\rangle}| = q^2$. This contradicts Lagrange's Theorem. Thus, $C_{\langle x^{k_1}y^{k_2}\rangle}$ does not permute with $C_{\langle x^iy^j\rangle}$, Proposition 2.2 then concludes that $\langle x^{k_1}y^{k_2}\rangle_{Id}$ is not joinable with $\langle x^iy^j\rangle_{Id}$. □

The following corollary is a direct result from Proposition 3.2.

**Corollary 3.3** *Let $p$ and $q$ be two distinct odd primes, with $p > q$ and $G = C_p \rtimes C_q = \langle x, y|x^p = y^q = 1, xy = yx^\alpha\rangle$ for some $\alpha \in \mathbb{Z}_p^* \setminus \{1\}$. Then, $\langle x^iy^j\rangle_{Id} \notin J(G)$ if $j \neq 0$.*

Let us introduce a useful notation here. For $s \in \{1, 2, ..., p-1\}$, the 2-cyclotomic coset of $\mathbb{Z}_p$ containing $s$ is defined as $\mathfrak{C}_s = \{s(2^k)|k \in \mathbb{N}\}$. For the remaining $\{\langle x^iy^j\rangle_{Id}|j = 0\}$, the value of $\alpha \in \mathbb{Z}_p^* \setminus \{1\}$ from $G = C_p \rtimes C_q = \langle x, y|x^p = y^q = 1, xy = yx^\alpha\rangle$ determines their joinability. Before that, the following technical lemma is needed.

**Lemma 3.4** *Let $m, n \in \mathbb{Z}^+$ and $s \in \{1, 2, \ldots, m-1\}$. Let $G = \langle x, y | x^m = y^n = 1, xy = yx^\alpha \rangle$ for some $\alpha \in \mathbb{Z}_m^* \setminus \{1\}$. For every $i \in \{0, 1, 2, \ldots, m-1\}$ and $j \in \{0, 1, 2, \ldots, n-1\}$, $x^{s2^{k_1}}(x^i y^j)^{2^{k_2}} = (x^i y^j)^{2^{k_2}} x^{s2^{k_1}\alpha^{2^{k_2}j}}$ for $k_1, k_2 \in \mathbb{N}$.*

*Proof* The proof can be directly shown using multidimensional mathematical induction on $k_1, k_2 \in \mathbb{N}$. □

**Theorem 3.5** *Let $p$ and $q$ be two distinct odd primes, with $p > q$ and $G = C_p \rtimes C_q = \langle x, y | x^p = y^q = 1, xy = yx^\alpha \rangle$ for some $\alpha \in \mathbb{Z}_p^* \setminus \{1\}$. Then, for $s \in \{1, 2, \ldots, p-1\}$, $\langle x^s \rangle_{Id} \in J(G)$ if $\alpha \in \mathfrak{C}_1$, where $\mathfrak{C}_1$ is the 2-cyclotomic coset of $\mathbb{Z}_p$ containing 1.*

*Proof* Note that $\langle x^s \rangle_{Id} \in J(G)$ if and only if $\langle x^s \rangle_{Id} \langle x^i y^j \rangle_{Id} = \langle x^i y^j \rangle_{Id} \langle x^s \rangle_{Id}$ for each pair of $i \in \{0, 1, 2, \ldots, p-1\}$ and $j \in \{0, 1, 2, \ldots, q-1\}$. Let $g = x^{s2^{k_1}}(x^i y^j)^{2^{k_2}} \in supp(\langle x^s \rangle_{Id} \langle x^i y^j \rangle_{Id})$ for some $k_1, k_2 \in \mathbb{N}$. Then, by Lemma 3.4, $g = (x^i y^j)^{2^{k_2}} x^{s2^{k_1}\alpha^{2^{k_2}j}}$. Now, suppose that $\alpha \in \mathfrak{C}_1$, then $\alpha = 2^\beta$ for some $\beta \in \mathbb{N}$. Then, $g = (x^i y^j)^{2^{k_2}} x^{s2^{k_1}2^{\beta 2^{k_2}j}} = (x^i y^j)^{2^{k_2}} x^{s2^{k_1+\beta 2^{k_2}j}} \in supp(\langle x^i y^j \rangle_{Id} \langle x^s \rangle_{Id})$. Hence, $supp(\langle x^s \rangle_{Id} \langle x^i y^j \rangle_{Id}) \subseteq supp(\langle x^i y^j \rangle_{Id} \langle x^s \rangle_{Id})$. By a similar argument, it can be verified that $supp(\langle x^i y^j \rangle_{Id} \langle x^s \rangle_{Id}) \subseteq supp(\langle x^s \rangle_{Id} \langle x^i y^j \rangle_{Id})$ and thus we have that $\langle x^s \rangle_{Id} \langle x^i y^j \rangle_{Id} = \langle x^i y^j \rangle_{Id} \langle x^s \rangle_{Id}$. Therefore, $\langle x^s \rangle_{Id} \in J(G)$. □

As a whole, for non-abelian $G = C_p \rtimes C_q = \langle x, y | x^p = y^q = 1, xy = yx^\alpha \rangle$, if $\alpha \in \mathfrak{C}_1$, then $J(G) = \{\langle x^i y^j \rangle_{Id} | j = 0\}$.

### 3.2 Dihedral Groups

Recall the dihedral groups $D_{2n} = C_n \rtimes C_2 = \langle a, b | a^n = b^2 = 1, ab = ba^{-1} \rangle$ with $|D_{2n}| = 2n$. Every $g \in D_{2n}$ is either in the form of $a^k$ or $a^k b$ for some $k \in \mathbb{N}$. For $g = a^k b$, note that $ord(g) = 2$.

