




# Composite matrices from group rings, composite $G$ -codes and constructions of self-dual codes

Steven T. Dougherty<sup>1</sup> · Joe Gildea<sup>2</sup> · Adrian Korban<sup>2</sup>  · Abidin Kaya<sup>3</sup>

Received: 25 February 2020 / Revised: 9 February 2021 / Accepted: 17 April 2021 / Published online: 19 May 2021  
© The Author(s) 2021

## Abstract

In this work, we define composite matrices which are derived from group rings. We extend the idea of  $G$ -codes to composite  $G$ -codes. We show that these codes are ideals in a group ring, where the ring is a finite commutative Frobenius ring and  $G$  is an arbitrary finite group. We prove that the dual of a composite  $G$ -code is also a composite  $G$ -code. We also define quasi-composite  $G$ -codes. Additionally, we study generator matrices, which consist of the identity matrices and the composite matrices. Together with the generator matrices, the well known extension method, the neighbour method and its generalization, we find extremal binary self-dual codes of length 68 with new weight enumerators for the rare parameters  $\gamma = 7, 8$  and  $9$ . In particular, we find 49 new such codes. Moreover, we show that the codes we find are inaccessible from other construction

**Keywords** Composite matrices · Group rings · Composite  $G$ -codes · Self-orthogonal composite  $G$ -codes · Codes over rings · Self-dual codes

**Mathematics Subject Classification** 94B05 · 16S34

## 1 Introduction

Recently, the authors in [13] have defined  $G$ -codes which are ideals in a group ring, where the ring is a finite commutative Frobenius ring and  $G$  is an arbitrary finite group. This idea is based on applying the matrix  $\sigma(v)$ , where  $v$  is a group ring element, which was first introduced in [21]. In another recent paper [19], the authors also apply the matrix  $\sigma(v)$  to

---

Communicated by V. A. Zinoviev.

✉ Adrian Korban  
adrian3@windowslive.com

<sup>1</sup> Department of Mathematics, University of Scranton, Scranton, PA 18510, USA

<sup>2</sup> Department of Mathematical and Physical Sciences, University of Chester, Thornton Science Park, Pool Ln, Chester CH2 4NU, England

<sup>3</sup> Harmony School of Technology, Houston TX 77038, USA

form generator matrices of the form  $[I \mid \sigma(v)]$ , where  $I$  is the identity matrix, to search for extremal self-dual codes.

In [10] and [11], the authors amend the generator matrices of the form  $[I \mid \sigma(v)]$ . Namely, they replace the matrices  $\sigma(v)$  with more complex matrices and call these the composite constructions. The authors define a number of composite constructions which they apply to search for extremal self-dual codes, but no general theory is given. Later in [9], the authors generalize the idea of composite constructions, amend the matrix  $\sigma(v)$  and define the composite constructions, which they also call the composite matrices, in a more general and rigorous way.

In this work, we look at the composite matrices and compare them to the matrices obtained from  $\sigma(v)$ . We look at when these matrices are equivalent and when they are not. We next apply the more general and rigorous definition of the composite matrices to define composite  $G$ -codes. This is an extension of  $G$ -codes mentioned earlier. We show that these codes are ideals in the group ring, and that the dual of a composite  $G$ -code is also a composite  $G$ -code. Moreover, we show when the composite  $G$ -codes are self-orthogonal and self-dual. Additionally, we define quasi-composite  $G$ -codes and extend some known results to quasi  $G$ -codes.

We generalize the theory of the composite constructions defined in [10] and [11]. Namely, we show in general when and under what conditions such matrices produce self-dual codes, rather than showing it for individual cases as in [10] and [11]. Lastly in this paper, we combine the ideas of composite matrices, the well known extension method and the neighbour construction and its generalization (see [18] for details), to search for extremal binary self-dual codes of length 68. As a result, we obtain 49 such codes with parameters that were not known in the literature before.

The rest of the work is organized as follows. In Sect. 2, we give preliminary definitions and results on codes, group rings and special matrices. We also recall the construction of  $G$ -codes from [13]. In Sect. 3, we define the composite matrix which was introduced in [9] and compare it with the matrix  $\sigma(v)$ . In Sect. 4, we define the composite  $G$ -codes and show that these are ideals in the group ring. In Sect. 5, we study when the composite  $G$ -codes are self-orthogonal and self-dual. Section 6 consists of a study of quasi-composite  $G$ -codes. In Sect. 7, we generalize the theory of the composite constructions from [10] and [11]. Additionally, we find new extremal self-dual binary codes of length 68. We finish with concluding remarks and directions for possible future research.

## 2 Preliminaries

### 2.1 Codes, group rings and special matrices

We begin by recalling the standard definitions from coding theory. In this paper, all rings are assumed to be commutative, finite, Frobenius rings with a multiplicative identity. Denote the character module of  $R$  by  $\widehat{R}$ . A code  $C$  of length  $n$  over a Frobenius ring  $R$  is a subset of  $R^n$ . For a finite ring  $R$  the following are equivalent:

- (1)  $R$  is a Frobenius ring;
- (2) As a left module,  $\widehat{R} \cong {}_R R$ ;
- (3) As a right module  $\widehat{R} \cong R_R$ .

We consider codes over Frobenius rings since such rings have good duality properties which are reflected by the equivalent statements above. If the code is a submodule of  $R^n$ ,

then we say that the code is linear. For a full description of Frobenius rings and codes over Frobenius rings, see [5]. Elements of the code  $C$  are called codewords of  $C$ . Let  $\mathbf{x} = (x_1, x_2, \dots, x_n)$  and  $\mathbf{y} = (y_1, y_2, \dots, y_n)$  be two elements of  $R^n$ . The duality is understood in terms of the Euclidean inner product, namely:

$$\langle \mathbf{x}, \mathbf{y} \rangle_E = \sum x_i y_i.$$

The dual  $C^\perp$  of the code  $C$  is defined as

$$C^\perp = \{ \mathbf{x} \in R^n \mid \langle \mathbf{x}, \mathbf{y} \rangle_E = 0 \text{ for all } \mathbf{y} \in C \}.$$

We say that  $C$  is self-orthogonal if  $C \subseteq C^\perp$  and is self-dual if  $C = C^\perp$ .

We next recall the standard definitions and notations for group rings. Let  $RG$  denote the group ring of the group  $G$  over the ring  $R$ . A non-zero element  $z$  in a ring  $R$  is said to be a zero-divisor in  $R$  if and only if there exists a non-zero element  $r \in R$  with  $z * r = 0$ . When  $R$  has an identity  $1_R$ , we say  $u$  is a unit in  $R$  if and only if there exists an element  $w \in R$  with  $u * w = 1_R$ . The group of units of  $R$  is denoted by  $U(R)$ . Let  $R_{n \times n}$  denote the ring of  $n \times n$  matrices with coefficients from  $R$ . While group rings can be given for infinite rings and infinite groups, we are only concerned with group rings where both the ring and the group are finite. Let  $G$  be a finite group of order  $n$ , then the group ring  $RG$  consists of  $\sum_{i=1}^n \alpha_i g_i$ ,  $\alpha_i \in R, g_i \in G$ .

Addition in the group ring is done by coordinate addition, namely

$$\sum_{i=1}^n \alpha_i g_i + \sum_{i=1}^n \beta_i g_i = \sum_{i=1}^n (\alpha_i + \beta_i) g_i. \tag{1}$$

The product of two elements in a group ring is given by

$$\left( \sum_{i=1}^n \alpha_i g_i \right) \left( \sum_{j=1}^n \beta_j g_j \right) = \sum_{i,j} \alpha_i \beta_j g_i g_j. \tag{2}$$

It follows that the coefficient of  $g_k$  in the product is  $\sum_{g_i g_j = g_k} \alpha_i \beta_j$ . For more details on group rings, see [25] and [26].

A right circulant matrix is one where each row is shifted one element to the right relative to the preceding row. Since we shall always shift to the right in this work, we shall simply call it a circulant matrix. We label the circulant matrix as  $A = \text{circ}(\alpha_1, \alpha_2, \dots, \alpha_n)$ , where  $\alpha_i$  are rings elements. The transpose of a matrix  $A$ , denoted by  $A^T$ , is a matrix whose rows are the columns of  $A$ , that is  $A_{ij}^T = A_{ji}$ .

### 2.2 G-codes

The following matrix construction was given by Hurley in [21]. The same matrix construction was used to study group codes over commutative Frobenius rings in [13]. Let  $R$  be a finite commutative Frobenius ring and let  $G = \{g_1, g_2, \dots, g_n\}$  be a group of order  $n$ . Let  $v = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \dots + \alpha_{g_n} g_n \in RG$ . Define the matrix  $\sigma(v) \in M_n(R)$  to be

$$\sigma(v) = \begin{pmatrix} \alpha_{g_1^{-1} g_1} & \alpha_{g_1^{-1} g_2} & \alpha_{g_1^{-1} g_3} & \dots & \alpha_{g_1^{-1} g_n} \\ \alpha_{g_2^{-1} g_1} & \alpha_{g_2^{-1} g_2} & \alpha_{g_2^{-1} g_3} & \dots & \alpha_{g_2^{-1} g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1} g_1} & \alpha_{g_n^{-1} g_2} & \alpha_{g_n^{-1} g_3} & \dots & \alpha_{g_n^{-1} g_n} \end{pmatrix}. \tag{3}$$

We note that the elements  $g_1^{-1}, g_2^{-1}, \dots, g_n^{-1}$  are the elements of the group  $G$  in a some given order. For a given element  $v \in RG$ , we define the  $G$ -code over the ring  $R$  :

$$C(v) = \langle \sigma(v) \rangle, \tag{4}$$

where this indicates that the code is formed by taking the row space of  $\sigma(v)$  over the ring  $R$ . It has been shown that  $C(v)$  corresponds to an ideal in the group ring  $RG$ .

### 3 The composite $\Omega(v)$ matrix

In this section, we define the composite matrix  $\Omega(v)$  which was first introduced in [9] and compare it with the matrix  $\sigma(v)$ .

Let  $R$  be a finite commutative Frobenius ring. Let  $\{g_1, g_2, \dots, g_n\}$  be a fixed listing of the elements of  $G$ . Let  $\{(h_i)_1, (h_i)_2, \dots, (h_i)_r\}$  be a fixed listing of the elements of  $H_i$ , where  $H_i$  is any group of order  $r$ . Let  $r$  be a factor of  $n$  with  $n > r$  and  $n, r \neq 1$ . Also, let  $G_r$  be a subset of  $G$  containing  $r$  distinct elements of  $G$ . Define the following map:

$$\begin{aligned} \phi : H_i &\mapsto G_r \\ (h_i)_1 &\xrightarrow{\phi} g_{j-1}g_k \\ (h_i)_2 &\xrightarrow{\phi} g_{j-1}g_{k+1} \\ &\vdots \qquad \qquad \qquad \vdots \\ (h_i)_r &\xrightarrow{\phi} g_{j-1}g_{k+(r-1)}. \end{aligned}$$

It was shown in [9] that the map  $\phi$  is a bijection.

Let  $v = \alpha_{g_1}g_1 + \alpha_{g_2}g_2 + \dots + \alpha_{g_n}g_n \in RG$ . Define the matrix  $\Omega(v) \in M_n(R)$  to be

$$\Omega(v) = \begin{pmatrix} A_1 & A_2 & A_3 & \dots & A_{\frac{n}{r}} \\ A_{\frac{n}{r}+1} & A_{\frac{n}{r}+2} & A_{\frac{n}{r}+3} & \dots & A_{\frac{2n}{r}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ A_{\frac{(r-1)n}{r}+1} & A_{\frac{(r-1)n}{r}+2} & A_{\frac{(r-1)n}{r}+3} & \dots & A_{\frac{n^2}{r^2}} \end{pmatrix}, \tag{5}$$

where at least one block has the following form:

$$A_l = \begin{pmatrix} \alpha_{g_j^{-1}g_k} & \alpha_{g_j^{-1}g_{k+1}} & \dots & \alpha_{g_j^{-1}g_{k+(r-1)}} \\ \alpha_{g_{j+1}^{-1}g_k} & \alpha_{g_{j+1}^{-1}g_{k+1}} & \dots & \alpha_{g_{j+1}^{-1}g_{k+(r-1)}} \\ \alpha_{g_{j+2}^{-1}g_k} & \alpha_{g_{j+2}^{-1}g_{k+1}} & \dots & \alpha_{g_{j+2}^{-1}g_{k+(r-1)}} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_{j+r-1}^{-1}g_k} & \alpha_{g_{j+r-1}^{-1}g_{k+1}} & \dots & \alpha_{g_{j+r-1}^{-1}g_{k+(r-1)}} \end{pmatrix},$$

and the other blocks are of the form:

$$A'_l = \begin{pmatrix} \alpha_{g_j^{-1}g_k} & \alpha_{g_j^{-1}g_{k+1}} & \cdots & \alpha_{g_j^{-1}g_{k+(r-1)}} \\ \alpha_{\phi_l((h_i)_2^{-1}(h_i)_1)} & \alpha_{\phi_l((h_i)_2^{-1}(h_i)_2)} & \cdots & \alpha_{\phi_l((h_i)_2^{-1}(h_i)_r)} \\ \alpha_{\phi_l((h_i)_3^{-1}(h_i)_1)} & \alpha_{\phi_l((h_i)_3^{-1}(h_i)_2)} & \cdots & \alpha_{\phi_l((h_i)_3^{-1}(h_i)_r)} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{\phi_l((h_i)_r^{-1}(h_i)_1)} & \alpha_{\phi_l((h_i)_r^{-1}(h_i)_2)} & \cdots & \alpha_{\phi_l((h_i)_r^{-1}(h_i)_r)} \end{pmatrix},$$

where in both cases, when  $l = 1$  then  $j = 1, k = 1$ , when  $l = 2$  then  $j = 1, k = r + 1$ , when  $l = 3$  then  $j = 1, k = 2r + 1, \dots$  when  $l = \frac{n}{r}$  then  $j = 1, k = n - r + 1$ . When  $l = \frac{n}{r} + 1$  then  $j = r + 1, k = 1$ , when  $l = \frac{n}{r} + 2$  then  $j = r + 1, k = r + 1$ , when  $l = \frac{n}{r} + 3$  then  $j = r + 1, k = 2r + 1, \dots$  when  $l = \frac{2n}{r}$  then  $j = r + 1, k = n - r + 1, \dots$ , and so on.

