International Journal of Mathematics and
Computer Science, **16**(2021), no. 3, 857–869

Complete Identification of Generators and Check Elements of Zero Divisor Codes over Cyclic Group Rings

**Andy Chuin Liang Kang, Miin Huey Ang,
Azhana Ahmad, Zhen Chuan Ng**

School of Mathematical Sciences
Universiti Sains Malaysia
11800 USM, Penang, Malaysia

email: mathamh@usm.my, AndyLiang715@gmail.com,
azhana@usm.my, zhenchuanng@usm.my

(Received February 1, 2021, Revised March 28, 2021,
Accepted May 8, 2021)

Abstract

Let F_q be a finite field with $q = p^n$ where p is a prime and C_m be a cyclic group of order m with generator g. Let u be a zero divisor in a cyclic group ring F_qC_m having W as a F_q-submodule. Then $C = Wu$ is called a zero divisor code over F_qC_m with generator u. To implement zero divisor codes in real world, each C needs a generator u as well as explicitly identifying its respective check element which is a principle zero divisor partner of u. In this paper, an algebraic study on zero divisors of F_qC_m is done by viewing each $u = \sum_{i=0}^{m-1} \alpha_i g^i \in F_qC_m$ as the polynomial $u(g) = \sum_{i=0}^{m-1} \alpha_i g^i \in F_q[g]$. It is found that $gcd(u(g), g^m - 1)$ plays a vital role in extracting important properties of zero divisors in F_qC_m. Using the obtained results, the set of all zero divisors in F_qC_m or all generators of zero divisor codes over F_qC_m is completely identified with its cardinality stated explicitly. This paper ends with an explicit identification of a check element for each zero divisor code over F_qC_m.

Key words and phrases: Cyclic Group Ring, Principal Zero Divisor Partner, Zero Divisor Code, Check Element
AMS (MOS) Subject Classifications: 94B99, 20C05
ISSN 1814-0432, 2021, http://ijmcs.future-in-tech.net

1 Introduction

Let F_q be a finite field with $q = p^n$ where p is a prime and $G = \{g_0 = 1, g_1, ..., g_{m-1}\}$ be an abelian group of order m. Then $F_qG = \{\sum_{g\in G} \alpha_g g | \alpha_g \in F_q\}$ is called a group ring of G over F_q, which has algebraic structures of both commutative ring and F_q-module. In addition, let $M_{m\times m}(F_q)$ be the ring of $m \times m$ matrices over F_q. With respect to the ordered listing of elements in G, there exists an injective homomorphism $\sigma_G : F_qG \to M_{m\times m}(F_q)$[1]. For each $a \in F_qG$, the $\sigma_G(a)$ is called the group ring matrix of a (with respect to the ordered listing G). Clearly, different ordered listings of elements in G give different group ring matrices of a. However, all group ring matrices of a share the same rank called the rank of a, denoted as $rank(a)$, that is $rank(a) = rank(\sigma_G(a))$.

Let W be a F_q-submodule of F_qG and $u \in F_qG$ be a zero divisor. Then for all $x \in W$, $f_{W,u} : W \to F_qG$ such that $(x)f_{W,u} = xu$ is an encoding linear map for a code $C = Im(f_{W,u}) = \{xu | x \in W\} = Wu$. Note that the respective code is a F_q-submodule of F_qG and it is named zero divisor code with a generator u relative to the F_q-submodule W [2].

Recall that a code with larger minimal distance can detect or correct more errors [5]. For non-isomorphic groups G of order $m \in \mathbb{N}$, with respects to a F_q-submodule W, different generators give different minimal distances for the zero divisor codes over F_qG. Hence, it is a necessity to study algebraic methods to completely identify all generators for zero divisor codes over F_qG for non-isomorphic groups G. Idempotents form a special class of zero divisors in F_qG. Recently, a complete algebraic identification of all idempotents in F_qG and some interesting algebraic results on zero divisor codes with idempotent generators have been obtained [6, 7, 8].

On the other hand, in the decoding of $C = Wu$, a check element of C is an element $v \in F_qG$ such that $C = \{a \in F_qG | av = 0\}$ [2]. In other words, for a respective received message $w \in F_qG$ if $wv \neq 0$, then clearly w is received with errors. Let $u' \in F_qG$ be a zero divisor partner of u. Then $uu' = 0$ or $\sigma_G(u)\sigma_G(u') = 0$ implies the row space of $\sigma_G(u)$ is a subspace of the null space of $\sigma_G(u')$. Thus $rank(\sigma_G(u')) \leq |G| - rank(\sigma_G(u))$ or $rank(u') \leq |G| - rank(u)$. Note that $rank(u') < |G| - rank(u)$ if and only if $C \subsetneq \{a \in F_qG | au' = 0\}$. Hence, a $u' \in F_qG$ such that $rank(u') = |G| - rank(u)$ is a natural check element of C and thus it is specifically denoted as v, called principal zero divisor partner of u [2].

