University of Chester

A thesis submitted for the degree of Doctor of Philosophy in Mathematics

Group Codes, Composite Group Codes and Constructions of Self-Dual Codes

Author: Adrian Korban

Supervisor: Dr. Joe Gildea

Department of Mathematical and Physical Sciences

August 11, 2021

Contents

Abstract

The main research presented in this thesis is around constructing binary self-dual codes using group rings together with some well-known code construction methods and the study of group codes and composite group codes over different alphabets. Both these families of codes are generated by the elements that come from group rings.

A search for binary self-dual codes with new weight enumerators is an ongoing research area in algebraic coding theory. For this reason, we present a generator matrix in which we employ the idea of a bisymmetric matrix with its entries being the block matrices that come from group rings and give the necessary conditions for this generator matrix to produce a self-dual code over a finite commutative Frobenius ring. Together with our generator matrix and some well-known code construction methods, we find many binary self-dual codes with parameters $[68, 34, 12]$ that have weight enumerators that were not known in the literature before.

There is an extensive literature on the study of different families of codes over different alphabets and specifically finite fields and finite commutative rings. The study of codes over rings opens up a new direction for constructing new binary self-dual codes with a rich automorphism group via the algebraic structure of the rings through the Gray maps associated with them. In this thesis, we introduce a new family of rings, study its algebraic structure and show that each member of this family is a commutative Frobenius ring. Moreover, we study group codes over this new family of rings and show that one can obtain codes with a rich automorphism group via the associated Gray map.

We extend a well established isomorphism between group rings and the subring of the $n \times n$ matrices and show its applications to algebraic coding theory. Our extension enables one to construct many complex $n \times n$ matrices over the ring R that are fully defined by the elements appearing in the first row. This property allows one to build generator matrices with these complex matrices so that the search field is practical in terms of the computational times. We show how these complex matrices are constructed using group rings, study their properties and present many interesting examples of complex matrices over the ring R.

Using our extended isomorphism, we define a new family of codes which we call the composite group codes or for simplicity, composite G-codes. We show that these new codes are ideals in the group ring RG and prove that the dual of a composite G-code is also a composite G-code. Moreover, we study generator matrices of the form $[I_n \mid \Omega(v)]$, where I_n is the $n \times n$ identity matrix and $\Omega(v)$ is the composite matrix that comes from the extended isomorphism mentioned earlier. In particular, we show when such generator matrices produce self-dual codes over finite commutative Frobenius rings. Additionally, together with some generator matrices of the type $[I_n \mid \Omega(v)]$ and the well-known extension and neighbour methods, we find many new binary self-dual codes with parameters $[68, 34, 12]$.

Lastly in this work, we study composite G-codes over formal power series rings and finite chain rings. We extend many known results on projections and lifts of codes over these alphabets. We also extend some known results on γ-adic codes over the infinite ring R_∞.

Acknowledgements

First and foremost, I would like to thank my supervisor, Dr. Joe Gildea, for his ongoing support, invaluable guidance and feedback. I am thankful for his commitment, effort and time. I am extremely grateful for his understanding he has shown in allowing me to study in my own way while working full time.

I would also like to thank the following academics for their commitment, help and guidance; Prof. Steven Dougherty, Dr. Abidin Kaya, Dr. Alexander Tylyshchak, Prof. Bahattin Yildiz and Dr. Serap Sahinkaya. I am grateful for their valuable feedback and time when working on joint projects.

Lastly, I would like to thank my parents and family for their ongoing support and encouragement, and my partner, Patrycja, for her support and understanding.

Chapter 1

Introduction

In this thesis, we mainly study codes over rings. We give the standard definitions and results on codes and codes over rings required to understand the work presented in later chapters, however, it is assumed that the reader is familiar with the basic definitions, results and notation from group theory, ring and module theory, algebraic coding theory and linear algebra. Most of the chapters in this thesis are work either submitted or accepted for publication. We now give a brief summary of each chapter.

Chapter 1: In this chapter, we give the standard definitions and results on rings, codes over rings and finite fields. We recall some known techniques such as; the extension and neighbour methods, for constructing codes over rings that we employ in later chapters of this work. We also give the definitions of some well-known matrices and recall the definitions and basic results on group rings. We next recall an established isomorphism between group rings and a subring of the $n \times n$ matrices. We finally present the definition and some results on group codes over finite commutative Frobenius rings.

Chapter 2: In the second chapter, we present a generator matrix in which we employ the idea of a bisymmetric matrix whose entries are the block matrices that come from group rings. We give the necessary conditions that this generator matrix has to meet in order to produce a self-dual code over a finite commutative Frobenius ring of characteristic 2. We also construct, together with our generator matrix, the well-known extension and neighbour methods, new binary self-dual codes with parameters $[68, 34, 12]$. This chapter is joint work with Dr. Joe Gildea, Dr. Abidin Kaya and Dr. Alexander Tylyshchak. The results presented in this chapter are published in [35].