**Theorem 3.6** *Let $D_{2n} = \langle a, b | a^n = b^2 = 1, ab = ba^{-1} \rangle$. Then, $I_{\langle Id \rangle}(D_{2n}) = I_{\langle Id \rangle}(C_{\langle a \rangle})$.*

*Proof* For each $k \in \mathbb{N}$, as $ord(a^k b) = 2$, $a^k b$ cannot be a generator for any $\langle g \rangle_{Id} \in I_{\langle Id \rangle}(D_{2n})$ by Theorem 1.5. This results in $\langle g \rangle_{Id} \in I_{\langle Id \rangle}(D_{2n})$ if and only if $g \in C_{\langle a \rangle}$ with $ord(g)$ odd. Thus, it follows from Theorem 1.5 that $\langle g \rangle_{Id} \in I_{\langle Id \rangle}(D_{2n})$ if and only if $I_{\langle Id \rangle}(C_{\langle a \rangle})$. □

The following corollary is a result from Theorem 1.4 and Theorem 3.6.

**Corollary 3.7** *Let $D_{2n} = \langle a, b | a^n = b^2 = 1, ab = ba^{-1} \rangle$. Then, $J(D_{2n}) = I_{\langle Id \rangle}(D_{2n})$.*

We provide an example to illustrate the case when $n = 7$.

**Example 3.8** *Let $D_{14} = \langle a, b | a^7 = b^2 = 1, ab = ba^{-1} \rangle$. It can be verified that there are three generated idempotents in $F_2 C_{\langle a \rangle}$, namely 1, $\langle a \rangle_{Id} = a + a^2 + a^4$ and $\langle a^3 \rangle_{Id} = a^3 + a^5 + a^6$. Thus, $I_{\langle Id \rangle}(C_{\langle a \rangle}) = \{1, \langle a \rangle_{Id}, \langle a^3 \rangle_{Id}\}$. By Theorem 3.6, $I_{\langle Id \rangle}(D_{14}) = I_{\langle Id \rangle}(C_{\langle a \rangle})$. Then, it follows from Corollary 3.7 that $J(D_{14}) = I_{\langle Id \rangle}(D_{14}) = \{1, \langle a \rangle_{Id}, \langle a^3 \rangle_{Id}\}$.*

### 3.3 Non-abelian Groups of Order $2^k p$

Let $G$ be of order $2^k p$, where $k \in \mathbb{Z}^+$ and $p > 2$ is a prime. Let $\alpha$ be the total number of Sylow $p$-subgroups of $G$. The result on $J(G)$ depends on the uniqueness of the Sylow $p$-subgroup of $G$.

**Proposition 3.9** *Let $|G| = 2^k p$ where $p$ is a prime such that $p > 2$.*

1. *If the Sylow $p$-subgroup of $G$ is unique, then $J(G) = I_{\langle Id \rangle}(G)$.*
2. *If the Sylow $p$-subgroups of $G$ are not unique, then $J(G) = \{1\}$.*

*Proof* Suppose that $C_p$ is the unique Sylow $p$-subgroup of $G$, note that $C_p$ is the only odd order subgroup of $G$. By Theorem 1.5, all $\langle g \rangle_{Id} \in I_{\langle Id \rangle}(G)$ have generator $g \in C_p$. Then, $I_{\langle Id \rangle}(G) = I_{\langle Id \rangle}(C_p)$. By Theorem 1.4, $J(G) = I_{\langle Id \rangle}(G)$.

On the other hand, suppose that the Sylow $p$-subgroups of $G$ are not unique. Let $\langle g \rangle_{Id} \in I_{\langle Id \rangle}(G) \setminus \{1\}$. Then, $ord(g)$ must be odd by Theorem 1.5. Hence, $g \in C_p$ for some Sylow $p$-subgroup $C_p$ of $G$. Note that $C_{\langle g \rangle} = C_p$ is not a normal subgroup of $G$. Also, $C_{\langle g \rangle}$ is a maximal odd order subgroup of $G$. Thus, $C_{\langle g \rangle}$ is not an odd-subnormal subgroup of $G$. Then, it follows from Theorem 2.9 that $\langle g \rangle_{Id} \notin J(G)$. Hence, $J(G) = \{1\}$. □

This characterization of $J(G)$ leads to the corollary for the case where $|G| = 2^k p$ and $p$ is a prime such that $p > 2^k$.

**Corollary 3.10** *Let $|G| = 2^k p$ with $p > 2^k$ is a prime. Then, $J(G) = I_{\langle Id \rangle}(G)$.*

*Proof* We claim that the Sylow $p$-subgroup of $G$ is unique and thus the result follows from Proposition 3.9. Suppose that there exist $P_1$ and $P_2$, distinct Sylow $p$-subgroups of $G$, note that $P_1 \cap P_2 = \{1\}$. Then, $P_1 P_2$ has $p^2$ distinct elements. This results in $|G| > p^2 > 2^k p$. □

## 4 Equivalency of Zero-divisor Codes in $F_2G$

Throughout this section, $G$ denotes a finite group (not necessary non-abelian). Results in Section 2,3 and [9] imply that most of the groups $G$ have a pool of non-trivial idempotents to serve as the generator for their respective zero-divisor codes in $F_2G$. This section gives a comprehensive study on the equivalency of general zero-divisor codes in $F_2G$ based on Definition 1.2, where $W_1u_1$ and $W_2u_2$ are said to be equivalent if there exists an $F_2$-linear isomorphism $\varphi : W_1u_1 \to W_2u_2$, such that for every $c \in W_1u_1$, $wt(c) = wt((c)\varphi)$.

The property $wt(c) = wt((c)\varphi)$ for every $c \in W_1u_1$ of $\varphi$ is called weight-preserving. For every $Wu$, the notation $supp(Wu)$ denotes $\bigcup_{c \in Wu} supp(c)$. For the remaining paper, $W_1u_1$ and $W_2u_2$ are zero-divisor codes in $F_2G_1$ and $F_2G_2$ respectively, with $supp(W_1u_1) \subseteq G_1$ and $supp(W_2u_2) \subseteq G_2$.