We note that if the above matrix  $\Omega(v)$  consists of blocks which are of the  $A_l$  form only, then it is the same as the matrix  $\sigma(v)$  from [21]. Therefore, from now on we assume that the matrix  $\Omega(v)$  consists of at least one block of the  $A'_l$  form. It is also clear that the matrix  $\Omega(v)$  cannot be constructed when the order of the group  $G$  is odd. In each block, the first row consists of  $r$  distinct elements of  $G$ . The map  $\phi_l$  is applied in individual blocks which means we can employ  $\frac{n^2}{r^2}$  different maps  $\phi_l$  and  $\frac{n^2}{r^2}$  different groups of order  $r$  (if that many exist). This is the advantage of our construction over the matrix  $\sigma(v)$ , namely, by employing different groups of order  $r$  and by applying the maps  $\phi_l$  in individual blocks, we construct more complex matrices over the ring  $R$ . We call the matrix  $\Omega(v)$  the composite  $G$ -matrix.

The rows of the matrix  $\sigma(v)$  in [21] consist of the vectors that correspond to the elements  $hv$  in  $RG$  where  $h$  is any element of  $G$ . This is not the case in the composite matrix  $\Omega(v)$ .

**Example 1** Let  $G = \langle x, y \mid x^4 = y^2 = 1, x^y = x^{-1} \rangle \cong D_8$ . Let  $v = \alpha_1 + \alpha_x x + \alpha_{x^2} x^2 + \alpha_{x^3} x^3 + \alpha_y y + \alpha_{xy} xy + \alpha_{x^2 y} x^2 y + \alpha_{x^3 y} x^3 y \in RD_8$ , where  $\alpha_{g_i} \in R$ . Let  $H_1 = \langle a, b \mid a^2 = b^2 = 1, ab = ba \rangle \cong C_2 \times C_2$ . We now define the composite matrix as:

$$\Omega(v) = \begin{pmatrix} A'_1 & A'_2 \\ A_3 & A_4 \end{pmatrix} = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \alpha_{g_1^{-1}g_3} & \alpha_{g_1^{-1}g_4} & \alpha_{g_1^{-1}g_5} & \alpha_{g_1^{-1}g_6} & \alpha_{g_1^{-1}g_7} & \alpha_{g_1^{-1}g_8} \\ \alpha_{\phi_1((h_1)_2^{-1}(h_1)_1)} & \alpha_{\phi_1((h_1)_2^{-1}(h_1)_2)} & \alpha_{\phi_1((h_1)_2^{-1}(h_1)_3)} & \alpha_{\phi_1((h_1)_2^{-1}(h_1)_4)} & \alpha_{\phi_2((h_1)_2^{-1}(h_1)_1)} & \alpha_{\phi_2((h_1)_2^{-1}(h_1)_2)} & \alpha_{\phi_2((h_1)_2^{-1}(h_1)_3)} & \alpha_{\phi_2((h_1)_2^{-1}(h_1)_4)} \\ \alpha_{\phi_1((h_1)_3^{-1}(h_1)_1)} & \alpha_{\phi_1((h_1)_3^{-1}(h_1)_2)} & \alpha_{\phi_1((h_1)_3^{-1}(h_1)_3)} & \alpha_{\phi_1((h_1)_3^{-1}(h_1)_4)} & \alpha_{\phi_2((h_1)_3^{-1}(h_1)_1)} & \alpha_{\phi_2((h_1)_3^{-1}(h_1)_2)} & \alpha_{\phi_2((h_1)_3^{-1}(h_1)_3)} & \alpha_{\phi_2((h_1)_3^{-1}(h_1)_4)} \\ \alpha_{\phi_1((h_1)_4^{-1}(h_1)_1)} & \alpha_{\phi_1((h_1)_4^{-1}(h_1)_2)} & \alpha_{\phi_1((h_1)_4^{-1}(h_1)_3)} & \alpha_{\phi_1((h_1)_4^{-1}(h_1)_4)} & \alpha_{\phi_2((h_1)_4^{-1}(h_1)_1)} & \alpha_{\phi_2((h_1)_4^{-1}(h_1)_2)} & \alpha_{\phi_2((h_1)_4^{-1}(h_1)_3)} & \alpha_{\phi_2((h_1)_4^{-1}(h_1)_4)} \\ \alpha_{g_5^{-1}g_1} & \alpha_{g_5^{-1}g_2} & \alpha_{g_5^{-1}g_3} & \alpha_{g_5^{-1}g_4} & \alpha_{g_5^{-1}g_5} & \alpha_{g_5^{-1}g_6} & \alpha_{g_5^{-1}g_7} & \alpha_{g_5^{-1}g_8} \\ \alpha_{g_6^{-1}g_1} & \alpha_{g_6^{-1}g_2} & \alpha_{g_6^{-1}g_3} & \alpha_{g_6^{-1}g_4} & \alpha_{g_6^{-1}g_5} & \alpha_{g_6^{-1}g_6} & \alpha_{g_6^{-1}g_7} & \alpha_{g_6^{-1}g_8} \\ \alpha_{g_7^{-1}g_1} & \alpha_{g_7^{-1}g_2} & \alpha_{g_7^{-1}g_3} & \alpha_{g_7^{-1}g_4} & \alpha_{g_7^{-1}g_5} & \alpha_{g_7^{-1}g_6} & \alpha_{g_7^{-1}g_7} & \alpha_{g_7^{-1}g_8} \\ \alpha_{g_8^{-1}g_1} & \alpha_{g_8^{-1}g_2} & \alpha_{g_8^{-1}g_3} & \alpha_{g_8^{-1}g_4} & \alpha_{g_8^{-1}g_5} & \alpha_{g_8^{-1}g_6} & \alpha_{g_8^{-1}g_7} & \alpha_{g_8^{-1}g_8} \end{pmatrix}.$$

where

$$\begin{aligned} \phi_1 : (h_1)_i &\xrightarrow{\phi_1} g_1^{-1}g_i & \phi_2 : (h_1)_i &\xrightarrow{\phi_2} g_1^{-1}g_j \\ \text{for } i = \{1, 2, 3, 4\} & & \text{for when } \{i = 1, j = 5, i = 2, j = 6, i = 3, j = 7, i = 4, j = 8\} \end{aligned}$$

in  $A'_1$  and  $A'_2$ . This results in a composite matrix over  $R$  of the following form:

$$\Omega(v) = \begin{pmatrix} \alpha_1 & \alpha_x & \alpha_{x^2} & \alpha_{x^3} & \alpha_y & \alpha_{xy} & \alpha_{x^2y} & \alpha_{x^3y} \\ \alpha_x & \alpha_1 & \alpha_{x^3} & \alpha_{x^2} & \alpha_{xy} & \alpha_y & \alpha_{x^3y} & \alpha_{x^2y} \\ \alpha_{x^2} & \alpha_{x^3} & \alpha_1 & \alpha_x & \alpha_{x^2y} & \alpha_{x^3y} & \alpha_y & \alpha_{xy} \\ \alpha_{x^3} & \alpha_{x^2} & \alpha_x & \alpha_1 & \alpha_{x^3y} & \alpha_{x^2y} & \alpha_{xy} & \alpha_y \\ \alpha_y & \alpha_{x^3y} & \alpha_{x^2y} & \alpha_{xy} & \alpha_1 & \alpha_{x^3} & \alpha_{x^2} & \alpha_x \\ \alpha_{xy} & \alpha_y & \alpha_{x^3y} & \alpha_{x^2y} & \alpha_x & \alpha_1 & \alpha_{x^3} & \alpha_{x^2} \\ \alpha_{x^2y} & \alpha_{xy} & \alpha_y & \alpha_{x^3y} & \alpha_{x^2} & \alpha_x & \alpha_1 & \alpha_{x^3} \\ \alpha_{x^3y} & \alpha_{x^2y} & \alpha_{xy} & \alpha_y & \alpha_{x^3} & \alpha_{x^2} & \alpha_x & \alpha_1 \end{pmatrix}.$$

We now look at the rows of  $\Omega(v)$  and see what their corresponding element in  $RD_8$  is, in terms of  $v$ . Let  $r_1, r_2, \dots, r_8$  be the rows of  $\Omega(v)$ , then each row is formed by multiplying each term of  $v$  by an element of  $G$ . The elements of  $G$  do not have to be the same but they can be. For example:

$$r_1 = \alpha_{(1)1}(1)1 + \alpha_{(1)x}(1)x + \alpha_{(1)x^2}(1)x^2 + \alpha_{(1)x^3}(1)x^3 + \alpha_{(1)y}(1)y + \alpha_{(1)xy}(1)xy + \alpha_{(1)x^2y}(1)x^2y + \alpha_{(1)x^3y}(1)x^3y,$$

the first row of  $\Omega(v)$  is obtained by multiplying each term of  $v$  by the same group element of  $G$ , namely 1.

$$r_2 = \alpha_{(x)1}(x)1 + \alpha_{(x^3)x}(x^3)x + \alpha_{(x)x^2}(x)x^2 + \alpha_{(x^3)x^3}(x^3)x^3 + \alpha_{(x)y}(x)y + \alpha_{(x^3)xy}(x^3)xy + \alpha_{(x)x^2y}(x)x^2y + \alpha_{(x^3)x^3y}(x^3)x^3y,$$

the second row of  $\Omega(v)$  is obtained by multiplying the terms of  $v$  by the group elements of  $G$ ;  $x$  or  $x^3$ .

$$r_8 = \alpha_{(x^3y)1}(x^3y)1 + \alpha_{(x^3y)x}(x^3y)x + \alpha_{(x^3y)x^2}(x^3y)x^2 + \alpha_{(x^3y)x^3}(x^3y)x^3 + \alpha_{(x^3y)y}(x^3y)y + \alpha_{(x^3y)xy}(x^3y)xy + \alpha_{(x^3y)x^2y}(x^3y)x^2y + \alpha_{(x^3y)x^3y}(x^3y)x^3y,$$

the eighth row of  $\Omega(v)$  is obtained by multiplying each term of  $v$  by the same group element of  $G$ , namely  $x^3y$ .

Example 1 highlights the difference between the matrix  $\sigma(v)$  from [21] and the matrix  $\Omega(v)$ . Namely, each row of  $\sigma(v)$  consists of vectors that correspond to the elements  $hv$  in  $RG$  with  $h \in G$  (we multiply each term of  $v$  by the same group element of  $G$ ) where in  $\Omega(v)$ , some rows are formed by multiplying the terms of  $v$  by different group elements of  $G$ . Therefore, we can say that each row of  $\Omega(v)$  corresponds to an element in  $RG$  of the following form:

$$v_j^* = \sum_{i=1}^n \alpha_{g_{ji}g_i} g_{ji} g_i, \tag{6}$$

where  $\alpha_{g_{ji}g_i} \in R$ ,  $g_i, g_{ji} \in G$  and  $j$  is the  $j$ th row of the matrix  $\Omega(v)$ . In other words, we can define the composite matrix  $\Omega(v)$  as

$$\Omega(v) = \begin{pmatrix} \alpha_{g_{11}g_1} & \alpha_{g_{12}g_2} & \alpha_{g_{13}g_3} & \dots & \alpha_{g_{1n}g_n} \\ \alpha_{g_{21}g_1} & \alpha_{g_{22}g_2} & \alpha_{g_{23}g_3} & \dots & \alpha_{g_{2n}g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_{n1}g_1} & \alpha_{g_{n2}g_2} & \alpha_{g_{n3}g_3} & \dots & \alpha_{g_{nn}g_n} \end{pmatrix}, \tag{7}$$

where the elements  $g_{ji}$  are simply the group elements  $G$ . Which elements of  $G$  these are, depends how the composite matrix is defined, i.e., what groups we employ and how we define the  $\phi_l$  map in individual blocks.

It is possible to form a composite matrix so that each row of  $\Omega(v)$  corresponds to the elements  $\alpha_{g_{ji}}$  in  $RG$  where  $g_{ji}$  are equal for all  $i \in \{1, 2, \dots, n\}$ . If this is the case, then  $\Omega(v)$  is equivalent to  $\sigma(v)$ . We look at an example.