Chapter 3: This chapter is joint work with Prof. Steven Dougherty, Dr. Joe Gildea and Dr. Serap Sahinkaya. Here, we introduce a new family of finite commutative Frobenius rings, $\mathcal{B}_{j,k}$, whose base field is the finite field $\mathbb{F}_{p^r}$ and study its algebraic structure. We study group codes, self-dual group codes and reversible group codes over this new family of rings. We define a Gray map for the new family of rings and study projections and lifts of group codes under this Gray map. Moreover, we show that the Gray images of the group codes have a rich automorphism group. The work presented in this chapter has been accepted for publication and is to appear in the *Cryptography and Communications, Discrete Structures, Boolean Functions and Sequences* journal.

Chapter 4: In this chapter, which is joint work with Prof. Steven Dougherty and Dr. Joe Gildea, we extend the well established isomorphism between group rings and a subring of the $n \times n$ matrices. Our extension enables one to construct complex $n \times n$ matrices over the ring R which have applications in algebraic coding theory as we show in later chapters. We present a number of theoretical results on the extended isomorphism and give many interesting examples of the complex matrices. The results presented in this chapter are published in [18].

Chapter 5: Here, we define composite group codes which are codes generated by the group ring elements. We study the algebraic properties of these codes and we also study self-dual composite group codes. Moreover, we present a generator matrix which consists of the extended isomorphism and show when such generator matrix produces self-dual codes over finite commutative Frobenius rings of characteristic 2. We also construct, together with the generator matrix, the well-known extension and neighbour methods, new binary self-dual codes with parameters $[68, 34, 12]$. This chapter is joint work with Prof. Steven Dougherty, Dr. Joe Gildea and Dr. Abidin Kaya, and can be found in [21].

Chapter 6: In this chapter, we give an application of the extended isomorphism from Chapter 4 and the generator matrices from Chapter 5. Namely, we define a number of generator matrices using the extended isomorphism with groups of orders 8 and 4 and give the conditions for which each generator produces self-dual codes over a finite commutative Frobenius ring. Together with these generator matrices, the well-known extension and neighbour methods, we construct new binary self-dual codes with parameters $[68, 34, 12]$. This chapter is joint work with Prof. Steven Dougherty, Dr. Joe Gildea and Dr. Abidin Kaya, and can be found in [19].

Chapter 7: Here, we study composite group codes over formal power series rings and finite chain rings. We show that these codes are ideals in the group ring $R_\infty G$ and that the dual of a composite group code is also a composite group code in this setting. Moreover, we study projections and lifts of composite group codes over finite chain rings and over formal power series rings. Additionally, we extend some known results on γ- adic group codes over R_∞ to composite group codes and study these codes over principal ideal rings. The work presented in this chapter is published in [56].

Chapter 8: In the final chapter of this work, we summarise the work and results presented in this thesis. We highlight the importance of the results presented in all the previous chapters and critically examine what could have been done differently. We also give possible directions for future research as either extensions of applications of the results presented in this thesis.

1.1 Self-Dual Codes

The study of self-dual codes over finite fields and rings is an ongoing research area in coding theory. This is mainly due to their connections to other areas in Mathematics such as; combinatorics, design theory and number theory. In [2], it is shown that one can produce interesting designs using self-dual codes over fields. In [3], it is shown that one of the most powerful techniques for producing optimal unimodular lattices uses self-dual codes over rings. Moreover, the well-known proof of the non-existence of the projective plane of order 10 used the theory of binary self-dual codes, please see [57] for a complete explanation of this proof.

Self-dual codes are also interesting in their own rite – the construction and enumeration of binary self-dual codes of different lengths have gained the attention from many people. It is a well-known fact that a binary self-dual code must have an even length, dimension of half its length and a minimum weight d (please see [49] for details). We refer to such a code as a binary $[2n, n, d]$ self-dual code. The desirable property of a binary self-dual code is that it has the maximum value of d for a given length $2n$. It is well-known that a linear code with the minimum distance d can detect up to $d-1$ or correct up to $\lfloor\frac{(d-1)}{2}\rfloor$ errors in any codeword (please see [49] for details), this is why, in a binary self-dual code, we want the value of d to be as large as possible for a given length. The bounds for the minimum distance d of self-dual codes, for certain values of n, are given in [62]. A traditional, and probably the most known technique for constructing binary self-dual codes is to consider a generator matrix of the form $(I_n \mid A)$, where I_n is the $n \times n$ identity matrix and A is some $n \times n$ matrix over the finite field of order 2, usually defined by the elements appearing in the first row. Please see [39, 55] for some examples of this technique. Another known technique to construct binary self-dual codes with is to consider generator matrices that produce codes with a fixed order of the automorphism group, please see [65, 66, 67] for very detailed examples of this approach. In early 1990s, a series of landmark papers [7, 45, 46] were published which showed that linear codes can be obtained as images, under a Gray map, of codes over rings. Since then, many researchers have studied codes over different rings (commutative and non-commutative) and their associated Gray maps which can lead to constructing new binary self-dual codes. In [64], J. Wood, shows that the class of rings that are an acceptable alphabet for coding theory and the study of linear codes, is the class of Frobenius rings. This is because the two foundational and well-known MacWilliams Theorems apply to this particular class of rings, please see [60] for a detailed description of these two theorems and why they are so important in coding theory. One can see [24], for some examples of Frobenius rings and their associated Gray maps. Some interesting examples of constructing binary self-dual codes from codes over rings via their associated Gray maps can be found in [25, 26].