We first show that the existence of an injective function $\chi : supp(W_1u_1) \to supp(W_2u_2)$ associated to a function $\varphi : W_1u_1 \to W_2u_2$ in such a way that $(\sum_{g \in supp(W_1u_1)} a_g g)\varphi = \sum_{g \in supp(W_1u_1)} a_g \chi(g)$ plays a vital role in making $\varphi$ a weight-preserving injective $F_2$-linear map.

**Theorem 4.1** *Let $W_1u_1$ and $W_2u_2$ be zero-divisor codes in $F_2G_1$ and $F_2G_2$ respectively. If there exists a function $\varphi : W_1u_1 \to W_2u_2$ in such a way that $(\sum_{g\in supp(W_1u_1)} a_g g)\varphi = \sum_{g\in supp(W_1u_1)} a_g\chi(g)$ for some function $\chi : supp(W_1u_1) \to supp(W_2u_2)$, then $\varphi$ is a weight-preserving injective $F_2$ -linear map if and only if $\chi$ is injective.*

*Proof* Suppose that $\chi$ is injective. Then, for each $c = \sum_{g\in supp(W_1u_1)} a_g g \in W_1u_1$,

$$wt((c)\varphi) = wt(\sum_{g\in supp(W_1u_1)} a_g\chi(g)) = wt(\sum_{g\in supp(W_1u_1)} a_g g) = wt(c).$$

Thus, $\varphi$ is a weight-preserving function. Note that $\varphi$ is closed under scalar multiplication over $F_2$ and for $c_1 = \sum_{g\in supp(W_1u_1)} a_g g, c_2 = \sum_{g\in supp(W_1u_1)} b_g g \in W_1u_1$,

$$\begin{aligned}(c_1 + c_2)\varphi &= \sum_{g\in supp(W_1u_1)} (a_g + b_g)\chi(g)\\ &= \sum_{g\in supp(W_1u_1)} a_g\chi(g) + \sum_{g\in supp(W_1u_1)} b_g\chi(g)\\ &= (c_1)\varphi + (c_2)\varphi\end{aligned}$$

Hence, $\varphi$ is an $F_2$-linear map with:

$$Ker(\varphi) = \{\sum_{g\in supp(W_1u_1)} a_g g \in W_1u_1 | (\sum_{g\in supp(W_1u_1)} a_g g)\varphi = 0\}.$$

By the choice of $\varphi$, note that $Ker(\varphi) = \{0\}$, thus $\varphi$ is injective.

Conversely, suppose that $\chi$ is not injective, there exist $g_1, g_2 \in supp(W_1u_1)$, $g_1 \neq g_2$ such that $\chi(g_1) = \chi(g_2)$. Note that as $W_1u_1$ is a linear code, there always exists $v \in W_1u_1$ such that $g_1, g_2 \in supp(v)$. Then, $wt((v)\varphi) \leq wt(v) - 1$, thus $\varphi$ is not weight-preserving. □

The following corollary is a direct result from Theorem 4.1.

**Corollary 4.2** *Let $W_1u_1$ and $W_2u_2$ be zero-divisor codes in $F_2G_1$ and $F_2G_2$ respectively. If there exists a function $\varphi : W_1u_1 \to W_2u_2$ in such a way that $(\sum_{g\in supp(W_1u_1)} a_g g)\varphi = \sum_{g\in supp(W_1u_1)} a_g\chi(g)$ for some function $\chi : supp(W_1u_1) \to supp(W_2u_2)$, then $W_1u_1$ is equivalent to $Im(\varphi)$ if and only if $\chi$ is injective.*

Consider $W_1u_1 = F_2G_1u_1$ and $W_2u_2 = F_2G_2u_2$ from the family of ideal zero-divisor codes in $F_2G_1$ and $F_2G_2$ respectively. Then, $supp(F_2G_1u_1) = G_1$ and $supp(F_2G_2u_2) = G_2$. Let $\chi : G_1 \to G_2$ be an injective function. To utilize Corollary 4.2, the focus is next concentrated on the sufficient conditions for the existence of $\varphi$ in the form of:

$$(\sum_{g\in G_1} a_g g)\varphi = \sum_{g\in G_1} a_g\chi(g) \tag{4.1}$$

Let $c = (\sum_{g\in G_1} a_g g)u_1 \in F_2G_1u_1$. Note that $c = \sum_{g\in G_1}\sum_{g_1\in supp(u_1)} a_g g g_1 = \sum_{g\in G_1, a_g\neq 0}\sum_{g_1\in supp(u_1)} g g_1$. Then, we have:

$$(c)\varphi = (\sum_{g\in G_1, a_g\neq 0}\sum_{g_1\in supp(u_1)} g g_1)\varphi = \sum_{g\in G_1, a_g\neq 0}\sum_{g_1\in supp(u_1)} \chi(g g_1) \tag{4.2}$$

On the other hand, in order to have $(c)\varphi \in F_2G_2u_2$:

$$(c)\varphi = (\sum_{h\in G_2} b_h h)u_2 = \sum_{h\in G_2}\sum_{g_2\in supp(u_2)} b_h h g_2 = \sum_{h\in G_2, b_h\neq 0}\sum_{g_2\in supp(u_2)} h g_2. \tag{4.3}$$

Then, by (4.2) and (4.3),

$$\sum_{g\in G_1, a_g\neq 0}\sum_{g_1\in supp(u_1)} \chi(g g_1) = \sum_{h\in G_2, b_h\neq 0}\sum_{g_2\in supp(u_2)} h g_2 \tag{4.4}$$