From the algebraic point of view, it is interesting to investigate the family of groups that assures the existence of a principal zero divisor partner for

each zero divisor u in the respective group ring [3, 4]. Till now, it is still a great challenge to convert the obtained algebraic results into an algebraic algorithm to explicitly identify a check element for each zero divisor code over the respective group ring.

Let $C_m = \langle g \rangle = \{g^0 = 1, g, g^2, ..., g^{m-1}\}$ be a cyclic group of order m with generator g and thus $F_qC_m = \left\{\sum_{i=0}^{m-1} \alpha_i g^i | \alpha_i \in F_q\right\}$. Let $F_q[g]$ be the ring of polynomials over F_q with indeterminate g. Note that

$$\begin{aligned} F_q[g]/\langle g^m - 1\rangle &= \left\{ \left(\sum_{i=0}^{m-1} \alpha_i g^i \right) + \langle g^m - 1\rangle \middle| \alpha_i \in F_q \right\} \\ &= \left\{ \sum_{i=0}^{m-1} \left[(\alpha_i + \langle g^m - 1\rangle) \left(g^i + \langle g^m - 1\rangle \right) \right] \middle| \alpha_i \in F_q \right\}. \end{aligned}$$

As $F_q \cong \bar{F}_q = \{\alpha + \langle g^m - 1\rangle | \alpha \in F_q\}$ and $C_m \cong G = \langle g + \langle g^m - 1\rangle \rangle$, it can be seen that F_qC_m is isomorphic to $F_q[g]/\langle g^m - 1\rangle$ [9]. Throughout this paper, let $a(g) = \sum_{i=0}^{m-1} \alpha_i g^i \in F_q[g]$ be the polynomial form of a group ring element $a = \sum_{i=0}^{m-1} \alpha_i g^i \in F_qC_m$. However, any results obtained through the polynomial form will need to be reduced modulo $g^m - 1$ before it is applied into F_qC_m. In [3], Hurley proved that if $u(g)|(g^m - 1)$, then $u' \in F_qC_m$ such that $u(g)u'(g) = g^m - 1$ is a principal zero divisor partner of u.

In this paper, an algebraic method to explicitly identify a check element of $C = Wu$ (or a principal zero divisor partner of $u \in F_qC_m$) regardless of whether $u(g)$ is a divisor of $g^m - 1$ is discussed. Before that, for the completeness of our study, an algebraic method to completely identify all generators for zero divisor codes over F_qC_m or all zero divisors in F_qC_m is introduced.

2 Identification of Generators For Zero Divisor Codes Over F_qC_m

As the complete identification of generators for zero divisor codes over F_qC_m implies the complete identification of zero divisors in F_qC_m and vice-versa, a practical method is firstly developed to sort out zero divisors among non-zero elements in F_qC_m.

Let a be a non-zero element in F_qC_m. We show that the determination of whether a is a unit or a zero divisor can be done by using the greatest

common divisor of $a(g)$ and g^m-1 that is $gcd(a(g), g^m-1)$. Before that, we need the following result:

Lemma 2.1. *Let $a \in F_qC_m$. Then $gcd(a(g), g^m-1) = 1$ if and only if there exist $\beta, \eta \in F_qC_m$ such that $\beta(g)a(g) + \eta(g)(g^m-1) = 1$.*

Proof. Assume that $gcd(a(g), g^m-1) = 1$. Then from [5], it is known that there exist $\beta(g) = \sum_{i=0}^{m-1} \beta_i g^i, \eta(g) = \sum_{i=0}^{m-1} \eta_i g^i \in F_q[g]$, equivalently $\beta, \eta \in F_qC_m$, such that $\beta(g)a(g) + \eta(g)(g^m-1) = 1$. Conversely, assume that there exist $\beta, \eta \in F_qC_m$, such that $\beta(g)a(g)+\eta(g)(g^m-1) = 1$. Let $gcd(a(g), g^m-1) = d(g)$. Note that since $d(g)|a(g)$ and $d(g)|g^m-1$, then it follows that $d(g)|(\beta(g)a(g) + \eta(g)(g^m-1))$ which implies $d(g)|1$. Hence, $d(g) = 1$. □

Theorem 2.2. *Let $a \in F_qC_m - \{0\}$. Then a is a unit if and only if $gcd(a(g), g^m-1) = 1$. Otherwise, a is a zero divisor.*

Proof. By Lemma 2.1, $gcd(a(g), g^m-1) = 1$ if and only if there exist $\beta, \eta \in F_qC_m$ such that $a(g)\beta(g) + (g^m-1)\eta(g) = 1$ if and only if $a(g)\beta(g) = 1-(g^m-1)\eta(g) \equiv 1 (\text{mod } g^m-1)$ if and only if $a\beta = 1$ (recall that $F_qC_m \cong F_q[g]/\langle g^m-1\rangle$) if and only if a is a unit. As each non-zero element in F_qC_m is either a unit or a zero divisor [1], the result of a is a zero divisor if and only if $gcd(a(g), g^m-1) \neq 1$ followed. □

Using Theorem 2.2, note that $gcd(a(g), g^m-1)) \neq 1$ if and only if $1 \leq deg(a(g)) \leq m-1$ and $a(g)$ is a multiple of some irreducible factors of g^m-1. Thus it is clear that the initial step to detect all zero divisors of F_qC_m is by identifying the complete factorization of g^m-1 into product of irreducible polynomials over F_q.