In this thesis, we want to give more possible ways of constructing new binary self-dual codes that were not known in the literature before. For this reason, we introduce new ideas and extend existing techniques to obtain new extremal binary self-dual codes of length 68. We present a number of generator matrices of the form $(I_n \mid A)$, where I_n is the $n \times n$ identity matrix and A is an $n \times n$ matrix over a finite commutative Frobenius ring, derived from group rings, and fully defined by the elements appearing in the first row. Additionally, we give a generator matrix in which the identity matrix is replaced with a block matrix and the matrix A is replaced with a 4×4 bisymmetric matrix where the blocks come from group rings. We use these generator matrices together with some well-known code construction methods, to obtain many self-dual codes over a finite commutative Frobenius ring, whose binary images, under some Gray maps, are self-dual codes of length 68 with new parameters in their weight enumerators. We next extend a well established isomorphism between group rings and a subring of the $n \times n$ matrices so that one can construct very complex matrices over any ring. We use this extended isomorphism to introduce a new family of codes, called composite group codes which are generated from group ring elements, where the ring is a finite commutative Frobenius ring. We show that binary self-dual with parameters $[72, 36, 16]$ cannot have the form of a composite group code. Moreover, we present a new family of finite Frobenius rings, give its associated Gray map and we study group codes, self-dual group codes and reversible group codes over this new family of Frobenius rings. Additionally, we study the new family of codes, the composite group codes over formal power series rings and finite chain rings and show that one can construct an infinite family of composite group codes from just one composite group code.

1.2 Rings and Codes over Rings

In this work, we study different families of codes over finite commutative rings. That is, we shall assume throughout this text that a ring has a multiplicative identity and that the multiplication is commutative.

We start by recalling some basic definitions on rings, codes and codes over rings to understand the notation used in later chapters.

Definition 1. *([33]) Let R be a ring.*

*(1) A non-zero element a of R is called a **zero-divisor** if there is a non-zero element b in R such that either $ab = 0$ or $ba = 0$.*

*(2) Assume R has an identity $1 \neq 0$. An element u of R is called a **unit** in R if there is some v in R such that $uv = vu = 1$. The set of units of R is denoted by $U(R)$.*

Definition 2. *([33]) Let $M_n(R)$ denote the **ring of** $n \times n$ **matrices** with coefficients from R.*

Definition 3. *([33]) The **characteristic** of a ring R is the smallest positive integer n such that $1 + 1 + \cdots + 1 = 0$ (n times) in R; if no such integer exists the characteristic of R is said to be 0.*

Definition 4. *([33]) Let R be a ring, let I be a subset of R and let $r \in R$.*

(1) $rI = \{ra \mid a \in I\}$ and $Ir = \{ar \mid a \in I\}$.

*(2) A subset I of R is a **left ideal** of R if*

(i) I is a subring of R, and

(ii) I is closed under left multiplication by elements from R, i.e. $rI \subseteq I$ for all $r \in R$.

*Similarly I is a **right ideal** if (i) holds and in place of (ii) one has*

(ii)' I is closed under right multiplication by elements from R, i.e. $Ir \subseteq I$ for all $r \in R$.