In addition, suppose that $\chi$ further satisfies the following conditions: For every $g \in G_1$ and $g_1 \in supp(u_1)$, $\chi(gg_1) = \chi(g)\chi(g_1)$ and $\chi(supp(u_1)) = supp(u_2)$. Then, from (4.4):

$$\begin{aligned}(c)\varphi &= \sum_{g\in G_1, a_g\neq 0}\sum_{g_1\in supp(u_1)} \chi(g g_1)\\ &= \sum_{g\in G_1, a_g\neq 0}\sum_{g_1\in supp(u_1)} \chi(g)\chi(g_1)\\ &= \sum_{g\in G_1, a_g\neq 0} \chi(g) \sum_{g_1\in supp(u_1)} \chi(g_1)\\ &= (\sum_{g\in G_1, a_g\neq 0} \chi(g))u_2\end{aligned}$$

These two conditions on $\chi$ guarantee the existence of $\varphi : F_2G_1u_1 \to F_2G_2u_2$ in such a way that $(\sum_{g\in G_1} a_g g)\varphi = \sum_{g\in G_1} a_g\chi(g)$ for a given injective function $\chi : G_1 \to G_2$. Furthermore, if $\chi$ is surjective, notice that $(c)\varphi = (\sum_{g\in G_1, a_g\neq 0} \chi(g))u_2$ also indicates that $\varphi$ is onto. A bijective $\chi$ that satisfies each of the two properties imposed earlier is defined formally.

**Definition 4.3** *Let $u_1$ and $u_2$ be zero-divisors in $F_2G_1$ and $F_2G_2$ respectively. Let $\chi : A \to B$ be a bijective function for $A \subseteq G_1$ and $B \subseteq G_2$. Then:*

1. *$\chi$ is denoted as $\chi_{u_1,u_2}$ if $\chi(supp(u_1)) = supp(u_2)$.*
2. *$\chi$ is termed a $u_1$-homomorphism if $\chi(gh) = \chi(g)\chi(h)$ for every $g \in A$ and $h \in supp(u_1)$.*

Using the terms in Definition 4.3, Theorem 4.1 and Corollary 4.2, the following two results naturally hold.

**Theorem 4.4** *Let $u_1$ and $u_2$ be zero-divisors in $F_2G_1$ and $F_2G_2$ respectively. If $\chi_{u_1,u_2} : G_1 \to G_2$ is a $u_1$-homomorphism, then there exists a weight-preserving $F_2$ -linear isomorphism $\varphi : F_2G_1u_1 \to F_2G_2u_2$ in such a way that $(\sum_{g\in G_1} a_g g)\varphi = \sum_{g\in G_1} a_g\chi_{u_1,u_2}(g)$.*

**Corollary 4.5** *Let $u_1$ and $u_2$ be zero-divisors in $F_2G_1$ and $F_2G_2$ respectively. If there exists $\chi_{u_1,u_2} : G_1 \to G_2$ which is a $u_1$-homomorphism, then $F_2G_1u_1$ and $F_2G_2u_2$ are equivalent ideal zero-divisor codes.*

For each $F_2$-submodule $W_1$ of $F_2G_1$, $W_1u_1$ is a subcode of $F_2G_1u_1$. Suppose that $F_2G_1u_1$ and $F_2G_2u_2$ are equivalent by a weight-preserving $F_2$-linear isomorphism $\varphi : F_2G_1u_1 \to F_2G_2u_2$. Define $\varphi_\downarrow$ by restricting $\varphi$ to a smaller domain $W_1u_1$, and then it is easy to see that the equivalency of $F_2G_1u_1$ and $F_2G_2u_2$ implies the equivalency of $W_1u_1$ and $Im(\varphi_\downarrow)$, a subcode of $F_2G_2u_2$. The following result gives the detail of $Im(\varphi_\downarrow)$ when $(\sum_{g\in G_1} a_g g)\varphi = \sum_{g\in G_1} a_g\chi_{u_1,u_2}(g)$ with respect to a $u_1$-homomorphism $\chi_{u_1,u_2} : G_1 \to G_2$.

**Corollary 4.6** *Let $u_1$ and $u_2$ be zero-divisors in $F_2G_1$ and $F_2G_2$ respectively. Let $W_1$ be an $F_2$-submodule of $F_2G_1$ with basis $\alpha$ such that $\alpha u_1$ is a basis for $W_1u_1$. If there exists a $u_1$-homomorphism $\chi_{u_1,u_2} : G_1 \to G_2$, then $W_1u_1$ is equivalent to $W_2u_2$, where $W_2$ is an $F_2$-submodule of $F_2G_2$ with a basis in the form of $\beta = \{\sum_{g\in supp(v)} \chi_{u_1,u_2}(g) | v \in \alpha\}$.*

*Proof* Note that $F_2G_1u_1$ and $F_2G_2u_2$ are equivalent with respect to some weight-preserving $F_2$-linear isomorphism $\varphi : F_2G_1u_1 \to F_2G_2u_2$ in such a way that $((\sum_{g\in G_1} a_g g)u_1)\varphi = (\sum_{g\in G_1} a_g\chi_{u_1,u_2}(g))u_2$ for $u_1$-homomorphism $\chi_{u_1,u_2} : G_1 \to G_2$.

Define $\varphi_\downarrow$ to be the restriction of $\varphi$ onto the smaller domain $W_1u_1$ and also $\chi_{u_1,u_2}\prime : supp(W_1u_1) \to supp(Im(\varphi_\downarrow))$ by restricting the domain and codomain of $\chi_{u_1,u_2}$ to $supp(W_1u_1) \subseteq G_1$ and $supp(Im(\varphi_\downarrow)) \subseteq G_2$. Clearly, $\varphi_\downarrow$ is a weight preserving injective $F_2$-linear map such that

$$(\sum_{g\in supp(W_1u_1)} a_g g)\varphi_\downarrow = \sum_{g\in supp(W_1u_1)} a_g\chi_{u_1,u_2}\prime(g)$$

and $\chi_{u_1,u_2}\prime$ is a $u_1$-homomorphism. Hence, $W_1u_1$ is a code with basis $\alpha u_1$, with $|\alpha u_1| = |\alpha|$ and is equivalent to $Im(\varphi_\downarrow)$. Note that $(c)\varphi_\downarrow = ((\sum_{v\in\alpha} a_v v)u_1)\varphi_\downarrow = ((\sum_{v\in\alpha} a_v \sum_{g\in supp(v)} g)u_1)\varphi_\downarrow = (\sum_{v\in\alpha} a_v \sum_{g\in supp(v)} \chi_{u_1,u_2}\prime(g))u_2$.