Let $m \in \mathbb{N}$ such that $gcd(m, q) = 1$. Recall that for each $0 \leq j \leq m-1$, the cyclotomic coset of q modulo m containing j is $C_j = \{jq^i \text{mod } m | i = 0, 1, 2, ...\}$ [5]. The following is a result that can be used to identify all irreducible factors of g^m-1 over F_q for the case of $gcd(m, q) = 1$.

Theorem 2.3. *[5] Let $m \in \mathbb{N}-1$ such that $gcd(m, q) = 1$. Suppose that n is a positive integer satisfying $m|(q^n-1)$. Let α be a primitive element of F_{q^n} and $M_j(g) = \prod_{i \in C_j}(g-\alpha^i)$ be the minimal polynomial of α^j with respect to F_q. Let $\{s_1, ..., s_t\}$ be a complete set of representatives of cyclotomic cosets of q modulo m. Then g^m-1 has a total of t distinct monic irreducible factors over F_q where $g^m-1 = \prod_{i=1}^{t} M_{((q^n-1)s_i/m)}(g)$.*

Consider the case of $gcd(m, q) \neq 1$. Recall that for $\alpha_1, \alpha_2 \in F_q$, $(\alpha_1 + \alpha_2)^{p^\vartheta} = \alpha_1^{p^\vartheta} + \alpha_2^{p^\vartheta}$ for every $\vartheta \in \mathbb{N}$ [3]. Note that as a positive integer and

under the condition of $gcd(m,q) \neq 1$, $m = m'p^{\mu}$ for some $\mu, m' \in \mathbb{N}$ with $gcd(m',p) = 1$. Then $g^m - 1 = g^{m'p^{\mu}} - 1^{p^{\mu}} = (g^{m'} - 1)^{p^{\mu}}$.

Case 1. *$m' = 1$ that is $m = p^{\mu}$ for some $\mu \in \mathbb{N}$. Then* $g^m - 1 = g^{p^{\mu}} - 1^{p^{\mu}} = (g-1)^{p^{\mu}}$

Case 2. *$m' > 1$. Let n be a positive integer satisfying $m'|(q^n - 1)$. Then by Theorem 2.3,* $g^{m'} - 1 = \prod_{i=1}^{t} M_{((q^n-1)s_i/m')}(g)$ *and thus*

$$\begin{aligned} g^m - 1 &= g^{m'p^{\mu}} - 1^{p^{\mu}} \\ &= (g^{m'} - 1)^{p^{\mu}} \\ &= \left(\prod_{i=1}^{t} M_{((q^n-1)s_i/m')}(g) \right)^{p^{\mu}} \\ &= \prod_{i=1}^{t} \left(M_{((q^n-1)s_i/m')}(g) \right)^{p^{\mu}}. \end{aligned}$$

Hence, we have proved the following result:

Theorem 2.4. *Suppose that m is a positive integer such that $gcd(m,q) \neq 1$. Let $m = m'p^{\mu}$ for some $\mu, m' \in \mathbb{N}$ with $gcd(m',p) = 1$. Let n be a positive integer satisfying $m'|(q^n - 1)$. Then*

(i) $g^m - 1 = (g-1)^{p^{\mu}}$ *if* $m' = 1$;

(ii) $g^m - 1 = \prod_{i=1}^{t} \left(M_{((q^n-1)s_i/m')}(g) \right)^{p^{\mu}}$ *if* $m' > 1$.

From now on, let $m = m'p^{\mu}$ for some non-negative integer μ. Then $gcd(m,q) = 1$ if $\mu = 0$ or $gcd(m,q) \neq 1$ if $\mu \geq 1$. Recall from Theorem 2.4 that $g^m - 1 = \prod_{j=1}^{t} (M_j(g))^{p^{\mu}}$ with each $M_j(g)$ is a monic irreducible polynomial over F_q. For each $j \in \{1, 2, ..., t\}$, define

$$\Upsilon_j := \left\{ b(g)M_j(g) \middle| b(g) = \sum_{k=0}^{m-1-deg(M_j(g))} \epsilon_k g^k, \epsilon_k \in F_q \right\}. \qquad (2.1)$$

Note that for each $1 < s \leq p^{\mu}$,

$$\left\{ b(g)M_j(g)^s \left| b(g) = \sum_{k=0}^{m-1-s\cdot deg(M_j(g))} \epsilon_k g^k, \epsilon_k \in F_q \right. \right\}$$
$$\subset \left\{ b(g)M_j(g) \left| b(g) = \sum_{k=0}^{m-1-deg(M_j(g))} \epsilon_k g^k, \epsilon_k \in F_q \right. \right\}.$$

Hence, the set of all zero divisors in F_qC_m is $\bigcup_{j=1}^{t} \Upsilon_j - \{0\}$.