**Example 2** Let  $G = \langle x, y \mid x^4 = y^2 = 1, x^y = x^{-1} \rangle \cong D_8$ . Let  $v = \alpha_1 + \alpha_x x + \alpha_{x^2} x^2 + \alpha_{x^3} x^3 + \alpha_y y + \alpha_{xy} xy + \alpha_{x^2 y} x^2 y + \alpha_{x^3 y} x^3 y \in RD_8$ , where  $\alpha_{g_i} \in R$ . Then

$$\sigma(v) = \begin{pmatrix} \alpha_1 & \alpha_x & \alpha_{x^2} & \alpha_{x^3} & \alpha_y & \alpha_{xy} & \alpha_{x^2 y} & \alpha_{x^3 y} \\ \alpha_{x^3} & \alpha_1 & \alpha_x & \alpha_{x^2} & \alpha_{x^3 y} & \alpha_y & \alpha_{xy} & \alpha_{x^2 y} \\ \alpha_{x^2} & \alpha_{x^3} & \alpha_1 & \alpha_x & \alpha_{x^2 y} & \alpha_{x^3 y} & \alpha_y & \alpha_{xy} \\ \alpha_x & \alpha_{x^2} & \alpha_{x^3} & \alpha_1 & \alpha_{xy} & \alpha_{x^2 y} & \alpha_{x^3 y} & \alpha_y \\ \hline \alpha_y & \alpha_{x^3 y} & \alpha_{x^2 y} & \alpha_{xy} & \alpha_1 & \alpha_{x^3} & \alpha_{x^2} & \alpha_x \\ \alpha_{xy} & \alpha_y & \alpha_{x^3 y} & \alpha_{x^2 y} & \alpha_x & \alpha_1 & \alpha_{x^3} & \alpha_{x^2} \\ \alpha_{x^2 y} & \alpha_{xy} & \alpha_y & \alpha_{x^3 y} & \alpha_{x^2} & \alpha_x & \alpha_1 & \alpha_{x^3} \\ \alpha_{x^3 y} & \alpha_{x^2 y} & \alpha_{xy} & \alpha_y & \alpha_{x^3} & \alpha_{x^2} & \alpha_x & \alpha_1 \end{pmatrix}.$$

Now let  $H_1 = \langle a \mid a^4 = 1 \rangle \cong C_4$  and define the composite matrix as:

$$\Omega(v) = \begin{pmatrix} A'_1 & A'_2 \\ A_3 & A_4 \end{pmatrix} = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \alpha_{g_1^{-1}g_3} & \alpha_{g_1^{-1}g_4} & \alpha_{g_1^{-1}g_5} & \alpha_{g_1^{-1}g_6} & \alpha_{g_1^{-1}g_7} & \alpha_{g_1^{-1}g_8} \\ \alpha_{\phi_1((h_1)_2^{-1}(h_1)_1)} & \alpha_{\phi_1((h_1)_2^{-1}(h_1)_2)} & \alpha_{\phi_1((h_1)_2^{-1}(h_1)_3)} & \alpha_{\phi_1((h_1)_2^{-1}(h_1)_4)} & \alpha_{\phi_2((h_2)_2^{-1}(h_2)_1)} & \alpha_{\phi_2((h_2)_2^{-1}(h_2)_2)} & \alpha_{\phi_2((h_2)_2^{-1}(h_2)_3)} & \alpha_{\phi_2((h_2)_2^{-1}(h_2)_4)} \\ \alpha_{\phi_1((h_1)_3^{-1}(h_1)_1)} & \alpha_{\phi_1((h_1)_3^{-1}(h_1)_2)} & \alpha_{\phi_1((h_1)_3^{-1}(h_1)_3)} & \alpha_{\phi_1((h_1)_3^{-1}(h_1)_4)} & \alpha_{\phi_2((h_2)_3^{-1}(h_2)_1)} & \alpha_{\phi_2((h_2)_3^{-1}(h_2)_2)} & \alpha_{\phi_2((h_2)_3^{-1}(h_2)_3)} & \alpha_{\phi_2((h_2)_3^{-1}(h_2)_4)} \\ \alpha_{\phi_1((h_1)_4^{-1}(h_1)_1)} & \alpha_{\phi_1((h_1)_4^{-1}(h_1)_2)} & \alpha_{\phi_1((h_1)_4^{-1}(h_1)_3)} & \alpha_{\phi_1((h_1)_4^{-1}(h_1)_4)} & \alpha_{\phi_2((h_2)_4^{-1}(h_2)_1)} & \alpha_{\phi_2((h_2)_4^{-1}(h_2)_2)} & \alpha_{\phi_2((h_2)_4^{-1}(h_2)_3)} & \alpha_{\phi_2((h_2)_4^{-1}(h_2)_4)} \\ \hline \alpha_{g_5^{-1}g_1} & \alpha_{g_5^{-1}g_2} & \alpha_{g_5^{-1}g_3} & \alpha_{g_5^{-1}g_4} & \alpha_{g_5^{-1}g_5} & \alpha_{g_5^{-1}g_6} & \alpha_{g_5^{-1}g_7} & \alpha_{g_5^{-1}g_8} \\ \alpha_{g_6^{-1}g_1} & \alpha_{g_6^{-1}g_2} & \alpha_{g_6^{-1}g_3} & \alpha_{g_6^{-1}g_4} & \alpha_{g_6^{-1}g_5} & \alpha_{g_6^{-1}g_6} & \alpha_{g_6^{-1}g_7} & \alpha_{g_6^{-1}g_8} \\ \alpha_{g_7^{-1}g_1} & \alpha_{g_7^{-1}g_2} & \alpha_{g_7^{-1}g_3} & \alpha_{g_7^{-1}g_4} & \alpha_{g_7^{-1}g_5} & \alpha_{g_7^{-1}g_6} & \alpha_{g_7^{-1}g_7} & \alpha_{g_7^{-1}g_8} \\ \alpha_{g_8^{-1}g_1} & \alpha_{g_8^{-1}g_2} & \alpha_{g_8^{-1}g_3} & \alpha_{g_8^{-1}g_4} & \alpha_{g_8^{-1}g_5} & \alpha_{g_8^{-1}g_6} & \alpha_{g_8^{-1}g_7} & \alpha_{g_8^{-1}g_8} \end{pmatrix}.$$

where

$$\phi_1 : (h_1)_i \xrightarrow{\phi_1} g_1^{-1} g_i \quad \phi_2 : (h_1)_i \xrightarrow{\phi_2} g_1^{-1} g_j$$

for  $i = \{1, 2, 3, 4\}$  for when  $\{i = 1, j = 5, i = 2, j = 6, i = 3, j = 7, i = 4, j = 8\}$

in  $A'_1$  and  $A'_2$ . Then

$$\Omega(v) = \begin{pmatrix} \alpha_1 & \alpha_x & \alpha_{x^2} & \alpha_{x^3} & \alpha_y & \alpha_{xy} & \alpha_{x^2 y} & \alpha_{x^3 y} \\ \alpha_{x^3} & \alpha_1 & \alpha_x & \alpha_{x^2} & \alpha_{x^3 y} & \alpha_y & \alpha_{xy} & \alpha_{x^2 y} \\ \alpha_{x^2} & \alpha_{x^3} & \alpha_1 & \alpha_x & \alpha_{x^2 y} & \alpha_{x^3 y} & \alpha_y & \alpha_{xy} \\ \alpha_x & \alpha_{x^2} & \alpha_{x^3} & \alpha_1 & \alpha_{xy} & \alpha_{x^2 y} & \alpha_{x^3 y} & \alpha_y \\ \hline \alpha_y & \alpha_{x^3 y} & \alpha_{x^2 y} & \alpha_{xy} & \alpha_1 & \alpha_{x^3} & \alpha_{x^2} & \alpha_x \\ \alpha_{xy} & \alpha_y & \alpha_{x^3 y} & \alpha_{x^2 y} & \alpha_x & \alpha_1 & \alpha_{x^3} & \alpha_{x^2} \\ \alpha_{x^2 y} & \alpha_{xy} & \alpha_y & \alpha_{x^3 y} & \alpha_{x^2} & \alpha_x & \alpha_1 & \alpha_{x^3} \\ \alpha_{x^3 y} & \alpha_{x^2 y} & \alpha_{xy} & \alpha_y & \alpha_{x^3} & \alpha_{x^2} & \alpha_x & \alpha_1 \end{pmatrix}.$$

Clearly, in this specific case,  $\Omega(v)$  is equivalent to  $\sigma(v)$ .

Example 2 leads to the following result.

**Corollary 3.1** *The matrix  $\Omega(v)$  is equivalent to the matrix  $\sigma(v)$  if the group elements  $g_{ji}$  in Equation 6 are the same for all  $i \in \{1, 2, \dots, n\}$ .*

We also have the following result.

**Corollary 3.2** *Let  $v = \alpha_{g_1}g_1 + \alpha_{g_2}g_2 + \dots + \alpha_{g_n}g_n \in RG$  and  $\sigma(v)$  be the corresponding matrix over  $R$ . Let  $v'$  be also an element of  $RG$  but with a different ordering of the elements to  $v$ . Then  $\sigma(v')$  is permutation equivalent to  $\sigma(v)$ .*

This corollary leads to the following Theorem. We omit the proof.

**Theorem 3.3** *Let  $\Omega(v)$  be a composite matrix over  $R$  such that at least one row of  $\Omega(v)$  corresponds to an element in  $RG$  of the form*

$$v_j^* = \sum_{i=1}^n \alpha_{g_{j_i}g_i}g_{j_i}g_i,$$

where  $g_{j_i}$  is not the same for all  $i \in \{1, 2, \dots, n\}$ . Here,  $\alpha_{g_{j_i}g_i} \in R$ ,  $g_i, g_{j_i} \in G$  and  $j$  is the  $j$ th row of the matrix  $\Omega(v)$ . Then  $\Omega(v)$  is not permutation equivalent to  $\sigma(v)$  for any arrangement of the elements of  $G$  in  $v$ .

### 4 Composite G-codes

We are now ready to introduce the code construction.

For a given element  $v \in RG$  and some groups  $H_i$  of order  $r$ , we define the following code over the ring  $R$  :

$$C(v) = \langle \Omega(v) \rangle. \tag{8}$$

The code is formed by taking the row space of  $\Omega(v)$  over the ring  $R$ . As in [13], the code  $C(v)$  is a linear code over the ring  $R$ , since it is the row space of a generator matrix. It is not possible to determine the size of the code immediately from the matrix.

**Example 3** Let  $G = \langle x, y \mid x^4 = 1, y^2 = x^2, x^y = x^{-1} \rangle \cong Q_8$ . Let  $v = \sum_{i=0}^3 \alpha_i + 1x^i + \alpha_{i+5}x^i y \in RQ_8$ , where  $\alpha_i = \alpha_{g_i} \in R$ . Let  $H_1 = \langle a, b \mid a^2 = b^2 = 1, ab = ba \rangle \cong C_2 \times C_2$ . We now define the composite matrix as:

$$\Omega(v) = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} = \left( \begin{array}{cccc|cccc} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \alpha_{g_1^{-1}g_3} & \alpha_{g_1^{-1}g_4} & \alpha_{g_1^{-1}g_5} & \alpha_{g_1^{-1}g_6} & \alpha_{g_1^{-1}g_7} & \alpha_{g_1^{-1}g_8} \\ \alpha_{\phi_1((h_1)_2^{-1}(h_1)_1)} & \alpha_{\phi_1((h_1)_2^{-1}(h_1)_2)} & \alpha_{\phi_1((h_1)_2^{-1}(h_1)_3)} & \alpha_{\phi_1((h_1)_2^{-1}(h_1)_4)} & \alpha_{g_2^{-1}g_5} & \alpha_{g_2^{-1}g_6} & \alpha_{g_2^{-1}g_7} & \alpha_{g_2^{-1}g_8} \\ \alpha_{\phi_1((h_1)_3^{-1}(h_1)_1)} & \alpha_{\phi_1((h_1)_3^{-1}(h_1)_2)} & \alpha_{\phi_1((h_1)_3^{-1}(h_1)_3)} & \alpha_{\phi_1((h_1)_3^{-1}(h_1)_4)} & \alpha_{g_3^{-1}g_5} & \alpha_{g_3^{-1}g_6} & \alpha_{g_3^{-1}g_7} & \alpha_{g_3^{-1}g_8} \\ \alpha_{\phi_1((h_1)_4^{-1}(h_1)_1)} & \alpha_{\phi_1((h_1)_4^{-1}(h_1)_2)} & \alpha_{\phi_1((h_1)_4^{-1}(h_1)_3)} & \alpha_{\phi_1((h_1)_4^{-1}(h_1)_4)} & \alpha_{g_4^{-1}g_5} & \alpha_{g_4^{-1}g_6} & \alpha_{g_4^{-1}g_7} & \alpha_{g_4^{-1}g_8} \\ \hline \alpha_{g_5^{-1}g_1} & \alpha_{g_5^{-1}g_2} & \alpha_{g_5^{-1}g_3} & \alpha_{g_5^{-1}g_4} & \alpha_{g_5^{-1}g_5} & \alpha_{g_5^{-1}g_6} & \alpha_{g_5^{-1}g_7} & \alpha_{g_5^{-1}g_8} \\ \alpha_{g_6^{-1}g_1} & \alpha_{g_6^{-1}g_2} & \alpha_{g_6^{-1}g_3} & \alpha_{g_6^{-1}g_4} & \alpha_{\phi_4((h_1)_2^{-1}(h_1)_1)} & \alpha_{\phi_4((h_1)_2^{-1}(h_1)_2)} & \alpha_{\phi_4((h_1)_2^{-1}(h_1)_3)} & \alpha_{\phi_4((h_1)_2^{-1}(h_1)_4)} \\ \alpha_{g_7^{-1}g_1} & \alpha_{g_7^{-1}g_2} & \alpha_{g_7^{-1}g_3} & \alpha_{g_7^{-1}g_4} & \alpha_{\phi_4((h_1)_3^{-1}(h_1)_1)} & \alpha_{\phi_4((h_1)_3^{-1}(h_1)_2)} & \alpha_{\phi_4((h_1)_3^{-1}(h_1)_3)} & \alpha_{\phi_4((h_1)_3^{-1}(h_1)_4)} \\ \alpha_{g_8^{-1}g_1} & \alpha_{g_8^{-1}g_2} & \alpha_{g_8^{-1}g_3} & \alpha_{g_8^{-1}g_4} & \alpha_{\phi_4((h_1)_4^{-1}(h_1)_1)} & \alpha_{\phi_4((h_1)_4^{-1}(h_1)_2)} & \alpha_{\phi_4((h_1)_4^{-1}(h_1)_3)} & \alpha_{\phi_4((h_1)_4^{-1}(h_1)_4)} \end{array} \right).$$