Let $W_2u_2 = Im(\varphi_\downarrow)$ where $W_2$ is an $F_2$-submodule of $F_2G_2$. Clearly, $W_2$ is spanned by $\beta = \{\sum_{g\in supp(v)} \chi_{u_1,u_2}(g) | v \in \alpha\}$. Then, $\beta u_2$ contains a basis for $W_2u_2$. However, note that $|\beta u_2| = |\beta| = |\alpha| = |\alpha u_1|$ as $\chi_{u_1,u_2}$ is bijective. As $\varphi_\downarrow$ is an isomorphism, $\gamma = \beta u_2$ is linearly independent over $F_2$ and thus $\gamma$ is a basis for $Im(\varphi_\downarrow) = W_2u_2$. Hence, $\beta$ is a basis for $W_2u_2$ otherwise $|\gamma| > |\beta|$.□

## 5 Equivalency of Zero-divisor Codes in $F_2G$ with Idempotent Generator

The studies of zero-divisor codes with idempotent generators are discussed from this point onwards. Classically, cyclic and dihedral groups with the same order $2n$

for $n > 2$ can never be isomorphic as commutativity holds for the former but not latter. In the next subsection, we answer the earlier conjecture partially, that is having our classified idempotent as generator, each zero-divisor code in $F_2D_{2n}$ is equivalent to some zero-divisor code in $F_2C_{2n}$.

### 5.1 Zero-divisor Codes in $F_2D_{2n}$ and $F_2C_{2n}$

Throughout this subsection, we denote $C_{2n} = C_{\langle x \rangle}$ as a cyclic group of order $2n$ and $D_{2n} = \langle a, b | a^n = b^2 = 1, ab = ba^{-1} \rangle$ as a dihedral group of order $2n$. Let $n = 2^\alpha \beta$ for some integer $\alpha \geq 0$ and odd integer $b > 1$, then $I_{\langle Id \rangle}(C_{2n}) = I_{\langle Id \rangle}(C_{\langle x^{2(2^\alpha)} \rangle})$ by Theorem 1.5. On the other hand, $I_{\langle Id \rangle}(D_{2n}) = I_{\langle Id \rangle}(C_{\langle a \rangle}) = I_{\langle Id \rangle}(C_{\langle a^{2^\alpha} \rangle})$ by Theorem 3.6. We thus obtain a one-to-one mapping from $I(C_{2n})$ to $I(D_{2n})$ as follows.

**Proposition 5.1** *Let* $I_{\langle Id \rangle}(C_{2n}) = \{\langle x^{2s_i} \rangle_{Id} | i \in \{1, 2, \ldots, l\}\}$ *and* $\alpha_1, \alpha_2, ..., \alpha_l \in F_2$. *Define* $\rho : I(C_{2n}) \to I(D_{2n})$ *by* $\rho(\sum_{i=1}^{l} \alpha_i \langle x^{2s_i} \rangle_{Id}) = \sum_{i=1}^{l} \alpha_i \langle a^{s_i} \rangle_{Id}$. *Then,* $\rho$ *is a one-to-one mapping.*

Setting each pair of idempotents in Proposition 5.1 as generator of ideal zero-divisor codes in $F_2C_{2n}$ and $F_2D_{2n}$ respectively, the two resultant codes are always equivalent as shown by the following theorem.

**Theorem 5.2** *Let* $I_{\langle Id \rangle}(C_{2n}) = \{\langle x^{2s_i} \rangle_{Id} | i \in \{1, 2, \ldots, l\}\}$ *and* $\alpha_1, \alpha_2, ..., \alpha_l \in F_2$. *Consider* $e_1 = \sum_{i=1}^{l} \alpha_i \langle a^{s_i} \rangle_{Id} \in I(D_{2n})$ *and* $e_2 = \sum_{i=1}^{l} \alpha_i \langle x^{2s_i} \rangle_{Id} \in I(C_{2n})$. *Then,* $F_2D_{2n}e_1$ *and* $F_2C_{2n}e_2$ *are equivalent ideal zero-divisor codes.*

*Proof* First, note that $\{(2i+1) \bmod 2n | i \in \{0, 1, \ldots, n-1\}\} = \{(-2i-1) \bmod 2n | i \in \{0, 1, \ldots, n-1\}\}$ and $(x^{2i+1})^{-1} = x^{-2i-1}$. Then, $C_{2n}$ can be partitioned as follows

$$\begin{aligned} C_{2n} &= \{x^{2i} | i \in \{0, 1, \ldots, n-1\} \cup \{x^{2i+1} | i \in \{0, 1, \ldots, n-1\} \\ &= \{x^{2i} | i \in \{0, 1, \ldots, n-1\} \cup \{x^{-2i-1} | i \in \{0, 1, \ldots, n-1\}. \end{aligned}$$

Define $\chi : D_{2n} \to C_{2n}$ such that

$$\chi(a^i b^j) = \begin{cases} x^{-2i-1} & j = 1 \\ x^{2i} & j = 0 \end{cases} \tag{5.1}$$

Clearly, $\chi$ is bijective and $\chi(supp(e_1)) = supp(e_2)$. Hence, $\chi = \chi_{e_1,e_2}$. Let $a^{2^k s_j} \in supp(e_1)$ for some $k \in \mathbb{Z}^+$. Then, for every $a^i b \in D_{2n}$, $\chi((a^i b)(a^{2^k s_j}))$ can be written as:

$$\chi(a^{i-2^k s_j} b) = x^{-2(i-2^k s_j)-1} = x^{-2i-1} x^{2(2^k s_j)} = \chi(a^i b)\chi(a^{2^k s_j}).$$