Theorem 2.5. *Let $g^m - 1 = \prod_{j=1}^{t}(M_j(g))^{p^\mu}$ where p is prime, $\mu \geq 0$ and each $M_j(g)$ is a monic irreducible polynomial over F_q. For each $j \in \{1, 2, ..., t\}$, let Υ_j be defined as in Equation (2.1). Then $Z_{F_qC_m} = \bigcup_{j=1}^{t} \Upsilon_j - \{0\}$ where $Z_{F_qC_m}$ is the set of all zero divisors in F_qC_m.*

Corollary 2.6. *The set of all generators for zero divisor codes over F_qC_m is $Z_{F_qC_m}$.*

Next, the cardinality of $Z_{F_qC_m}$ is studied. By Theorem 2.5, $|Z_{F_qC_m}| = \left|\bigcup_{j=1}^{t} \Upsilon_j - \{0\}\right|$. As $\Upsilon_{j_1} \cap \Upsilon_{j_2}$ is not necessary an empty set for all $j_1, j_2 \in \{1, 2, ..., t\}$, $|Z_{F_qC_m}| \leq \sum_{j=1}^{t} |\Upsilon_j| - 1$. Hence, inclusion-exclusion principle is used to find $|Z_{F_qC_m}|$ by expanding the notation from Equation (2.1). For each $\lambda \in \{1, 2, ..., t\}$, define

$$\Upsilon_{j_1,...,j_\lambda} := \left\{ b(g)\left(M_{j_1}(g)\cdots M_{j_\lambda}(g)\right) \left| b(g) = \sum_{k=0}^{m-1-\sum_{r=1}^{\lambda} deg(M_{j_r}(g))} \epsilon_k g^k, \epsilon_k \in F_q \right. \right\}. \tag{2.2}$$

For each $\lambda \in \{2, ..., t\}$, it is obvious that $\Upsilon_{j_1,...,j_\lambda} \subseteq \bigcap_{k=1}^{\lambda} \Upsilon_{j_k}$. Conversely, as each $M_{j_k}(g)$ is irreducible, then if $a(g) \in \bigcap_{k=1}^{\lambda} \Upsilon_{j_k}$, $a(g) = b(g)\left(M_{j_1}(g)\cdots M_{j_\lambda}(g)\right)$ for some $b(g) = \sum_{k=0}^{m-1-\sum_{r=1}^{\lambda} deg(M_{j_r}(g))} \epsilon_k g^k$. Thus for each $\lambda \in \{2, ..., t\}$, $\bigcap_{k=1}^{\lambda} \Upsilon_{j_k} \subseteq \Upsilon_{j_1,...,j_\lambda}$. Therefore, $\Upsilon_{j_1,...,j_\lambda} = \bigcap_{k=1}^{\lambda} \Upsilon_{j_k}$ for each $\lambda \in \{2, ..., t\}$.

In particular, consider the case of $\mu = 0$. Let $a(g) \in \bigcap_{j=1}^{t} \Upsilon_j$. Then as each $M_{j_k}(g)$ is irreducible and $deg\left(a(g)\right) \leq m-1$, $a(g) = b(g)\left(M_1(g)\cdots M_t(g)\right)$ implies that $b(g) = 0$. Hence, the following result is obtained:

Lemma 2.7. *Let $g^m - 1 = \prod_{j=1}^{t}\left(M_j(g)\right)^{p^\mu}$ where p is prime, $\mu \geq 0$ and each $M_j(g)$ is a monic irreducible polynomial over F_q. Let Υ_j be defined*

as in Equation (2.1) for each $j \in \{1, 2, ..., t\}$ *and* $\Upsilon_{j_1,...,j_\lambda}$ *be defined as in Equation (2.2) for each* $\lambda \in \{1, 2, ..., t\}$. *Then* $\bigcap_{k=1}^{\lambda} \Upsilon_{j_k} = \Upsilon_{j_1,...,j_\lambda}$ *for each* $\lambda \in \{2, ..., t\}$. *In addition, if* $\mu = 0$, *then* $\bigcap_{j=1}^{t} \Upsilon_j = \{0\}$.

The next result gives the value of $|Z_{F_qC_m}|$.

Theorem 2.8. *Let* $g^m - 1 = \prod_{j=1}^{t} (M_j(g))^{p^\mu}$ *where* p *is prime,* $\mu \geq 0$ *and each* $M_j(g)$ *is a monic irreducible polynomial over* F_q. *Then* $|Z_{F_qC_m}| = \left(\sum_{\lambda=0}^{t}(-1)^{\lambda+1}\left(\sum_{1\leq j_1<\cdots<j_\lambda\leq t} q^{m-\sum_{r=1}^{\lambda} deg(M_{j_r}(g))}\right)\right) - 1$.