where:

$$\begin{aligned} \phi_1 : (h_1)_i &\xrightarrow{\phi_1} g_1^{-1}g_i & \phi_4 : (h_1)_i &\xrightarrow{\phi_4} g_5^{-1}g_j \\ \text{for } i &= \{1, 2, 3, 4\} & \text{for when } \{i &= 1, j = 5, i = 2, j = 6, i = 3, j = 7, i = 4, j = 8\}, \end{aligned}$$



in  $A'_1$  and  $A'_4$  respectively. This results in a composite matrix over  $R$  of the following form:

$$\Omega(v) = \left( \begin{array}{cc|cc} X_1 & Y_1 & X_2 & \\ \hline Y_1 & X_1 & & \\ X_3 & X_4 & Y_4 & \\ & & Y_4 & X_4 \end{array} \right) = \left( \begin{array}{cccc|cccc} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 \\ \alpha_2 & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_8 & \alpha_5 & \alpha_6 & \alpha_7 \\ \alpha_3 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_7 & \alpha_8 & \alpha_5 & \alpha_6 \\ \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_5 \\ \hline \alpha_7 & \alpha_6 & \alpha_5 & \alpha_8 & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_2 \\ \alpha_8 & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_5 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_4 \\ \alpha_6 & \alpha_5 & \alpha_8 & \alpha_7 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_1 \end{array} \right).$$

If we let  $v = x^3 + xy + x^2y + x^3y \in \mathbb{F}_2 Q_8$ , where  $\langle x, y \rangle \cong Q_8$ , then

$$\mathcal{C}(v) = \langle \Omega(v) \rangle = \left( \begin{array}{cccccccc} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \end{array} \right)$$

and  $\mathcal{C}(v)$  is equivalent to

$$\left( \begin{array}{cccccccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array} \right).$$

Clearly  $\mathcal{C}(v) = \langle \Omega(v) \rangle$  is the [8, 4, 4] extended Hamming code.

In the above example, the group  $C_2 \times C_2$  was applied twice in two different blocks:  $A'_1$  and  $A'_4$ . As mentioned in the previous section, we can employ more than one group of order  $r$ , please see [9] for details.

We now extend two results from [13]; we show that the codes constructed from the composite matrices are also ideals in the group ring. We then show that the automorphism group of such codes contains the group  $G$  as a subgroup.

**Theorem 4.1** *Let  $R$  be a finite commutative Frobenius ring,  $G$  a finite group of order  $n$ . Let  $H_i$  be finite groups of order  $r$  such that  $r$  is a factor of  $n$  with  $n > r$  and  $n, r \neq 1$ . Also, let  $v \in RG$  and  $\mathcal{C}(v) = \langle \Omega(v) \rangle$  be the corresponding code in  $R^n$ . Define  $I(v)$  to be the set of elements of  $RG$  such that  $\sum \alpha_i g_i \in I(v)$  if and only if  $(\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathcal{C}(v)$ . Then  $I(v)$  is a left ideal in  $RG$ .*

**Proof** We saw above that the rows of  $\Omega(v)$  consist precisely of the vectors that correspond to the elements of the form  $v_j^* = \sum_{i=1}^n \alpha_{g_j g_i} g_j g_i$  in  $RG$ , where  $\alpha_{g_j g_i} \in R$ ,  $g_i, g_j \in G$  and  $j$  is the  $j$ th row of the matrix  $\Omega(v)$ . We also know that some of the elements  $g_j$  equal to  $\phi_l(h_i)$  for some map  $\phi_l$  and the elements  $h_i$  of  $H_i$ . Let  $a = \sum \alpha_i g_i$  and  $b = \sum \beta_i g_i$  be two elements in  $I(v)$ , then  $a + b = \sum (\alpha_i + \beta_i) g_i$  which corresponds to the sum of the corresponding elements in  $\mathcal{C}(v)$ . This implies that  $I(v)$  is closed under addition.

Let  $w_1 = \sum \beta_i g_i \in RG$ . Then if  $w_2$  corresponds to a vector in  $\mathcal{C}(v)$ , it is of the form  $\sum \gamma_j v_j^*$ . Then  $w_1 w_2 = \sum \beta_i g_i \sum \gamma_j v_j^* = \sum \beta_i \gamma_j g_i v_j^*$  which corresponds to an element in  $\mathcal{C}(v)$  and gives that the element is in  $I(v)$ . Therefore  $I(v)$  is a left ideal of  $RG$ .  $\square$

**Corollary 4.2** *Let  $R$  be a finite commutative Frobenius ring and  $G$  a finite group of order  $n$ . Let  $H_i$  be finite groups of order  $r$  such that  $r$  is a factor of  $n$  with  $n > r$  and  $n, r \neq 1$ . Also, let  $v \in RG$  and let  $\mathcal{C}(v) = \langle \Omega(v) \rangle$  be the corresponding code in  $R^n$ . Then the automorphism group of  $\mathcal{C}(v)$  has a subgroup isomorphic to the group  $G$ .*

**Proof** Since  $I(v)$  is an ideal in  $RG$  we have that  $I(v)$  is held invariant by the action of the elements of the group  $G$ . It follows immediately that the automorphism group of  $\mathcal{C}(v)$  contains the group  $G$  as a subgroup. □

Similarly, as in [13], the codes constructed by the above technique are held invariant by the action of the group  $G$  on the coordinates. We can therefore construct a code whose automorphism group must contain the group  $G$ . Moreover, in our construction, we apply groups of order  $r$  and the bijective maps  $\phi_l$  in individual blocks to determine the permutation of the coordinates in each row of a code. For this reason, we refer to a code constructed by the above technique as a composite  $G$ -code.

We also have the following as a result of Corollary 4.2.

**Corollary 4.3** *The putative [72, 36, 16] code cannot be of the form  $\mathcal{C}(v) = \langle \Omega(v) \rangle$  for any  $v \in \mathbb{F}_2G$  for any group  $G$ .*

**Proof** It is well known that the automorphism group of a putative [72, 36, 16] code must have order less than or equal to 5 (see [13] for details). If it were of this construction, some group of order 72 would have to be in its automorphism group. Therefore, the code cannot be formed from this construction. □

We finish this section with one more result which is a generalization of the result from [13]. We show that if  $\mathcal{C}$  is a composite  $G$ -code for some  $G$  then its orthogonal  $\mathcal{C}^\perp$  is also a composite  $G$ -code.

Let  $I$  be an ideal in a group ring  $RG$ . Define  $\mathcal{R}(I) = \{w \mid vw = 0, \forall v \in I\}$ . It is immediate that  $\mathcal{R}(I)$  is an ideal of  $RG$ .

Let  $v = \alpha_{g_1}g_1 + \alpha_{g_2}g_2 + \dots + \alpha_{g_n}g_n \in RG$  and  $\mathcal{C}(v)$  be the corresponding code. Let  $\Psi : RG \rightarrow R^n$  be the canonical map that sends  $\alpha_{g_1}g_1 + \alpha_{g_2}g_2 + \dots + \alpha_{g_n}g_n$  to  $(\alpha_{g_1}, \alpha_{g_2}, \dots, \alpha_{g_n})$ . Let  $I$  be the ideal  $\Psi^{-1}(\mathcal{C})$ . Let  $\mathbf{w} = (w_1, w_2, \dots, w_n) \in \mathcal{C}^\perp$ . Then

$$[(\alpha_{g_{j_1}g_1}, \alpha_{g_{j_2}g_2}, \dots, \alpha_{g_{j_n}g_n}), (w_1, w_2, \dots, w_n)] = 0, \forall j, \tag{9}$$

where  $g_{j_i} \in G$ . This gives that

$$\sum_{i=0}^n \alpha_{g_{j_i}g_i} w_i = 0, \forall j. \tag{10}$$

Let  $w = \Psi^{-1}(\mathbf{w}) = \sum w_{g_i}g_i$  and define  $\bar{\mathbf{w}} \in RG$  to be  $\bar{\mathbf{w}} = b_{g_1}g_1 + b_{g_2}g_2 + \dots + b_{g_n}g_n$  where

$$b_{g_i} = w_{g_i}^{-1}. \tag{11}$$

Then

$$\sum_{i=1}^n \alpha_{g_{j_i}g_i} w_i = 0 \implies \sum_{i=1}^n \alpha_{g_{j_i}g_i} b_{g_i}^{-1} = 0. \tag{12}$$

Here  $g_{j_i}g_i g_i^{-1} = g_{j_i}$ , hence this is the coefficient of  $g_{j_i}$  in the product of  $\bar{\mathbf{w}}$  and  $v_j^*$ . This gives that  $\bar{\mathbf{w}} \in \mathcal{R}(I)$  if and only if  $\mathbf{w} \in \mathcal{C}^\perp$ .

Let  $\phi : R^n \rightarrow RG$  by  $\phi(\mathbf{w}) = \bar{\mathbf{w}}$ . It is clear that  $\phi$  is a bijection between  $C^\perp$  and  $\mathcal{R}(\Psi^{-1}(C))$ .

**Theorem 4.4** *Let  $C = \mathcal{C}(v)$  be a code in  $RG$  formed from the vector  $v \in RG$ . Then  $\Psi^{-1}(C^\perp)$  is an ideal of  $RG$ .*

**Proof** We have that  $\Psi(\phi(C^\perp))$  is permutation equivalent to  $C^\perp$  and  $\phi(C^\perp)$  is an ideal and so  $\Psi^{-1}(C)$  is an ideal as well.  $\square$

### 5 Self-orthogonal composite G-codes

In this section, we extend more results from [13]. Namely, we show that the map  $\Omega : RG \rightarrow M_n(R)$  is an injective ring homomorphism, we show when our construction  $C = \langle \Omega(v) \rangle$  produces a self-orthogonal code and also when it produces a self-dual code.

Before we look at the theoretical results, we define the composite matrix  $\Omega(v)$  that we defined in the the previous section, in a different but equivalent form. Namely, let

$$\Omega(v) = \begin{pmatrix} \alpha_{g_{1_1}^{-1}g_1} & \alpha_{g_{1_2}^{-1}g_2} & \alpha_{g_{1_3}^{-1}g_3} & \dots & \alpha_{g_{1_n}^{-1}g_n} \\ \alpha_{g_{2_1}^{-1}g_1} & \alpha_{g_{2_2}^{-1}g_2} & \alpha_{g_{2_3}^{-1}g_3} & \dots & \alpha_{g_{2_n}^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_{n_1}^{-1}g_1} & \alpha_{g_{n_2}^{-1}g_2} & \alpha_{g_{n_3}^{-1}g_3} & \dots & \alpha_{g_{n_n}^{-1}g_n} \end{pmatrix},$$

where  $g_{j_i}^{-1}$  are simply the elements of the group  $G$ . These elements are determined by how the matrix has been partitioned, what groups  $H_i$  of order  $r$  have been employed and how the maps  $\phi_l$  have been defined to form the composite matrix. This representation of the composite matrix  $\Omega(v)$  will make it easier to prove the upcoming results.