Similarly, for every $a^i \in D_{2n}$:

$$\chi(a^i a^{2^k s_j}) = \chi(a^{i+2^k s_j}) = x^{2(i+2^k s_j)} = x^{2i} x^{2(2^k s_j)} = \chi(a^i)\chi(a^{2^k s_j}).$$

This concludes that $\chi_{e_1,e_2}$ is an $e_1$-homomorphism, thus the proof follows from Corollary 4.5. □

**Example 5.3** *Utilizing Proposition 5.1, we establish a one-to-one correspondence from the idempotents in Example 1.6 to Example 3.8, a listing of all ideal zero-divisor codes in $F_2C_{14}$ with idempotent generator and its equivalent partner in $F_2D_{14}$ is obtained.*

| *Ideal Zero-divisor Codes in $F_2C_{14}$* | *Ideal Zero-divisor Codes in $F_2D_{14}$* |
|---|---|
| $F_2C_{14}$ | $F_2D_{14}$ |
| $F_2C_{14}\langle x^2\rangle_{Id}$ | $F_2D_{14}\langle a\rangle_{Id}$ |
| $F_2C_{14}\langle x^6\rangle_{Id}$ | $F_2D_{14}\langle a^3\rangle_{Id}$ |
| $F_2C_{14}(1+\langle x^2\rangle_{Id})$ | $F_2D_{14}(1+\langle a\rangle_{Id})$ |
| $F_2C_{14}(1+\langle x^6\rangle_{Id})$ | $F_2D_{14}(1+\langle a^3\rangle_{Id})$ |
| $F_2C_{14}(\langle x^2\rangle_{Id}+\langle x^6\rangle_{Id})$ | $F_2D_{14}(\langle a\rangle_{Id}+\langle a^3\rangle_{Id})$ |
| $F_2C_{14}(1+\langle x^2\rangle_{Id}+\langle x^6\rangle_{Id})$ | $F_2D_{14}(1+\langle a\rangle_{Id}+\langle a^3\rangle_{Id})$ |

Therefore, it follows that for each zero-divisor code in $F_2C_{2n}$ in the form of $W_1e_1$, the equivalent partner in $F_2D_{2n}$ is $W_2e_2$ , where $W_2$ can be obtained by Corollary 4.6.

## 5.2 Zero-divisor Codes in $F_2C_n$

In this last subsection, we continue the study of the equivalency of zero-divisor codes in $F_2C_n$ with idempotent generator. Note that for every $\langle x^s\rangle_{Id} \in I_{\langle Id\rangle}(C_n)$, $ord(x^s)$ must be odd by Theorem 1.5. Consider distinct idempotents $e_1 = \langle x^{s_1}\rangle_{Id}, e_2 = \langle x^{s_2}\rangle_{Id} \in I_{\langle Id\rangle}(C_n)$. For the case where $n$ is odd and $ord(x^{s_1}) = ord(x^{s_2}) = n$, both $x^{s_1}$ and $x^{s_2}$ are generators of $C_n$ and thus heuristically an $e_1$-homomorphism $\chi_{e_1,e_2} : C_n \to C_n$ is the automorphism of $C_n$ defined by $\chi_{e_1,e_2}(x^{s_1 i}) = x^{s_2 i}$. Then, by Corollary 4.5, the next result holds.

**Proposition 5.4** *Let $x^{s_1}, x^{s_2} \in C_n$ for odd $n$. If $ord(x^{s_1}) = ord(x^{s_2}) = n$, then $F_2C_n\langle x^{s_1}\rangle_{Id}$ and $F_2C_n\langle x^{s_2}\rangle_{Id}$ are equivalent ideal zero-divisor codes in $F_2C_n$.*

We summarize the case where $n$ is an odd prime in the next corollary.

**Corollary 5.5** *Let $n$ be an odd prime. All $F_2C_n\langle x^s\rangle_{Id}$ with $s \neq 0$ are equivalent ideal zero-divisor codes in $F_2C_n$.*

The establishment of equivalency between $F_2C_n\langle x^s\rangle_{Id}$ depends ultimately on the property of $\langle x^s\rangle_{Id}$. Gaining insight from Proposition 5.4, we prove that $ord(x^s)$ categorizes equivalent $F_2C_n\langle x^s\rangle_{Id}$. Before that, the following lemma is needed.

**Lemma 5.6** *For distinct $\langle x^{s_1}\rangle_{Id}, \langle x^{s_2}\rangle_{Id} \in I_{\langle Id\rangle}(C_n)$, if $ord(x^{s_1}) = ord(x^{s_2})$, then $|supp\langle x^{s_1}\rangle_{Id}| = |supp\langle x^{s_2}\rangle_{Id}|$.*

*Proof* Note that for $i \in \{1, 2\}$, $|supp\langle x^{s_i}\rangle_{Id}|$ is the smallest non-negative integer $k_i$ such that $ord(x^{s_i})|2^{k_i} - 1$. Then, it follows from $ord(x^{s_1}) = ord(x^{s_2})$ that $k_1 = k_2$. □

**Theorem 5.7** *For distinct $e_1 = \langle x^{s_1}\rangle_{Id}, e_2 = \langle x^{s_2}\rangle_{Id} \in I_{\langle Id\rangle}(C_n)$, $ord(x^{s_1}) = ord(x^{s_2})$ if and only if there exists an $e_1$-homomorphism $\chi_{e_1,e_2} : C_n \to C_n$.*