Proof. By Theorem 2.5, $|Z_{F_qC_m}| = |\bigcup_{j=1}^{t} \Upsilon_j - \{0\}|$.Then by inclusion-exclusion principle and Lemma 2.7, we have

$$\begin{aligned}
\left|\bigcup_{j=1}^{t} \Upsilon_j\right| &= \sum_{j=1}^{t} |\Upsilon_j| - \sum_{1\leq j_1<j_2\leq t} \left|\bigcap_{k=1}^{2} \Upsilon_{j_k}\right| + \sum_{1\leq j_1<j_2<j_3\leq t} \left|\bigcap_{k=1}^{3} \Upsilon_{j_k}\right| - ... + (-1)^{t+1} \left|\bigcap_{j=1}^{t} \Upsilon_j\right| \\
&= \sum_{j=1}^{t} |\Upsilon_j| - \sum_{1\leq j_1<j_2\leq t} |\Upsilon_{j_1,j_2}| + \sum_{1\leq j_1<j_2<j_3\leq t} |\Upsilon_{j_1,j_2,j_3}| - ... + (-1)^{t+1} |\Upsilon_{1,2,...,t}| \\
&= \sum_{\lambda=1}^{t}(-1)^{\lambda+1}\left(\sum_{1\leq j_1<\cdots<j_\lambda\leq t} |\Upsilon_{j_1,...,j_\lambda}|\right) \\
&= \sum_{\lambda=1}^{t}(-1)^{\lambda+1}\left(\sum_{1\leq j_1<\cdots<j_\lambda\leq t} q^{m-\sum_{r=1}^{\lambda} deg(M_{j_r}(g))}\right).
\end{aligned}$$

Thus,

$$\begin{aligned}
\left|Z_{F_qC_m}\right| &= \left|\bigcup_{j=1}^{t} \Upsilon_j - \{0\}\right| \\
&= \left(\sum_{\lambda=1}^{t}(-1)^{\lambda+1}\left(\sum_{1\leq j_1<\cdots<j_\lambda\leq t} q^{m-\sum_{r=1}^{\lambda} deg(M_{j_r}(g))}\right)\right) - 1.
\end{aligned}$$

□

For the case of $gcd(m, q) \neq 1$, recall that $m = m'p^\mu$ for some $\mu \geq 1$ with $gcd(m', p) = 1$. The following result gives the relation between $\left|Z_{F_qC_m}\right|$ and $\left|Z_{F_qC_{m'}}\right|$:

Corollary 2.9. *Let* $m = m'p^\mu \in \mathbb{N}$ *such that* p *is prime and* $\mu > 0$. *Then* $\left|Z_{F_qC_m}\right| = q^{(p^\mu-1)m'}\left(\left|Z_{F_qC_{m'}}\right| + 1\right) - 1$.

Proof. Recall from Theorem 2.8 that

$$|Z_{F_qC_m}| = \left(\sum_{\lambda=1}^{t}(-1)^{\lambda+1}\left(\sum_{1\le j_1<\cdots<j_\lambda\le t} q^{m-\sum_{r=1}^{\lambda} deg(M_{j_r}(g))}\right)\right) - 1 \text{ and}$$

$$|Z_{F_qC_{m'}}| = \left(\sum_{\lambda=1}^{t}(-1)^{\lambda+1}\left(\sum_{1\le j_1<\cdots<j_\lambda\le t} q^{m'-\sum_{r=1}^{\lambda} deg(M_{j_r}(g))}\right)\right) - 1.$$

Then

$$\begin{aligned}
\left|Z_{F_qC_m}\right| &= \left(\sum_{\lambda=1}^{t}(-1)^{\lambda+1}\left(\sum_{1\le j_1<\cdots<j_\lambda\le t} q^{p^\mu m'-\sum_{r=1}^{\lambda} deg(M_{j_r}(g))}\right)\right) - 1 \\
&= \left(\sum_{\lambda=1}^{t}(-1)^{\lambda+1}\left(\sum_{1\le j_1<\cdots<j_\lambda\le t} q^{(p^\mu-1)m'} q^{m'-\sum_{r=1}^{\lambda} deg(M_{j_r}(g))}\right)\right) - \\
&\quad q^{(p^\mu-1)m'} + q^{(p^\mu-1)m'} - 1 \\
&= q^{(p^\mu-1)m'}\left(\left(\sum_{\lambda=1}^{t}(-1)^{\lambda+1}\left(\sum_{1\le j_1<\cdots<j_\lambda\le t} q^{m'-\sum_{r=1}^{\lambda} deg(M_{j_r}(g))}\right) - 1\right) + 1\right) - 1 \\
&= q^{(p^\mu-1)m'}\left(\left|Z_{F_qC_{m'}}\right| + 1\right) - 1.
\end{aligned}$$