**Theorem 5.1** *Let  $R$  be a finite commutative Frobenius ring,  $G$  be a group of order  $n$  and  $H_i$  be finite groups of order  $r$  such that  $r$  is a factor of  $n$  with  $n > 1$  and  $n, r \neq 1$ . Then the map  $\Omega : RG \rightarrow M_n(R)$  is an injective ring homomorphism.*

**Proof** We need to show that the map  $\Omega$  preserves addition and multiplication. Let  $R$  be a finite commutative Frobenius ring,  $G$  be a group of order  $n$  and  $H_i$  be finite groups of order  $r$  such that  $r$  is a factor of  $n$  with  $n > 1$  and  $n, r \neq 1$ . Now define the mapping  $\Omega : RG \rightarrow M_n(R)$  as follows. Suppose  $v = \sum_{i=1}^n \alpha_{g_i} g_i$ . Then

$$\Omega(v) = \begin{pmatrix} \alpha_{g_{1_1}^{-1}g_1} & \alpha_{g_{1_2}^{-1}g_2} & \alpha_{g_{1_3}^{-1}g_3} & \dots & \alpha_{g_{1_n}^{-1}g_n} \\ \alpha_{g_{2_1}^{-1}g_1} & \alpha_{g_{2_2}^{-1}g_2} & \alpha_{g_{2_3}^{-1}g_3} & \dots & \alpha_{g_{2_n}^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_{n_1}^{-1}g_1} & \alpha_{g_{n_2}^{-1}g_2} & \alpha_{g_{n_3}^{-1}g_3} & \dots & \alpha_{g_{n_n}^{-1}g_n} \end{pmatrix},$$

where  $g_{j_i}^{-1}$  are simply the elements of the group  $G$  in some order. This order is determined by how the matrix has been partitioned, what groups  $H_i$  of order  $r$  have been employed and how the maps  $\phi_l$  have been defined to form the composite matrix  $\Omega(v)$ . This mapping is clearly surjective and injective. We now show that  $\Omega$  is additive and multiplicative. Let

$w = \sum_{i=1}^n \beta_{g_i} g_i$  then

$$\begin{aligned} \Omega(v+w) &= \begin{pmatrix} (\alpha + \beta)_{g_{1_1}^{-1} g_1} & (\alpha + \beta)_{g_{1_2}^{-1} g_2} & (\alpha + \beta)_{g_{1_3}^{-1} g_3} & \dots & (\alpha + \beta)_{g_{1_n}^{-1} g_n} \\ (\alpha + \beta)_{g_{2_1}^{-1} g_1} & (\alpha + \beta)_{g_{2_2}^{-1} g_2} & (\alpha + \beta)_{g_{2_3}^{-1} g_3} & \dots & (\alpha + \beta)_{g_{2_n}^{-1} g_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (\alpha + \beta)_{g_{n_1}^{-1} g_1} & (\alpha + \beta)_{g_{n_2}^{-1} g_2} & (\alpha + \beta)_{g_{n_3}^{-1} g_3} & \dots & (\alpha + \beta)_{g_{n_n}^{-1} g_n} \end{pmatrix} \\ &= \begin{pmatrix} \alpha_{g_{1_1}^{-1} g_1} & \alpha_{g_{1_2}^{-1} g_2} & \alpha_{g_{1_3}^{-1} g_3} & \dots & \alpha_{g_{1_n}^{-1} g_n} \\ \alpha_{g_{2_1}^{-1} g_1} & \alpha_{g_{2_2}^{-1} g_2} & \alpha_{g_{2_3}^{-1} g_3} & \dots & \alpha_{g_{2_n}^{-1} g_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_{n_1}^{-1} g_1} & \alpha_{g_{n_2}^{-1} g_2} & \alpha_{g_{n_3}^{-1} g_3} & \dots & \alpha_{g_{n_n}^{-1} g_n} \end{pmatrix} + \begin{pmatrix} \beta_{g_{1_1}^{-1} g_1} & \beta_{g_{1_2}^{-1} g_2} & \beta_{g_{1_3}^{-1} g_3} & \dots & \beta_{g_{1_n}^{-1} g_n} \\ \beta_{g_{2_1}^{-1} g_1} & \beta_{g_{2_2}^{-1} g_2} & \beta_{g_{2_3}^{-1} g_3} & \dots & \beta_{g_{2_n}^{-1} g_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \beta_{g_{n_1}^{-1} g_1} & \beta_{g_{n_2}^{-1} g_2} & \beta_{g_{n_3}^{-1} g_3} & \dots & \beta_{g_{n_n}^{-1} g_n} \end{pmatrix} \\ &= \Omega(v) + \Omega(w). \end{aligned}$$

Thus addition is preserved. Next, suppose  $v * w = t$ , where  $t = \sum_{i=1}^n \gamma_{g_i} g_i$ . Then

$$\Omega(v) * \Omega(w) = \begin{pmatrix} \gamma_{g_{1_1}^{-1} g_1} & \gamma_{g_{1_2}^{-1} g_2} & \gamma_{g_{1_3}^{-1} g_3} & \dots & \gamma_{g_{1_n}^{-1} g_n} \\ \gamma_{g_{2_1}^{-1} g_1} & \gamma_{g_{2_2}^{-1} g_2} & \gamma_{g_{2_3}^{-1} g_3} & \dots & \gamma_{g_{2_n}^{-1} g_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \gamma_{g_{n_1}^{-1} g_1} & \gamma_{g_{n_2}^{-1} g_2} & \gamma_{g_{n_3}^{-1} g_3} & \dots & \gamma_{g_{n_n}^{-1} g_n} \end{pmatrix} = \Omega(v * w).$$

Thus, multiplication is preserved. This concludes the proof. □

For an element  $v = \sum \alpha_i g_i \in RG$ , define the element  $v^T \in RG$  as  $v^T = \sum \alpha_i g_i^{-1}$ . This is sometimes known as the canonical involution for the group ring.

**Lemma 5.2** *Let  $R$  be a finite commutative Frobenius ring,  $G$  be a group of order  $n$  and  $H_i$  be finite groups of order  $r$  such that  $r$  is a factor of  $n$  with  $n > 1$  and  $n, r \neq 1$ . Then for an element  $v \in RG$ , we have that  $\Omega(v)^T = \Omega(v^T)$ .*

**Proof** The  $ij$ -th elements of  $\Omega(v^T)$  is  $\alpha_{(g_i^{-1} g_j)^{-1}} = \alpha_{g_{j_i}^{-1} g_i}$  which is the  $ji$ -th element of  $\Omega(v)$ . □

**Lemma 5.3** *Let  $R$  be a finite commutative Frobenius ring,  $G$  be a group of order  $n$  and  $H_i$  be finite groups of order  $r$  such that  $r$  is a factor of  $n$  with  $n > 1$  and  $n, r \neq 1$ . If  $v = v^T$  and  $v^2 = 0$  then  $C_v$  is a self-orthogonal code.*

**Proof** If  $v = v^T$  then  $\Omega(v)^T = \Omega(v^T)$  by Lemma 4.2. Then we have that  $(\Omega(v)\Omega(v))_{ij}$  is the inner-product of the  $i$ -th and  $j$ -th rows of  $\Omega(v)$ . Since  $v^2 = 0$ , by Theorem 4.1 we have that  $\Omega(v)\Omega(v) = \mathbf{0}$ . This gives that any two rows of  $\Omega(v)$  are orthogonal and hence they generate a self-orthogonal code. □

**Theorem 5.4** *Let  $R$  be a finite commutative Frobenius ring,  $G$  be a group of order  $n$  and  $H_i$  be finite groups of order  $r$  such that  $r$  is a factor of  $n$  with  $n > 1$  and  $n, r \neq 1$ . Let  $v$  be an element in  $RG$ . If  $v = v^T$ ,  $v^2 = 0$ , and  $|C_v| = |R^{\frac{n}{r}}|$  then  $C_v$  is a self-dual code.*

**Proof** By Lemma 4.3 the code  $C_v$  is self-orthogonal and since  $|C_v| = |R^{\frac{n}{r}}|$ , we have that  $C_v$  is self-dual. □

### 6 Quasi composite G-codes

In this section, we make a generalization of the notion of quasi-G-codes. In [6], the authors have developed a ring with a Gray map that could be used to describe certain families of quasi-cyclic groups. That same ring can be used in this setting to construct quasi-composite G-codes which we shall describe below. Self-dual codes over these rings were studied in [14]. Recently, in [1], the authors study the algebraic structure of quasi-group codes.

Let  $G$  be a finite group of order  $n$  and  $R$  a finite Frobenius commutative ring. Let  $C$  be a code in  $R^{sn}$  where the coordinates can be partitioned into  $n$  sets of size  $s$  where each set is assigned an element of  $G$ . If the code  $C$  is held invariant by the action of multiplying the coordinate set marker by every element of  $G$  then the code  $C$  is called a quasi-composite G-code of index  $s$ .

We now describe a family of rings to construct quasi-composite G-codes.

Let  $p_1, p_2, \dots, p_t$  be prime numbers with  $t \geq 0$  and  $p_i \neq p_j$  if  $i \neq j$ . Define  $\Delta$  to be  $\Delta = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ , for some  $k_i \geq 1, i = 1, \dots, t$ .

The ring is defined as follows:

$$R_{q,\Delta} = \mathbb{F}_q[u_{p_1,1}, \dots, u_{p_1,k_1}, u_{p_2,1}, \dots, u_{p_2,k_2}, \dots, u_{p_t,k_t}] / \langle u_{p_i,j}^{p_i} = 0 \rangle,$$

where the indeterminates  $\{u_{p_i,j}\}_{(1 \leq i \leq t, 1 \leq j \leq k_i)}$  commute.

Let  $i \in \{1, \dots, t\}, j \in \{1, \dots, k_i\}$ . Take the set of exponents  $J_i = \{0, 1, \dots, p_i - 1\}$  for the indeterminant  $u_{p_i,j}$ . For  $\alpha_i \in J_i^{k_i}$  denote  $u_{p_i,1}^{\alpha_i,1} \dots u_{p_i,k_i}^{\alpha_i,k_i}$  by  $u_i^{\alpha_i}$ . For a monomial  $u_1^{\alpha_1} \dots u_t^{\alpha_t}$  in  $R_{q,\Delta}$  write  $u^\alpha$ , where  $\alpha = (\alpha_1, \dots, \alpha_t) \in J_1^{k_1} \times \dots \times J_t^{k_t}$ .

Let  $J = J_1^{k_1} \times \dots \times J_t^{k_t}$ . Any element  $c$  in  $R_{q,\Delta}$  can be written as

$$c = \sum_{\alpha \in J} c_\alpha u^\alpha = \sum_{\alpha \in J} c_\alpha u_{p_1,1}^{\alpha_1,1} \dots u_{p_1,k_1}^{\alpha_1,k_1} \dots u_{p_t,1}^{\alpha_t,1} \dots u_{p_t,k_t}^{\alpha_t,k_t} \tag{13}$$

with  $c_\alpha \in \mathbb{F}_q$ .

It is immediate that  $R_{q,\Delta}$  is a commutative ring with  $|R_{q,\Delta}| = q^{p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}} = q^\Delta$ .

Next we define a Gray map on this ring. We will consider the elements in  $R_{q,\Delta}$  as  $q$ -ary vectors of  $\Delta$  coordinates. Order the elements of  $A_\Delta$  lexicographically and use this ordering to label the coordinate positions of  $\mathbb{F}_q^\Delta$ . Define the Gray map  $\Psi_\Delta : A_\Delta \rightarrow \mathbb{F}_q^\Delta$  as follows:

$$\Psi_\Delta(a)_b = \begin{cases} 1 & \text{if } \widehat{b} \subseteq \{\widehat{a} \cup 1\}, \\ 0 & \text{otherwise,} \end{cases}$$

where  $\Psi_\Delta(a)_b$  indicates the coordinate of  $\Psi_\Delta(a)$  corresponding to the position of the element  $b \in A_\Delta$  with the defined ordering.

It follows that  $\Psi_\Delta(a)_b$  is 1, if each indeterminate  $u_{p_i,j}$  in the monomial  $b$  with non-zero exponent is also in the monomial  $a$  with the same exponent. In other words, it is 1 when  $\widehat{b}$  is a subset of  $\widehat{a}$ . In order to consider all the subsets of  $\widehat{a}$ , we also add the empty subset that is given when  $b = 1$ ; that is we compare  $\widehat{b}$  to  $\widehat{a} \cup 1$ .

Finally, we extend  $\Psi_\Delta$  linearly for all elements of  $R_{q,\Delta}$ . Then  $\Psi_\Delta$  is a Gray map from  $R_{q,\Delta}$  to  $\mathbb{F}_q^\Delta$ .