*Proof* Suppose that $ord(x^{s_1}) = ord(x^{s_2})$. Then, $|supp\langle x^{s_1}\rangle_{Id}| = |supp\langle x^{s_2}\rangle_{Id}|$ by Lemma 5.6. Let $ord(x^{s_1}) = ord(x^{s_2}) = m$, then by Lagrange's Theorem, $mr = n$ for some $r \in \mathbb{Z}^+$. Thus, $C_n = \{x^{i+js_1} | i \in \{0, 1, \ldots, r-1\}, j \in \{0, 1, \ldots, m-1\}\}$. Hence, $\chi_{e_1,e_2} : C_n \to C_n$ can be defined as $\chi_{e_1,e_2}(x^{i+js_1}) = x^{i+js_2}$ for each $i \in \{0, 1, \ldots, r-1\}$ and $j \in \{0, 1, \ldots, m-1\}$. Note that $\chi_{e_1,e_2}$ is also an $e_1$-homomorphism as for every $t = i + js_1 \in \{0, 1, \ldots, n-1\}$ and $k \in \mathbb{Z}^+$, $\chi_{e_1,e_2}(x^t x^{s_1 2^k}) = \chi_{e_1,e_2}(x^{i+s_1(j+2^k)})$. We claim that $\chi_{e_1,e_2}(x^{i+s_1(j+2^k)}) = x^{i+s_2(j+2^k)}$. To prove the claim, it is sufficient to show that for $h \in \{0, 1, \ldots, m-1\}$ and $h' \in \mathbb{N} \setminus \{0, 1, \ldots, m-1\}$, $x^{i+hs_2} = x^{i+h's_2}$ if $x^{i+hs_1} = x^{i+h's_1}$. Let $h' = h + \alpha$, then:

$$\begin{aligned} x^{i+hs_1} &= x^{i+h's_1} \\ x^{hs_1} &= x^{h's_1} \\ x^{hs_1} &= x^{(h+\alpha)s_1} \\ 1 &= x^{\alpha s_1} \end{aligned}$$

This implies that $\alpha$ must be a multiple of $m$ and thus:

$$\begin{aligned} x^{i+h's_2} &= x^{i+(h+\alpha)s_2} \\ &= x^{i+hs_2} x^{s_2\alpha} \\ &= x^{i+hs_2}(1) \\ &= x^{i+hs_2}. \end{aligned}$$

This results in:

$$\begin{aligned} \chi_{e_1,e_2}(x^{i+s_1(j+2^k)}) &= x^{i+s_2(j+2^k)} \\ &= x^{i+js_2} x^{s_2 2^k} \\ &= \chi_{e_1,e_2}(x^t)\chi_{e_1,e_2}(x^{s_1 2^k}). \end{aligned}$$

Conversely, suppose that there exists an $e_1$-homomorphism $\chi_{e_1,e_2} : C_n \to C_n$. Without loss of generality, assume that $m_1 = ord(x^{s_1}) < ord(x^{s_2}) = m_2$ where both $m_1$ and $m_2$ are odd. Note that $\chi_{e_1,e_2}(x^{s_1}) = x^{2^k s_2}$ for some $k \in \mathbb{N}$. It can be shown by mathematical induction that $\chi_{e_1,e_2}((x^{s_1})^t) = (\chi_{e_1,e_2}(x^{s_1}))^t$ for every $t \in \mathbb{N}$. Hence,

$$\chi_{e_1,e_2}(1) = \chi_{e_1,e_2}((x^{s_1})^{m_1}) = (\chi_{e_1,e_2}(x^{s_1}))^{m_1} = (x^{2^k s_2})^{m_1} \neq 1$$

as $ord(x^{2^k s_2}) = ord(x^{s_2}) = m_2 > m_1$. This is a contradiction to $\chi_{e_1,e_2}(x^{s_1}) = x^{2^k s_2}$ for some $k \in \mathbb{N}$ as

$$\chi_{e_1,e_2}(x^{s_1}) = \chi_{e_1,e_2}(1x^{s_1}) = \chi_{e_1,e_2}(1)\chi_{e_1,e_2}(x^{s_1}) = \chi_{e_1,e_2}(1)x^{2^k s_2} \neq x^{2^k s_2}.$$

Thus, $ord(x^{s_1}) = ord(x^{s_2})$. □

Together with Corollary 4.5, Theorem 5.7 implies the following result.

**Corollary 5.8** *For distinct $e_1 = \langle x^{s_1}\rangle_{Id}, e_2 = \langle x^{s_2}\rangle_{Id} \in I_{\langle Id\rangle}(C_n)$, if $ord(x^{s_1}) = ord(x^{s_2})$, then $F_2C_ne_1$ and $F_2C_ne_2$ are equivalent ideal zero-divisor codes in $F_2C_n$.*

For zero-divisor codes in $F_2C_n$ having a finite sum of some generated idempotents as generator, it is not easy to define an $e_1$-homomorphism $\chi_{e_1,e_2} : C_n \to C_n$ explicitly for each $n$. We end this section with the following subcase.

**Proposition 5.9** *Let $l = |I_{\langle Id\rangle}(C_n)|$ and $\alpha_1, \alpha_2, \ldots, \alpha_l \in F_2$. Consider distinct $e_1 = \sum_{i=1}^{l} \alpha_i \langle x^{s_i}\rangle_{Id}, e_2 = \sum_{i=1}^{l} \alpha_i \langle x^{s_i k}\rangle_{Id} \in I(C_n)$ with $(n,k) = 1$. Then, $F_2C_ne_1$ and $F_2C_ne_2$ are equivalent ideal zero-divisor codes in $F_2C_n$.*

*Proof* As $(n,k) = 1$, define an $e_1$-homomorphism $\chi : C_n \to C_n$ as the automorphism that maps the generator $x$ to the generator $x^k$, that is $\chi(x^i) = x^{ik}$. Note that $\chi(supp(e_1)) = supp(e_2)$. Thus, $\chi = \chi_{e_1,e_2}$ and Corollary 4.5 affirms the equivalency between $F_2C_ne_1$ and $F_2C_ne_2$. □