□

Example 2.10. *Consider F_2C_3 with $gcd(3,2) = 1$. By Theorem 2.3, $g^3 - 1 = (g^2+g+1)(g+1)$ with $M_1(g) = g^2+g+1$ and $M_2(g) = g+1$ are all monic irreducible polynomials over F_2. Thus $\Upsilon_1 = \{g^2+g+1, 0\}$ and $\Upsilon_2 = \{g+1, g^2+1, g^2+g, 0\}$ as defined in Equation (2.1). Let $\chi_1 = \Upsilon_1 - \{0\} = \{g^2+g+1\}$ and $\chi_2 = \Upsilon_2 - \Upsilon_1 = \{g+1, g^2+1, g^2+g\}$. Note that $\chi_1 \cap \chi_2 = \emptyset$ and $\bigcup_{j=1}^{2}\chi_j = \bigcup_{j=1}^{2}\Upsilon_j - \{0\}$ that is $\{\chi_1, \chi_2\}$ forms a partition of $Z_{F_2C_3}$ by Theorem 2.5. Thus $|Z_{F_2C_3}| = 4$ with $Z_{F_2C_3} = \{g+1, g^2+1, g^2+g, g^2+g+1\}$. Note that this result is consistent with the value of $|Z_{F_2C_3}|$ obtained using Theorem 2.8 that is*

$$\begin{aligned}
|Z_{F_2C_3}| &= \left(2^{3-deg(M_1(g))} + 2^{3-deg(M_2(g))}\right) - \left(2^{3-deg(M_1(g))-deg(M_2(g))}\right) - 1 \\
&= (2+2^2) - 2^0 - 1 \\
&= 4.
\end{aligned}$$

Therefore, by Corollary 2.6, $Z_{F_2C_3} = \{g+1, g^2+1, g^2+g, g^2+g+1\}$ is the set of all generators of zero divisor codes over F_2C_3.

Let $W = F_2C_3$. It can be verified that there are two distinct zero divisor codes over F_2C_3 namely $C_1 = W(g+1) = W(g^2+1) = W(g^2+g) = \{0, g+1, g^2+g, g^2+1\}$ and $C_2 = W(g^2+g+1) = \{0, g^2+g+1\}$ with the minimal distance of C_1 and C_2 are 2 and 3 respectively [5]. Hence, in practice C_2 is better than C_1.

Example 2.11. *Consider F_2C_{12}. Recall that $g^3 - 1 = (g^2+g+1)(g+1)$ from Example 2.10. Note that $gcd(2,12) = 2$ and $12 = 4 \times 3$. Then by Theorem 2.4(ii), $g^{12} - 1 = (g^2+g+1)^4(g+1)^4$. By Corollary 2.9, $|Z_{F_2C_{12}}| = 2^{(4-1)\times 3}(|Z_{F_2C_3}| + 1) - 1 = 2^9(4+1) - 1 = 2559$. Note that*

$$\Upsilon_1 = \left\{ b(g)(g^2+g+1) \middle| b(g) = \sum_{k=0}^{9} \epsilon_k g^k, \epsilon_k \in F_2 \right\} \text{ and}$$

$$\Upsilon_2 = \left\{ b(g)(g+1) \middle| b(g) = \sum_{k=0}^{10} \epsilon_k g^k, \epsilon_k \in F_2 \right\}.$$

Hence, similar to Example 2.10, $Z_{F_2C_{12}} = \chi_1 \cup \chi_2$ is the set of all generators of zero divisor codes over F_2C_{12} where $\chi_1 \cap \chi_2 = \emptyset$ and

$$\chi_1 = \Upsilon_1 - \{0\} = \left\{ b(g)(g^2+g+1) \middle| b(g) = \sum_{k=0}^{9} \epsilon_k g^k, \epsilon_k \in F_2, b(g) \neq 0 \right\};$$

$$\chi_2 = \Upsilon_2 - \Upsilon_1$$
$$= \left\{ b(g)(g+1) \middle| b(g) = \sum_{k=0}^{10} \epsilon_k g^k, \epsilon_k \in F_2, b(g) \neq \left(\sum_{l=0}^{8} \delta_l g^l \right)(g^2+g+1), \delta_l \in F_2 \right\}$$

Then $|\chi_1| = 2^{10} - 1 = 1023$ and $|\chi_2| = 2^{11} - 2^9 = 1536$. Note that $|\chi_1| + |\chi_2| = 1023 + 1536 = 2559$ is consistent with $|Z_{F_2C_{12}}|$ obtained using Corollary 2.9.