**Theorem 6.1** *Let  $C$  be a composite G-code in  $R_{q,\Delta}$  for a finite group  $G$  of order  $n$ . Then  $\Psi(C)$  is a quasi-composite G-code of length  $n\Delta$  of index  $\Delta$  in  $\mathbb{F}_q^{\Delta n}$ .*

**Proof** Since  $C$  is a composite G-code in  $R_{q,\Delta}$ , each row of  $C$  corresponds to an element of the form  $v_j = c_{g_{j_1} g_1} g_{j_1} g_1 + c_{g_{j_2} g_2} g_{j_2} g_2 + \dots + c_{g_{j_n} g_n} g_{j_n} g_n$  in  $R_{q,\Delta} G$ , where  $c_{g_{j_i} g_i} \in$

$R_{q,\Delta}$ ,  $g_{j_i}g_i \in G$  and where  $j$  is the  $j$ th row of the code  $\mathcal{C}$ . Then  $\Psi_{\Delta}(v_j) = \Psi_{\Delta}(c_{g_{j_1}g_1})g_{j_1}g_1 + \Psi_{\Delta}(c_{g_{j_2}g_1})g_{j_2}g_2 + \dots + \Psi_{\Delta}(c_{g_{j_n}g_1})g_{j_n}g_n$ . Therefore  $\Psi_{\Delta}(\mathcal{C})$  is a quasi-composite  $G$ -code of length  $n\Delta$  of index  $\Delta$  in  $\mathbb{F}_q^{\Delta n}$ .  $\square$

**Theorem 6.2** *Let  $\mathcal{C}$  be a composite  $G$ -code of length  $n$  and of index  $k$  over  $R_{q,\Delta}$  for a finite group  $G$ . Then  $\Psi_{\Delta}(\mathcal{C})$  is a quasi-composite  $G$ -code of length  $n\Delta$  of index  $k\Delta$  in  $\mathbb{F}_q^{\Delta n}$ .*

**Proof** Since  $\mathcal{C}$  is a composite  $G$ -code in  $R_{q,\Delta}$ , each row of  $\mathcal{C}$  corresponds to an element of the form  $v_j = c_{g_{j_1}g_1}g_{j_1}g_1 + c_{g_{j_2}g_2}g_{j_2}g_2 + \dots + c_{g_{j_n}g_n}g_{j_n}g_n$  in  $R_{q,\Delta}G$ , where  $c_{g_{j_i}g_i} \in R_{q,\Delta}$ ,  $g_{j_i}g_i \in G$  and where  $j$  is the  $j$ th row of the code  $\mathcal{C}$ . Then  $\Psi_{k\Delta}(v_j) = \Psi_{k\Delta}(c_{g_{j_1}g_1})g_{j_1}g_1 + \Psi_{k\Delta}(c_{g_{j_2}g_2})g_{j_2}g_2 + \dots + \Psi_{k\Delta}(c_{g_{j_n}g_n})g_{j_n}g_n$ . Therefore  $\Psi_{\Delta}(\mathcal{C})$  is a quasi-composite  $G$ -code of length  $n\Delta$  of index  $k\Delta$  in  $\mathbb{F}_q^{\Delta n}$ .  $\square$

### 7 Generator matrices of the form $[I_n \mid \Omega(v)]$

In this section, we consider generator matrices of the form  $[I_n \mid \Omega(v)]$  to construct extremal binary self-dual codes. This approach was used in [10] and [11] where only groups of orders 4, 8 and 16 were considered to form the matrices  $\Omega(v)$ . In both papers: [10] and [11], the authors define a specific generator matrices of the form  $[I_n \mid \Omega(v)]$  for lengths 8 and 16. The authors also prove theoretical results on when these matrices produce self-dual codes over the Frobenius ring  $R$ . We generalize the theoretical results so that we show when the generator matrices of the form  $[I_n \mid \Omega(v)]$  produce self-dual codes for any possible case rather than looking at individual cases for specific composite matrices  $\Omega(v)$ . Before the theoretical results, we give a motivating example in which we compare the generator matrix of the form  $[I_n \mid \sigma(v)]$  with a generator matrix of the form  $[I_n \mid \Omega(v)]$ .

**Example 4** Let  $G = \langle x, y \mid x^8 = y^2 = 1, x^y = x^{-1} \rangle \cong D_{16}$ . Also let  $v = \sum_{i=0}^7 \sum_{j=0}^1 \alpha_{1+i+8j} x^i y^j \in \mathbb{F}_2 D_{16}$ , then

$$\sigma(v) = \begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix},$$

where  $A = \text{circ}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7, \alpha_8)$ ,  $B = \text{circ}(\alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12}, \alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha_{16})$  and  $\alpha_i \in \mathbb{F}_2$ . We now employ the generator matrix of the form  $[I_{16} \mid \sigma(v)]$  to search for binary self-dual codes with parameters [32, 16, 8]. We summarise the results in a table.

$\mathcal{C}_i$	Type	First row of $A$	First row of $B$	$ Aut(\mathcal{C}_i) $
$\mathcal{C}_1$	II	(0, 0, 0, 0, 0, 1, 0, 1)	(0, 0, 0, 1, 1, 1, 1, 1)	$2^{15} \cdot 3^2 \cdot 5 \cdot 7$
$\mathcal{C}_2$	I	(0, 0, 0, 0, 0, 1, 1, 1)	(0, 1, 0, 1, 1, 1, 1, 1)	$2^{15} \cdot 3^2$
$\mathcal{C}_3$	II	(0, 0, 0, 0, 1, 1, 1, 1)	(0, 0, 0, 1, 0, 0, 1, 1)	$2^5 \cdot 3 \cdot 5 \cdot 31$

**Example 5** We now amend  $\sigma(v)$  from the previous example by forming a composite matrix. Let  $G = \langle x, y \mid x^8 = y^2 = 1, x^y = x^{-1} \rangle \cong D_{16}$  and  $v = \sum_{i=0}^7 \sum_{j=0}^1 \alpha_{1+i+8j} x^i y^j \in$



$$\begin{aligned}
 B_1 &= \text{circ}(\alpha_5, \alpha_6, \alpha_7, \alpha_8), \\
 A_2 &= \text{circ}(\alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12}), \\
 B_2 &= \text{circ}(\alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha_{16}), \\
 A_3 &= \text{circ}(\alpha_9, \alpha_{16}, \alpha_{15}, \alpha_{14}), \\
 B_3 &= \text{circ}(\alpha_{13}, \alpha_{12}, \alpha_{11}, \alpha_{10}), \\
 A_4 &= \text{circ}(\alpha_1, \alpha_8, \alpha_7, \alpha_6), \\
 B_4 &= \text{circ}(\alpha_5, \alpha_4, \alpha_3, \alpha_2)
 \end{aligned}$$

and where  $\alpha_i \in \mathbb{F}_2$ . We now employ the generator matrix of the form  $[I_{16} \mid \Omega(v)]$  to search for binary self-dual codes with parameters  $[32, 16, 8]$ . We summarise the results in a table.

$C_i$	Type	$r_{A_1}$	$r_{B_1}$	$r_{A_2}$	$r_{B_2}$	$r_{A_3}$	$r_{B_3}$	$r_{A_4}$	$r_{B_4}$	$ Aut(C_i) $
$C_1$	II	(0, 0, 1, 0)	(0, 0, 1, 0)	(0, 0, 1, 0)	(1, 1, 1, 1)	(0, 1, 1, 1)	(1, 0, 1, 0)	(0, 0, 1, 0)	(0, 0, 1, 0)	$2^9 \cdot 3^2 \cdot 5$

The order of the automorphism group of the code obtained in Example 7 is different from the order of automorphism of codes obtained in Example 6. This shows that the composite matrices can be used to produce codes whose structure is not attainable from matrices of the form  $[I_n \mid \sigma(v)]$  or other classical techniques for producing extremal binary self-dual codes. In fact, this is the main motivating factor for this construction, that is, we construct codes whose automorphism group differs from other constructions which means we find codes that are inaccessible from other techniques.

**Theorem 7.1** *Let  $R$  be a finite commutative Frobenius ring,  $G$  be a group of order  $n$  and  $H_i$  be finite groups of order  $r$  such that  $r$  is a factor of  $n$  with  $n > 1$  and  $n, r \neq 1$ . Let  $v \in RG$  and let  $\Omega(v)$  be the corresponding composite matrix over  $R$ . The matrix  $G = [I_n \mid \Omega(v)]$  generates a self-dual code  $\mathcal{C}$  over  $R$  if and only if  $\Omega(v)\Omega(v)^T = -I_n$ .*

**Proof** The code  $\mathcal{C}$  is self-dual if and only if  $GG^T$  is the zero matrix over  $R$ . Now,

$$GG^T = [I_n \mid \Omega(v)][I_n \mid \Omega(v)]^T = [I_n \mid \Omega(v)\Omega(v)^T].$$

Thus,  $GG^T$  is the zero matrix over  $R$  if and only if  $\Omega(v)\Omega(v)^T = -I_n$ . □

We saw earlier in the work that  $\Omega(v^T) = \Omega(v)^T$ . Now using Theorem 7.1, the fact that  $\Omega$  is a ring homomorphism, and the fact that  $\Omega(v) = -I_n$  if and only if  $v = -1$ , we get the following corollary.

**Corollary 7.2** *Let  $R$  be a finite commutative Frobenius ring,  $G$  be a group of order  $n$  and  $H_i$  be finite groups of order  $r$  such that  $r$  is a factor of  $n$  with  $n > 1$  and  $n, r \neq 1$ . Let  $v \in RG$  and let  $\Omega(v)$  be the corresponding composite matrix over  $R$ . The matrix  $[I_n \mid \Omega(v)]$  generates a self-dual code over  $R$  if and only if  $vv^T = -1$ . In particular  $v$  has to be a unit.*

When we consider a ring of characteristic 2, we have  $-I_n = I_n$ , which leads to the following further important result:

**Corollary 7.3** *Let  $R$  be a finite commutative Frobenius ring of characteristic 2,  $G$  be a group of order  $n$  and  $H_i$  be finite groups of order  $r$  such that  $r$  is a factor of  $n$  with  $n > 1$  and*



$n, r \neq 1$ . Let  $v \in RG$  and let  $\Omega(v)$  be the corresponding composite matrix over  $R$ . Then the matrix  $[I_n \mid \Omega(v)]$  generates a self-dual code over  $R$  if and only if  $v$  satisfies  $vv^t = 1$ , namely  $v$  is a unitary unit in  $RG$ .

### 7.1 New extremal self-dual binary codes of length 68

In this section, we search for extremal binary self-dual codes of length 68 using the generator matrix described in the previous section with some other well-known techniques. We focus on this particular length, since there are still many Type I unknown codes of this length, i.e., codes of length 68 with parameters in their weight enumerators that are not known in the literature. Recently, much work has been done to find new, extremal, Type I binary self-dual codes of length 68, see [8, 10–12, 17] for some examples. We now describe our approach.

We apply the generator matrix of the form  $[I \mid \Omega(v)]$  over the ring  $\mathbb{F}_4 + u\mathbb{F}_4$  to find extremal self-dual codes whose binary images are the extremal self-dual binary codes of length 64. We then apply a very well known extension method to obtain codes of length 68. Similar approach can be found in [10]. We next apply a very recent technique, called a neighbor of a neighbor method (please see [18] for details), to find a family of neighbours which turn out to be extremal self-dual binary codes of length 68 with parameters not known in the literature before. In particular we find new codes of length 68 with the rare parameters of  $\gamma = 7, 8, 9$ . We split this section into the following subsections. In the first one, we describe the ring  $\mathbb{F}_4 + u\mathbb{F}_4$  and give the most up to date list of codes of length 68 with parameters known in the literature. Then we define the generator matrix of the form  $[I \mid \Omega(v)]$ , which we use to find codes of length 64. We then extend these codes to obtain codes of length 68. Finally, we apply the family of neighbours method to find codes of length 68 with parameters not known in the literature.

#### 7.1.1 The ring $\mathbb{F}_4 + u\mathbb{F}_4$ , the extension and neighbour methods

Let us recall the following Gray Maps from [16] and [7]:

$$\begin{aligned} \psi_{\mathbb{F}_4} : (\mathbb{F}_4)^n &\rightarrow (\mathbb{F}_2)^{2n} & \left| \begin{array}{l} \varphi_{\mathbb{F}_2+u\mathbb{F}_2} : (\mathbb{F}_2 + u\mathbb{F}_2)^n \rightarrow \mathbb{F}_2^{2n} \\ a\omega + b\bar{\omega} \mapsto (a, b), a, b \in \mathbb{F}_2^n \end{array} \right. & \left| \begin{array}{l} \varphi_{\mathbb{F}_4+u\mathbb{F}_4} : (\mathbb{F}_4 + u\mathbb{F}_4)^n \rightarrow \mathbb{F}_4^{2n} \\ a + bu \mapsto (b, a + b), a, b \in \mathbb{F}_2^n. \end{array} \right. \end{aligned}$$

In [24], these maps were generalized to the following Gray maps:

$$\begin{aligned} \psi_{\mathbb{F}_4+u\mathbb{F}_4} : (\mathbb{F}_4 + u\mathbb{F}_4)^n &\rightarrow (\mathbb{F}_2 + u\mathbb{F}_2)^{2n} & \left| \begin{array}{l} \varphi_{\mathbb{F}_4+u\mathbb{F}_4} : (\mathbb{F}_4 + u\mathbb{F}_4)^n \rightarrow \mathbb{F}_4^{2n} \\ a\omega + b\bar{\omega} \mapsto (a, b), a, b \in (\mathbb{F}_2 + u\mathbb{F}_2)^n \end{array} \right. & \left| \begin{array}{l} \varphi_{\mathbb{F}_4+u\mathbb{F}_4} : (\mathbb{F}_4 + u\mathbb{F}_4)^n \rightarrow \mathbb{F}_4^{2n} \\ a + bu \mapsto (b, a + b), a, b \in \mathbb{F}_4^n. \end{array} \right. \end{aligned}$$

**Proposition 7.4** ([24]) *Let  $C$  be a code over  $\mathbb{F}_4 + u\mathbb{F}_4$ . If  $C$  is self-orthogonal, then so are  $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$  and  $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ . The code  $C$  is a Type I (resp. Type II) code over  $\mathbb{F}_4 + u\mathbb{F}_4$  if and only if  $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$  is a Type I (resp. Type II)  $\mathbb{F}_4$ -code, if and only if  $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$  is a Type I (resp. Type II)  $\mathbb{F}_2 + u\mathbb{F}_2$ -code. Furthermore, the minimum Lee weight of  $C$  is the same as the minimum Lee weight of  $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$  and  $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ .*

The next corollary follows immediately from the proposition and we will use this result repeatedly to produce binary codes.

**Corollary 7.5** *Suppose that  $C$  is a self-dual code over  $\mathbb{F}_4 + u\mathbb{F}_4$  of length  $n$  and minimum Lee distance  $d$ . Then  $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$  is a binary  $[4n, 2n, d]$  self-dual code. Moreover, the Lee weight enumerator of  $C$  is equal to the Hamming weight enumerator of  $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ . If  $C$  is Type I (Type II), then so is  $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ .*

For the computational results in later sections, we are going to use the following extension method to obtain codes of length  $n + 2$ .