## 6 Conclusion

This paper is on the usefulness of idempotent generators in establishing the equivalency of zero-divisor codes in $F_2G$, via their classifications on $I(G)$. For non-abelian $G$, the fact that $I(G)$ need not form a vector space over $F_2$ triggered the study of the *joinability* between distinct $\langle g\rangle_{Id}, \langle h\rangle_{Id} \in I_{\langle Id\rangle}(G)$. The study of $I_{\langle Id\rangle}(G)$ was mainly focused on its special subset $J(G) = \{\langle g\rangle_{Id} \in I_{\langle Id\rangle}(G) | \langle g\rangle_{Id} + \langle h\rangle_{Id} \in I(G)\}$. The condition that $C_{\langle g\rangle}$ permutes with $C_{\langle h\rangle}$ was proved to be necessary for $\langle g\rangle_{Id} + \langle h\rangle_{Id} \in I(G)$, and so for $\langle g\rangle_{Id} \in J(G)$, $C_{\langle g\rangle}$ must be odd-permutable and thus odd-subnormal in $G$. These results were then used to study $J(G)$ explicitly for groups of order $pq$, $2^kp$ and dihedral groups.

The non-triviality of $J(G)$ for these several families of $G$ ensures that there is a large pool of idempotents to serve as the generator of zero-divisor codes in $F_2G$ in order to study the equivalency between the resultant codes. In search of the weight-preserving $F_2$-linear isomorphism $\varphi : F_2G_1u_1 \to F_2G_2u_2$, we instinctively concentrated on those which are expressible in terms of $\chi : G_1 \to G_2$, that is $(\sum_{g\in G_1} a_g g)\varphi = \sum_{g\in G_1} a_g \chi(g)$. The exhibition of $\varphi$ being weight-preserving $F_2$-linear isomorphic is then completely dependent on the properties of $\chi$. Precisely, the existence of a bijective $\chi$ satisfying $\chi(supp(u_1)) = supp(u_2)$ simultaneously being a $u_1$-homomorphism suffices to guarantee that $\varphi$ a weight-preserving $F_2$-linear isomorphism.

The existence of a weight-preserving $F_2$-linear isomorphism $\varphi$ can be easily shown when both the generators $u_1$ and $u_2$ are our classified idempotents. Our previous classification of $I(C_{2n})$ and $I(D_{2n})$ amalgamated into the one-to-one mapping: $\sum_{i=1}^{l} \alpha_i \langle x^{2s_i}\rangle_{Id} \in I(C_{2n})$ if and only if $\sum_{i=1}^{l} \alpha_i \langle a^{s_i}\rangle_{Id} \in I(D_{2n})$. Showing the existence of $\chi$ in (5.1), we then prove that $F_2C_{2n}(\sum_{i=1}^{l} \alpha_i \langle x^{2s_i}\rangle_{Id})$ and $F_2D_{2n}(\sum_{i=1}^{l} \alpha_i \langle a^{s_i}\rangle_{Id})$ always form a pair of equivalent ideal zero-divisor codes. Hence, by Corollary 4.6, we show the conjecture "Every group ring code in $F_2D_{2n}$ is equivalent to some group ring codes in $F_2C_{2n}$" in the cases where the code generators are idempotents in the form illustrated in Theorem 1.7.

Last but not least, the order of the generator contributed to an elegant categorization on the equivalency of $F_2C_n\langle x^s\rangle_{Id}$. If $\langle x^{s_1}\rangle_{Id}, \langle x^{s_2}\rangle_{Id} \in I_{\langle Id\rangle}(C_n)$ such that $ord(x^{s_1}) = ord(x^{s_2})$, then the desirable $\chi$ exists, resulting in $F_2C_n\langle x^{s_1}\rangle_{Id}$ and $F_2C_n\langle x^{s_2}\rangle_{Id}$ being equivalent.

**Acknowledgements** This work was supported by Universiti Sains Malaysia (USM) Research University (RU) Grant no.1001/PMATHS/8011037 and Bridging Grant no.304.PMATHS.6316013.

## References

1. Berman, S.D., On the Theory of Group Codes, Kibernetika, Vol.3, 31-39 (1967)
2. Bogart, K., Goldberg, D., Gordon, J., An Elementary Proof of the MacWilliams Theorem on Equivalence of Codes, Information and Control, Vol.37, 19-22 (1978)
3. Ferraz, R.A., Milies, C.P., Idempotents in Group Algebras and Minimal Abelian Codes, Finite Field and Their Applications, 13, 382-393 (2007)
4. Hurley, P., Hurley, T., Codes from Zero-divisor and Units in Group Rings, International Journal of Information Theory and Coding Theory, Vol.1, 57-87 (2009)
5. Hurley, T., Convolutional Codes from Units in Matrix and Group Rings, International Journal of Pure and Applied Mathematics, Vol.50, 431-463 (2009)
6. Hurley, T., Self-dual, Dual-containing and Related Quantum Code from Group Rings, CoRR, abs/0711.3983. (2007)
7. MacWilliams, F.J., Binary Codes Which Are Ideals in the Group Algebra of an Abelian Group, The Bell System Technical Journal, 987-1011 (1970)
8. Milies, C.P., Sehgal, S.K., An Introduction to Group Rings, Springer, Netherlands (2002)
9. Ong, K.L., Ang, M.H., Full Identification of Idempotents in Binary Abelian Group Rings, Journal of the Indonesian Mathematical Society, Vol.23, 67-75 (2017)
10. Ong, K.L., Ang, M.H., Study of Idempotents in Cyclic Group Rings over $F_2$, AIP Conference Proceedings 1739 (2016)
11. Robinson, D.S.J., A Course in the Theory of Groups, Springer 2nd Edition, 393-396, United States of America (1996)
12. Sahni, A., Sehgal, P.T., Minimum Cyclic Codes of Length $p^nq$, Finite Field and Their Applications, Vol.28, 1017-1036 (2012)
13. Tan, Z.S., Ang, M.H., Teh, W.C., Group Ring Codes over Dihedral Group, Malaysia Journal of Mathematical Sciences, Vol.9(S), 37-52 (2015)