3 Identification of Check Elements For Zero Divisor Codes Over F_qC_m

Throughout this section, let $u \in F_qC_m$ be a zero divisor with $d(g) = gcd(u(g), g^m - 1)$ and $C = Wu$ is its corresponding zero divisor code. Then by Theorem 2.2, $d(g) \neq 1$. The following result shows that u is a zero divisor implies d is also a zero divisor.

Proposition 3.1. *Let $u \in F_qC_m$ such that u is a zero divisor and $d(g) = gcd(u(g), g^m - 1)$. Then d is a zero divisor in F_qC_m.*

Proof. Note that $deg(d(g)) \leq deg(u(g))$ as $d(g) = gcd(u(g), g^m - 1)$. It is then clear that $gcd(d(g), g^m - 1) = d(g) \neq 1$. Thus by Theorem 2.2, d is a zero divisor in F_qC_m. □

Next, the remaining discussion is proceed toward developing a method to explicitly identify a check element for C. Note that as $d(g)$ is a divisor of both $g^m - 1$ and $u(g)$, there exist $d'(g), d''(g) \in F_q[g]$ such that

$$d(g)d'(g) = g^m - 1 \tag{3.1}$$

and

$$d(g)d''(g) = u(g). \tag{3.2}$$

By comparing the degrees of polynomials on the both sides of the Equation 3.1 and Equation 3.2 respectively, it is clear that $d', d'' \in F_qC_m$.

Note that d' is a zero divisor partner of d as Equation (3.1) in $F_q[g]$ implies $dd' = 0$ in F_qC_m. In addition, d' is a principal zero divisor partner of d by Equation (3.1) [3]. On the other hand, by Equation (3.2), $gcd(u(g), g^m-1) = gcd(d(g)d''(g), g^m-1) = d(g)$ which implies that $d''(g)$ and g^m-1 are coprime. Then by Theorem 2.2, d'' is a unit. Therefore, we have proven the following result:

Lemma 3.2. *Let $u \in F_qC_m$ such that u is a zero divisor and $d(g) = gcd(u(g), g^m - 1)$.*

(i) If $d(g)d'(g) = g^m-1$, then $d' \in F_qC_m$ is a principal zero divisor partner of d;

(ii) If $d(g)d''(g) = u(g)$, then $d'' \in F_qC_m$ is a unit.

Our next result shows that regardless of whether $u(g)$ divides $g^m - 1$, both u and d share the same set of principal zero divisor partners.

Theorem 3.3. *Let $u \in F_qC_m$ such that u is a zero divisor and $d(g) = gcd(u(g), g^m - 1)$. Then $d' \in F_qC_m$ is a check element of $C = Wu$ if and only if d' is a principal zero divisor partner of d.*

Proof. Let $d'' \in F_qC_m$ such that $u = dd''$. By Lemma 3.2(ii), d'' is a unit. Thus the corresponding group ring matrix $\sigma_{C_m}(d'')$ is also a unit. Hence, we have

$$rank(u) = rank(\sigma_{C_m}(u)) = rank(\sigma_{C_m}(d)\sigma_{C_m}(d'')) = rank(\sigma_{C_m}(d)) = rank(d). \tag{3.3}$$

Assume that d' is a principal zero divisor partner of d. Then $dd' = 0$ and $rank(d) + rank(d') = |C_m|$. Note that $ud' = dd''d' = (dd')d'' = 0$ and by Equation (3.3), $rank(u) + rank(d') = rank(d) + rank(d') = |C_m|$. Conversely, assume that d' is a check element of C. Then $ud' = 0$ and $rank(u) + rank(d') = |C_m|$. Note that $ud' = dd''d' = (dd')d'' = 0$. Since d'' is a unit, then $dd' = 0$. In addition, by Equation (3.3), $rank(d) + rank(d') = rank(u) + rank(d') = |C_m|$. □

Lastly, the following result gives a method to explicitly identify a check element for each zero divisor code over F_qC_m.

Theorem 3.4. *Let $u \in F_qC_m$ such that u is a zero divisor and $d(g) = gcd(u(g), g^m - 1)$. Then $v \in F_qC_m$ is a check element of $C = Wu$ if $d(g)v(g) = g^m - 1$.*

Proof. Suppose that $v \in F_qC_m$ is a zero divisor partner of u such that $d(g)v(g) = g^m - 1$. Then by Lemma 3.2(i), v is a principal zero divisor partner of d and thus v is a check element of C by Theorem 3.3. □

In short, using Theorem 3.3 and Theorem 3.4, an algebraic algorithm to explicitly identify a check element of a zero divisor code over F_qC_m is designed as follows:

Algorithm 3.5. *Let $C = Wu$ be a zero divisor code over F_qC_m. For each group ring element $a = \sum_{i=0}^{m-1} \alpha_i g^i \in F_qC_m$, recall that $a(g) = \sum_{i=0}^{m-1} \alpha_i g^i \in F_q[g]$ represents the polynomial form of a in $F_q[g]$ and vice-versa.*

Step 1: Find $d(g) = gcd(u(g), g^m - 1)$ using Euclidean Algorithm.