**Theorem 7.6** [15] *Let  $\mathcal{C}$  be a self-dual code of length  $n$  over a commutative Frobenius ring with identity  $R$  and  $G = (r_i)$  be a  $k \times n$  generator matrix for  $\mathcal{C}$ , where  $r_i$  is the  $i$ -th row of  $G$ ,  $1 \leq i \leq k$ . Let  $c$  be a unit in  $R$  such that  $c^2 = -1$  and  $X$  be a vector in  $S^n$  with  $\langle X, X \rangle = -1$ . Let  $y_i = \langle r_i, X \rangle$  for  $1 \leq i \leq k$ . The following matrix*

$$\left[ \begin{array}{cc|c} 1 & 0 & X \\ \hline y_1 & cy_1 & r_1 \\ \vdots & \vdots & \vdots \\ y_k & cy_k & r_k \end{array} \right]$$

*generates a self-dual code  $\mathcal{D}$  over  $R$  of length  $n + 2$ .*

We will also apply the neighbor method and its generalization to search for new extremal binary self-dual codes from codes obtained directly from our constructions or from the described above, extension method. Two self-dual binary codes of length  $2n$  are said to be neighbors of each other if their intersection has dimension  $n - 1$ . Let  $x \in \mathbb{F}_2^{2n} - \mathcal{C}$  then  $\mathcal{D} = \langle x \rangle^\perp \cap \mathcal{C}, x \rangle$  is a neighbour of  $\mathcal{C}$ .

Recently in [18], the neighbor method has been extended and the following formula for constructing the  $k^{th}$ -range neighbour codes was provided:

$$\mathcal{N}_{(i+1)} = \langle x_i \rangle^\perp \cap \mathcal{N}_{(i)}, x_i \rangle,$$

where  $\mathcal{N}_{(i+1)}$  is the neighbour of  $\mathcal{N}_{(i)}$  and  $x_i \in \mathbb{F}_2^{2n} - \mathcal{N}_{(i)}$ .

There are two possibilities for the weight enumerators of extremal singly-even  $[64, 32, 12]_2$  codes ([4]):

$$\begin{aligned} W_{64,1} &= 1 + (1312 + 16\beta)y^{12} + (22016 - 64\beta)y^{14} + \dots, \quad 14 \leq \beta \leq 284, \\ W_{64,2} &= 1 + (1312 + 16\beta)y^{12} + (23040 - 64\beta)y^{14} + \dots, \quad 0 \leq \beta \leq 277. \end{aligned}$$

Recently, many new codes are constructed for both weight enumerators in [17], [22] and [29].

The weight enumerator of a singly-even, self-dual  $[68, 34, 12]_2$  code is in one of the following forms by [3,20]:

$$\begin{aligned} W_{68,1} &= 1 + (442 + 4\beta)y^{12} + (10864 - 8\beta)y^{14} + \dots, \\ W_{68,2} &= 1 + (442 + 4\beta)y^{12} + (14960 - 8\beta - 256\gamma)y^{14} + \dots, \end{aligned}$$

where  $\beta$  and  $\gamma$  are parameters and  $0 \leq \gamma \leq 9$ . The first examples of codes with a  $\gamma = 7$  in  $W_{68,2}$  are constructed in [28]. Many codes for different values of  $\beta$  and  $\gamma$  have been constructed in [8,12,17,19,27,28]. The first examples of codes with  $\gamma = 8, 9$  in  $W_{68,2}$  are constructed in [18]. For an up-to-date list of all known Type I binary self-dual codes with parameters  $[64, 32, 12]$  and  $[68, 43, 12]$  please see [23].

### 7.1.2 The generator matrix

We now define the generator matrix of the form  $[I \mid \Omega(v)]$  which we then employ to search for self-dual codes over the ring  $\mathbb{F}_4 + u\mathbb{F}_4$ . Of course,  $I$  is simply the identity matrix so we define  $\Omega(v)$ .

Let  $G = \langle x, y \mid x^4 = y^2 = 1, x^y = x^{-1} \rangle \cong D_8$ . Let  $v = \alpha_1 + \alpha_x x + \alpha_{x^2} x^2 + \alpha_{x^3} x^3 + \alpha_y y + \alpha_{xy} xy + \alpha_{x^2 y} x^2 y + \alpha_{x^3 y} x^3 y \in RD_8$ , where  $\alpha_{g_i} \in R$ . Let  $H_1 = \langle a, b \mid a^2 = b^2 = 1, ab = ba \rangle \cong C_2 \times C_2$  and  $H_2 = \langle c \mid c^4 = 1 \rangle \cong C_4$ . We now define  $\Omega(v)$  as:

$$\Omega(v) = \begin{pmatrix} A'_1 & A'_2 \\ A'_3 & A'_4 \end{pmatrix} = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \alpha_{g_1^{-1}g_3} & \alpha_{g_1^{-1}g_4} & \alpha_{g_1^{-1}g_5} & \alpha_{g_1^{-1}g_6} & \alpha_{g_1^{-1}g_7} & \alpha_{g_1^{-1}g_8} \\ \alpha_{\phi_1((h_2)_2^{-1}(h_2)_1)} & \alpha_{\phi_1((h_2)_2^{-1}(h_2)_2)} & \alpha_{\phi_1((h_2)_2^{-1}(h_2)_3)} & \alpha_{\phi_1((h_2)_2^{-1}(h_2)_4)} & \alpha_{\phi_2((h_1)_2^{-1}(h_1)_1)} & \alpha_{\phi_2((h_1)_2^{-1}(h_1)_2)} & \alpha_{\phi_2((h_1)_2^{-1}(h_1)_3)} & \alpha_{\phi_2((h_1)_2^{-1}(h_1)_4)} \\ \alpha_{\phi_1((h_2)_3^{-1}(h_2)_1)} & \alpha_{\phi_1((h_2)_3^{-1}(h_2)_2)} & \alpha_{\phi_1((h_2)_3^{-1}(h_2)_3)} & \alpha_{\phi_1((h_2)_3^{-1}(h_2)_4)} & \alpha_{\phi_2((h_1)_3^{-1}(h_1)_1)} & \alpha_{\phi_2((h_1)_3^{-1}(h_1)_2)} & \alpha_{\phi_2((h_1)_3^{-1}(h_1)_3)} & \alpha_{\phi_2((h_1)_3^{-1}(h_1)_4)} \\ \alpha_{\phi_1((h_2)_4^{-1}(h_2)_1)} & \alpha_{\phi_1((h_2)_4^{-1}(h_2)_2)} & \alpha_{\phi_1((h_2)_4^{-1}(h_2)_3)} & \alpha_{\phi_1((h_2)_4^{-1}(h_2)_4)} & \alpha_{\phi_2((h_1)_4^{-1}(h_1)_1)} & \alpha_{\phi_2((h_1)_4^{-1}(h_1)_2)} & \alpha_{\phi_2((h_1)_4^{-1}(h_1)_3)} & \alpha_{\phi_2((h_1)_4^{-1}(h_1)_4)} \\ \alpha_{g_5^{-1}g_1} & \alpha_{g_5^{-1}g_2} & \alpha_{g_5^{-1}g_3} & \alpha_{g_5^{-1}g_4} & \alpha_{g_5^{-1}g_5} & \alpha_{g_5^{-1}g_6} & \alpha_{g_5^{-1}g_7} & \alpha_{g_5^{-1}g_8} \\ \alpha_{\phi_3((h_2)_2^{-1}(h_2)_1)} & \alpha_{\phi_3((h_2)_2^{-1}(h_2)_2)} & \alpha_{\phi_3((h_2)_2^{-1}(h_2)_3)} & \alpha_{\phi_3((h_2)_2^{-1}(h_2)_4)} & \alpha_{\phi_4((h_1)_2^{-1}(h_1)_1)} & \alpha_{\phi_4((h_1)_2^{-1}(h_1)_2)} & \alpha_{\phi_4((h_1)_2^{-1}(h_1)_3)} & \alpha_{\phi_4((h_1)_2^{-1}(h_1)_4)} \\ \alpha_{\phi_3((h_2)_3^{-1}(h_2)_1)} & \alpha_{\phi_3((h_2)_3^{-1}(h_2)_2)} & \alpha_{\phi_3((h_2)_3^{-1}(h_2)_3)} & \alpha_{\phi_3((h_2)_3^{-1}(h_2)_4)} & \alpha_{\phi_4((h_1)_3^{-1}(h_1)_1)} & \alpha_{\phi_4((h_1)_3^{-1}(h_1)_2)} & \alpha_{\phi_4((h_1)_3^{-1}(h_1)_3)} & \alpha_{\phi_4((h_1)_3^{-1}(h_1)_4)} \\ \alpha_{\phi_3((h_2)_4^{-1}(h_2)_1)} & \alpha_{\phi_3((h_2)_4^{-1}(h_2)_2)} & \alpha_{\phi_3((h_2)_4^{-1}(h_2)_3)} & \alpha_{\phi_3((h_2)_4^{-1}(h_2)_4)} & \alpha_{\phi_4((h_1)_4^{-1}(h_1)_1)} & \alpha_{\phi_4((h_1)_4^{-1}(h_1)_2)} & \alpha_{\phi_4((h_1)_4^{-1}(h_1)_3)} & \alpha_{\phi_4((h_1)_4^{-1}(h_1)_4)} \end{pmatrix}$$

where:

$$\begin{aligned} \phi_1 : (h_2)_i &\xrightarrow{\phi_1} g_1^{-1} g_i & \phi_2 : (h_1)_i &\xrightarrow{\phi_2} g_1^{-1} g_j \\ \text{for } i = \{1, 2, 3, 4\} & & \text{for when } \{i = 1, j = 5, i = 2, j = 6, i = 3, j = 7, i = 4, j = 8\} & \\ \phi_3 : (h_1)_i &\xrightarrow{\phi_1} g_5^{-1} g_i & \phi_4 : (h_1)_i &\xrightarrow{\phi_2} g_5^{-1} g_j \\ \text{for } i = \{1, 2, 3, 4\} & & \text{for when } \{i = 1, j = 5, i = 2, j = 6, i = 3, j = 7, i = 4, j = 8\} & \end{aligned}$$

in  $A'_1, A'_2, A'_3$  and  $A'_4$ . This results in a composite matrix over  $R$  of the following form:

$$\Omega(v) = \begin{pmatrix} \alpha_1 & \alpha_x & \alpha_{x^2} & \alpha_{x^3} & \alpha_y & \alpha_{xy} & \alpha_{x^2 y} & \alpha_{x^3 y} \\ \alpha_x & \alpha_1 & \alpha_{x^3} & \alpha_{x^2} & \alpha_{xy} & \alpha_y & \alpha_{x^3 y} & \alpha_{x^2 y} \\ \alpha_{x^3} & \alpha_{x^2} & \alpha_1 & \alpha_x & \alpha_{x^2 y} & \alpha_{x^3 y} & \alpha_y & \alpha_{xy} \\ \alpha_{x^2} & \alpha_{x^3} & \alpha_x & \alpha_1 & \alpha_{x^3 y} & \alpha_{x^2 y} & \alpha_{xy} & \alpha_y \\ \hline \alpha_y & \alpha_{x^3 y} & \alpha_{x^2 y} & \alpha_{xy} & \alpha_1 & \alpha_{x^3} & \alpha_{x^2} & \alpha_x \\ \alpha_{x^3 y} & \alpha_y & \alpha_{xy} & \alpha_{x^2 y} & \alpha_{x^3} & \alpha_1 & \alpha_x & \alpha_{x^2} \\ \alpha_{x^2 y} & \alpha_{xy} & \alpha_y & \alpha_{x^3 y} & \alpha_{x^2} & \alpha_x & \alpha_1 & \alpha_{x^3} \\ \alpha_{xy} & \alpha_{x^2 y} & \alpha_{x^3 y} & \alpha_y & \alpha_x & \alpha_{x^2} & \alpha_{x^3} & \alpha_1 \end{pmatrix} \tag{14}$$

Therefore, the final form of the generator matrix which we later employ to search for self-dual codes has the following form:

$$[I \mid \Omega(v)], \tag{15}$$

where  $\Omega(v)$  is the composite matrix defined in (14).

### 7.1.3 Computational results

We now employ the generator matrix defined in (15) over the ring  $\mathbb{F}_4 + u\mathbb{F}_4$  to search for codes of length 16 whose binary images are the extremal self-dual codes of length 64. In fact, we only list one of the codes found. This code in turn is used to find new extremal binary self-dual codes of length 68. All the upcoming computational results were obtained by performing the searches using MAGMA ([2]).

We now apply Theorem 7.6 to the  $\psi_{\mathbb{F}_4+u\mathbb{F}_4}$ -image of the code in Table 1. As a result, we were able to find many extremal self-dual codes of length 68 but to save space, we only list one. This code is found in Table 2, where  $1 + u$  in  $\mathbb{F}_2 + u\mathbb{F}_2$ , is denoted by 3.

The order of the automorphism group of the code in Table 2 is 2. We note that the code from Table 2 has parameters that are not new in the literature.