Step 2: Find $d' \in F_qC_m$ such that $d(g)d'(g) = g^m - 1$.

Then d' is a check element of C.

Example 3.6. *Let $C = Wu$ be a zero divisor code over F_2C_{12} with $u = 1 + g + g^2 + g^5 + g^8$.*

Step 1: By using Euclidean Algorithm, we have

$$gcd(u(g), g^{12} - 1) = 1 + g + g^2.$$

Step 2: Using long division,

$$(1+g+g^3+g^4+g^6+g^7+g^9+g^{10})(1+g+g^2) = g^{12}-1.$$

Thus $v = 1+g+g^3+g^4+g^6+g^7+g^9+g^{10} \in F_2C_{12}$ *is a check element for* C *by Algorithm 3.5. Note that* $uv = 0$ *with*

$$\sigma_{C_{12}}(u) = \begin{pmatrix} 1&1&1&0&0&1&0&0&1&0&0&0\\ 0&1&1&1&0&0&1&0&0&1&0&0\\ 0&0&1&1&1&0&0&1&0&0&1&0\\ 0&0&0&1&1&1&0&0&1&0&0&1\\ 1&0&0&0&1&1&1&0&0&1&0&0\\ 0&1&0&0&0&1&1&1&0&0&1&0\\ 0&0&1&0&0&0&1&1&1&0&0&1\\ 1&0&0&1&0&0&0&1&1&1&0&0\\ 0&1&0&0&1&0&0&0&1&1&1&0\\ 0&0&1&0&0&1&0&0&0&1&1&1\\ 1&0&0&1&0&0&1&0&0&0&1&1\\ 1&1&0&0&1&0&0&1&0&0&0&1 \end{pmatrix} \text{ and}$$

$$\sigma_{C_{12}}(v) = \begin{pmatrix} 1&1&0&1&1&0&1&1&0&1&1&0\\ 0&1&1&0&1&1&0&1&1&0&1&1\\ 1&0&1&1&0&1&1&0&1&1&0&1\\ 1&1&0&1&1&0&1&1&0&1&1&0\\ 0&1&1&0&1&1&0&1&1&0&1&1\\ 1&0&1&1&0&1&1&0&1&1&0&1\\ 1&1&0&1&1&0&1&1&0&1&1&0\\ 0&1&1&0&1&1&0&1&1&0&1&1\\ 1&0&1&1&0&1&1&0&1&1&0&1\\ 1&1&0&1&1&0&1&1&0&1&1&0\\ 0&1&1&0&1&1&0&1&1&0&1&1\\ 1&0&1&1&0&1&1&0&1&1&0&1 \end{pmatrix}.$$

It can be verified that $rank(\sigma_{C_{12}}(u)) = 10$ *and* $rank(\sigma_{C_{12}}(v)) = 2$. *Hence*

$$rank(u) + rank(v) = rank(\sigma_{C_{12}}(u)) + rank(\sigma_{C_{12}}(v)) = 12 = |C_{12}|.$$

Therefore, $v = 1+g+g^3+g^4+g^6+g^7+g^9+g^{10}$ *is a check element of* $C = W(1+g+g^2+g^5+g^8)$ *over* F_2C_{12}. *Hence,* $g^2+g^5+g^8 \in F_2C_{12}$ *but* $g^2+g^5+g^8 \notin C$ *as*

$$(g^2+g^5+g^8)(1+g+g^3+g^4+g^6+g^7+g^9+g^{10}) = 1+g^2+g^3+g^5+g^6+g^8+g^9+g^{11} \neq 0.$$

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

References

[1] T. Hurley, Group rings and rings of matrices, Int. J. Pure Appl. Math, **31,** no. 3, (2006), 319-335.

[2] P. Hurley and T. Hurley, Module codes in group rings, 2007 IEEE International Symposium on Information Theory, (2017), 1981-1985.

[3] P. Hurley and T. Hurley, Codes from zero-divisors and units in group rings, Int. J. Information and Coding Theory, **1,** no. 1, (2009), 57-87.

[4] S. Jitman, S. Ling, H. Liu and X. Xie, Checkable codes from group rings, arXiv preprint arXiv:1012.5498 (2010).

[5] S. Ling and C. Xing, Coding theory: a first course, 2004.

[6] K. L. Ong and M. H. Ang, Study of idempotents in cyclic group rings over F_2, AIP Conference Proceedings, **1739,** no. 1, (2016), p.020011.

[7] K. L. Ong and M. H. Ang, Full Identification of Idempotens in Binary Abelian Group Rings, Journal of the Indonesian Mathematical Society, **23,** no. 2, (2017), 67-75.

[8] K. L. Ong and M. H. Ang, On equivalency of zero-divisor codes via classifying their idempotent generator, Des. Codes Cryptogr, **88,** (2020), 2051-2065.

[9] D. S. Passman, The algebraic structure of group rings, 1977.