**Table 1** Type I Codes of length 64 and their  $\beta$  values

$C_i$	$(\alpha_1, \alpha_x, \alpha_{x^2}, \alpha_{x^3}, \alpha_y, \alpha_{xy}, \alpha_{x^2y}, \alpha_{x^3y})$	$ Aut(C_i) $	$W_{64,2}$
1	$(0, w, u + 1, u + 1, u, wu + u, w, wu + u + 1)$	$2^4$	$\beta = 0$

**Table 2** Type I Codes of length 68 from Theorem 7.6

$C_{68,i}$	$C_i$	$c$	$X$	$\gamma$	$\beta$
$C_{68,1}$	$C_1$	1	$(0, 3, 3, u, 3, 1, 3, 3, 3, 3, 1, 1, 0, 3, 3, 1, 3, 1, 0, u, 1, 3, u, 3, 0, 1, 3, u, 3, 0, 3, 1)$	4	103

**Table 3**  $i^{th}$  neighbour of  $\mathcal{N}_{(0)}$

$i$	$\mathcal{N}_{(i+1)}$	$x_i$	$\gamma$	$\beta$
0	$\mathcal{N}_{(1)}$	(111101101001110111111100100111110)	4	101
1	$\mathcal{N}_{(2)}$	(01101001001111011110111111011011)	6	145
2	$\mathcal{N}_{(3)}$	(000010000010000011101110110000101)	7	152
3	$\mathcal{N}_{(4)}$	(111111100000010000111001100101011)	<b>7</b>	<b>143</b>
4	$\mathcal{N}_{(5)}$	(011001001010011011011110101111111)	8	162
5	$\mathcal{N}_{(6)}$	(110000101101111100111110010001011)	9	174
6	$\mathcal{N}_{(7)}$	(1110010010100011111100101110001100)	<b>9</b>	<b>167</b>
7	$\mathcal{N}_{(8)}$	(001100000000110110101001101100000)	<b>9</b>	<b>159</b>
8	$\mathcal{N}_{(9)}$	(1001101110001110110000111101000011)	<b>9</b>	<b>158</b>
9	$\mathcal{N}_{(10)}$	(1001011111100101110001001011110110)	<b>9</b>	<b>157</b>
10	$\mathcal{N}_{(11)}$	(101010110110110110111011111111010)	<b>9</b>	<b>152</b>
11	$\mathcal{N}_{(12)}$	(1111010110110000110111011010101010)	7	<b>131</b>
12	$\mathcal{N}_{(13)}$	(100001111111101111011000101010010)	<b>6</b>	<b>117</b>

We now apply the  $k^{th}$  range neighbour formula (mentioned earlier) to the code obtained in Table 2.

Let  $\mathcal{N}_{(0)} = \mathcal{C}$  where  $\mathcal{C}$  is the extremal binary self dual code of length 68 with parameters  $\beta = 103$  and  $\gamma = 4$ . Applying the  $k^{th}$  range formula, we obtain (Table 3):

We shall now separately consider the neighbours of  $\mathcal{N}_{(7)}, \mathcal{N}_{(8)}, \mathcal{N}_{(10)}, \mathcal{N}_{(11)}, \mathcal{N}_{(12)}$  and  $\mathcal{N}_{(13)}$ . We tabulate the results below. All the codes in Table 4 have an automorphism group of order 1. The codes in bold in Tables 3 and 4 indicate codes with new parameters, i.e., codes with these values in their weight enumerators were not known in the literature before.

As we can see, we were able to construct many extremal binary self-dual codes of length 68 with new weight enumerators for the rare parameters  $\gamma = 7, 8$  and  $9$ .

### 8 Conclusion

In this paper, we have extended the idea of  $G$ -codes to composite  $G$ -codes. We have shown that similarly as the  $G$ -codes, the composite  $G$ -codes are also ideals in the group ring  $RG$ . We have shown that the dual of a composite  $G$ -code is also a  $G$ -code. We have studied self-orthogonal and self-dual composite  $G$ -codes over rings. Moreover, we have extended

**Table 4** New codes of length 68 as neighbors

$\mathcal{N}_{(t)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, \dots, x_{68})$	$\gamma$	$\beta$	$\mathcal{N}_{(t)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, \dots, x_{68})$	$\gamma$	$\beta$
7		(0001000010111101010000011101000110)	7	141	7		(0100101001111001101010101010101110)	8	150
7		(0111001010000000100011000001011100)	8	151	7		(100110010100110101101111000011101101)	8	152
7		(001110011101010101011101100100)	9	164	7		(10000000100110000010100001010100011)	9	165
7		(00100101110000010011110000000000)	9	166	7		(00101010010100101010101010000000011)	9	168
7		(10001010010110100001001000100010)	9	170	7		(0110110001000000000110000010011110)	9	172
$\mathcal{N}_{(t)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, \dots, x_{68})$	$\gamma$	$\beta$	$\mathcal{N}_{(t)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, \dots, x_{68})$	$\gamma$	$\beta$
8		(01111001010101111001111101111011)	7	134	8		(10000011010100000010110110100010)	7	135
8		(1111010100000001100101001000000)	7	136	8		(111100011010000101100110111110)	7	137
8		(001000001100110010010010001100001)	7	138	8		(111100100110111001001100101001100)	7	139
8		(101101100110011011101100100011000)	8	144	8		(1111101100101100011011111010010)	8	147
8		(001100010101010000101101010100101)	8	148	8		(011011000000011001011001110100110)	8	149
8		(0001101100111000101110011001001001)	9	160	8		(1000001000111101010110000101010001)	9	161
8		(1110100010110010110000010010000101)	9	162	8		(0100011010001111001111101001011111)	9	163
$\mathcal{N}_{(t)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, \dots, x_{68})$	$\gamma$	$\beta$	$\mathcal{N}_{(t)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, \dots, x_{68})$	$\gamma$	$\beta$
10		(1101100110001000101001101111000)	7	132	10		(111100011010101010101010101000011)	8	143
10		(111010011011100010101000101011)	8	145	10		(001011110110011010000101100011110)	8	146
10		(1011010011010100001010001001011010)	9	156					
$\mathcal{N}_{(t)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, \dots, x_{68})$	$\gamma$	$\beta$	$\mathcal{N}_{(t)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, \dots, x_{68})$	$\gamma$	$\beta$
11		(010100010110011001100101000111100)	8	139	11		(101111110010000110111000010111100)	8	140
11		(110001100100011100000011011010110)	8	141	11		(1101111101101000011011111011101101)	9	151
11		(000110011110011010110111001111010)	9	154	11		(010010011110100100101010111000001)	9	155

**Table 4** continued

$\mathcal{N}_{(t)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, \dots, x_{68})$	$\gamma$	$\beta$	$\mathcal{N}_{(t)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, \dots, x_{68})$	$\gamma$	$\beta$
12		(11000111001011001111011110111001101100)	6	121	12		(1111100111100011111001011110101111)	6	123
12		(00011010000010111101010000001100001)	6	124	12				
$\mathcal{N}_{(t)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, \dots, x_{68})$	$\gamma$	$\beta$	$\mathcal{N}_{(t)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, \dots, x_{68})$	$\gamma$	$\beta$
13		(01011100110011010000010010000001000)	5	110	13		(10110111001101110110010111010101001)	6	120
13		(1000111010010011011000110000101011)	6	122	13				

the results on quasi- $G$ -codes to quasi-composite  $G$ -codes. We have also generalized results on self-dual codes obtained from generator matrices of the form  $[I \mid \Omega(v)]$ , where  $\Omega(v)$  is the composite matrix. Additionally in this work, we were able to construct the following extremal binary self-dual codes with new weight enumerators in  $W_{68,2}$ :

$$(\gamma = 5, \beta = \{110\}).$$

$$(\gamma = 6, \beta = \{117, 120, 121, 122, 123, 124\}).$$

$$(\gamma = 7, \beta = \{131, 132, 134, 135, 136, 137, 138, 139, 141, 143\}).$$

$$(\gamma = 8, \beta = \{139, 140, 141, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152\}).$$

$$(\gamma = 9, \beta = \{151, 152, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 170, 172\}).$$

A suggestion for future work would be to consider composite matrices of greater lengths to search for extremal binary self dual codes over different rings. For example, one may consider our approach to search for extremal binary self-dual codes of length 80. Another direction is to determine which codes are composite  $G$ -codes for a finite group  $G$ .

**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

## References

1. Borello M., Wolfgang W.: On the Algebraic Structure of Quasi Group Codes. [arXiv:1912.09167](https://arxiv.org/abs/1912.09167).
2. Bosma W., Cannon J., Playoust C.: The Magma algebra system. I. The user language. *J. Symb. Comput.* **24**, 235–265 (1997).
3. Buyuklieva S., Boukliev I.: Extremal self-dual codes with an automorphism of order 2. *IEEE Trans. Inf. Theory* **44**, 323–328 (1998).
4. Conway J.H., Sloane N.J.A.: A new upper bound on the minimal distance of self-dual codes. *IEEE Trans. Inf. Theory* **36**(6), 1319–1333 (1990).
5. Dougherty S.T.: *Algebraic Coding Theory Over Finite Commutative Rings*. SpringerBriefs in MathematicsSpringer, Cham (2017).
6. Dougherty S.T., Fernandez-Cordoba D., Ten-Valls R.: Quasi-cyclic codes as cyclic codes over a family of local rings. *Finite Fields Appl.* **40**, 138–149 (2016).
7. Dougherty S.T., Gaborit P., Harada M., Sole P.: Type II codes over  $\mathbb{F}_2 + u\mathbb{F}_2$ . *IEEE Trans. Inf. Theory* **45**, 32–45 (1999).
8. Dougherty S.T., Gildea J., Kaya A.: Quadruple bordered constructions of self-dual codes from group rings over Frobenius rings. *Cryptogr. Commun.* (2019). <https://doi.org/10.1007/s12095-019-00380-8>.
9. Dougherty S.T., Gildea J., Korban A.: Extending an established isomorphism between group rings and a subring of the  $n \times n$  matrices. *Int. J. Algebra Comput.* <https://doi.org/10.1142/S0218196721500223>.
10. Dougherty S.T., Gildea J., Korban A., Kaya A.: Composite constructions of self-dual codes from group rings and new extremal self-dual binary codes of length 68. *Adv. Math. Commun.* (2019). <https://doi.org/10.3934/amc.2020037>.
11. Dougherty S.T., Gildea J., Korban A., Kaya A.: New extremal self-dual binary codes of length 68 via composite construction,  $\mathbb{F}_2 + u\mathbb{F}_2$  lifts, extensions and neighbors. *Int. J. Inf. Coding Theory* **5**(3/4), 211–226 (2020).

12. Dougherty S.T., Gildea J., Korban A., Kaya A., Tylshchak A., Yildiz B.: Bordered constructions of self-dual codes from group rings. *Finite Fields Appl.* **57**, 108–127 (2019).
13. Dougherty S.T., Gildea J., Taylor R., Tylshchak A.: Group rings, G-codes and constructions of self-dual and formally self-dual codes. *Des. Codes Cryptogr.* **86**(9), 2115–2138 (2018).
14. Dougherty S.T., Kaya A., Salutrak E.: Constructions of self-dual codes and formally self-dual codes over rings. *AAECC* (2016). <https://doi.org/10.1007/s00s00-016-0288-5>.
15. Dougherty S.T., Kim J.L., Kulosman H., Liu H.: Self-dual codes over commutative Frobenius rings. *Finite Fields Appl.* **16**(1), 14–26 (2010).
16. Gaborit P., Pless V., Sole P., Atkin O.: Type II codes over  $\mathbb{F}_4$ . *Finite Fields Appl.* **8**, 171–183 (2002).
17. Gildea J., Kaya A., Korban A., Yildiz B.: Constructing self-dual codes from group rings and reverse circulant matrices. *Adv. Math. Commun.* <https://doi.org/10.3934/amc.2020077>.
18. Gildea J., Kaya A., Korban A., Yildiz B.: New extremal binary self-dual codes of length 68 from generalized neighbours. *Finite Fields Appl.* **67** (2020).
19. Gildea J., Kaya A., Taylor R., Yildiz B.: Constructions for self-dual codes induced from group rings. *Finite Fields Appl.* **51**, 71–92 (2018).
20. Harada M., Munemasa A.: Some restrictions on weight enumerators of singly even self-dual codes. *IEEE Trans. Inf. Theory* **52**, 1266–1269 (2006).
21. Hurley T.: Group rings and rings of matrices. *Int. J. Pure Appl. Math.* **31**(3), 319–335 (2006).
22. Kaya A.: New extremal binary self-dual codes of lengths 64 and 66 from  $R_2$ -lifts. *Finite Fields Appl.* **46**, 271–279 (2017).
23. Korban A.: All known type I binary [64, 32, 12] and [68, 34, 12] self-dual codes. <https://sites.google.com/view/adriankorban/binary-self-dual-codes>.
24. Ling S., Sole P.: Type II codes over  $\mathbb{F}_4 + u\mathbb{F}_4$ . *Eur. J. Comb.* **22**, 983–997 (2001).
25. Milies C.P., Sehgal S.K.: *An Introduction to Group Rings*. Kluwer, Dordrecht (2002).
26. Sehgal S.K.: *Units in Integral Group Rings*. Longman, Essex (1993).
27. Yankov N., Lee M.H., Gurel M., Ivanova M.: Self-dual codes with an automorphism of order 11. *IEEE Trans. Inf. Theory* **61**(3), 1188–1193 (2015).
28. Yankov N., Ivanova M., Lee M.H.: Self-dual codes with an automorphism of order 7 and s-extremal codes of length 68. *Finite Fields Appl.* **51**, 17–30 (2018).
29. Yankov N., Anev D.: On the self-dual codes with an automorphism of order 5. *AAECC* (2019). <https://doi.org/10.1007/s00200-019-00403-0>.