*(3) A subset I that is both a left ideal and a right ideal is called an **ideal** (or, for added emphasis, a **two-sided ideal**) of R.*

Definition 5. *([12]) An ideal $\mathfrak{a}$ is **maximal** if $\mathfrak{a}$ is not properly contained in any non-trivial ideal.*

Definition 6. *([12]) Let $\mathfrak{a}$ be an ideal of a finite commutative ring. We call the smallest $t \geq 1$ such that $\mathfrak{a}^t = \mathfrak{a}^{t+i}$ for $i \geq 0$ the **index of stability** of $\mathfrak{a}$.*

Definition 7. *([12]) A **principal ideal** ring is a ring in which each ideal is generated by a single element, that is every ideal $\mathfrak{a}$ can be written as $\mathfrak{a} = \langle a \rangle$ for some element a.*

Definition 8. *([12]) A **chain ring** is a principal ideal ring such that the ideals are linearly ordered by set theoretic containment.*

Definition 9. *([33]) Let R and S be rings.*

*(1) A **ring homomorphism** is a map $\varphi : R \to S$ satisfying*

(i) $\varphi(a+b) = \varphi(a) + \varphi(b)$ *for all* $a, b \in R$ *and*

(ii) $\varphi(ab) = \varphi(a)\varphi(b)$ *for all* $a, b \in R$.

(2) *The* ***kernel*** *of the ring homomorphism* φ, *denoted ker* φ, *is the set of elements of* R *that map to* 0 *in* S.

(3) *A bijective ring homomorphism is called an* ***isomorphism***.

In some of the later chapters, we use the generalised Chinese Remainder Theorem to prove some results with. For this reason, we now recall it.

Theorem 1. *([12]) Let* R *be a finite commutative ring, with maximal ideals* $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ *where the index of stability of* $\mathfrak{m}_i$ *is* e_i. *Then the map* $\Psi : R \to \prod_{i=1}^{s} R/\mathfrak{m}_i^{e_i}$, *defined by* $\Psi(x) = (x + \mathfrak{m}_1^{e_i}, \ldots, x + \mathfrak{m}_s^{e_s})$, *is a ring isomorphism.*

Definition 10. *([33]) Let* R *be a ring. A* ***left R-module*** *or a* ***left module over R*** *is a set* M *together with*

(1) *a binary operation* $+$ *on* M *under which* M *is an abelian group,*

(2) *an action of* R *on* M *(that is, a map* $R \times M \to M$*) denoted by* rm, *for all* $r \in R$ *and for all* $m \in M$ *which satisfies*

(a) $(r+s)m = rm + sm$, *for all* $r, s \in R, m \in M$,

(b) $(rs)m = r(sm)$, *for all* $r, s \in R, m \in M$,

(c) $r(m+n) = rm + rn$, *for all* $r \in R, m, n \in M$, *and*

(d) $1m = m$, *for all* $m \in M$.

The description "left"in the above definition indicates that the ring elements appear on the left; "right"R-modules can be defined analogously.

Definition 11. *([33]) Let* R *be a ring and* M *be a left* R*-module. For any submodule* N *of* M, *the* ***annihilator*** *of* N *is the ideal of* R *defined by*

$$Ann(N) = \{r \in R \mid rn = 0 \text{ for all } n \in N\}.$$

Definition 12. *([33]) Let* R *be a ring and let* M *and* N *be* R*-modules.*

(1) *A map* $\varphi : M \to N$ *is an* ***R-module homomorphism*** *if it respects the* R*-module structures of* M *and* N, *i.e.*

(a) $\varphi(x+y) = \varphi(x) + \varphi(y)$, *for all* $x, y \in M$ *and*

(b) $\varphi(\alpha x) = \alpha\varphi(x)$, *for all* $\alpha \in R, x \in M$.

(2) *An R-module homomorphism is an* ***isomorphism*** *(of R-modules) if it is both injective and surjective. The modules M and N are said to be isomorphic, denoted $M \cong N$, if there is some R-module isomorphism $\varphi : M \to N$.*

(3) *If $\varphi : M \to N$ is an R-module homomorphism, let ker $\varphi = \{m \in M \mid \varphi(m) = 0\}$ (the kernel of φ) and let $\varphi(M) = \{n \in N \mid n = \varphi(m)$ for some $m \in M\}$ (the image of φ, as usual).*

(4) *Let M and N be R-modules and define $Hom_R(M, N)$ to be the set of all R-module homomorphism from M into N.*

We now give a description of Frobenius rings. We specifically show how one can ensure that a ring is indeed a Frobenius ring. These tools will be used in one of the later chapters.

Definition 13. *([12]) Let M be the R-module. A* ***character*** *χ is a homomorphism given by $\chi : M \to \mathbb{C}^*$. We define $\widehat{M} = Hom_M(M, \mathbb{C}^*)$ to be the set of all characters associated to M. We note that this set forms a multiplicative abelian group. If M is a left R-module over a ring R, then the character group $\widehat{M}$ is a right R-module called the* ***character module*** *associated to M. The module action in the character module for $\chi \in \widehat{M}$ is defined by*

$$\chi^r(m) = \chi(rm)$$

for all $m \in M$ and $r \in R$. The character module can also be defined in the same way for right R-modules.

Theorem 2. *([12]) Suppose R is a finite ring. The following are equivalent:*

(1) *The ring R is* ***Frobenius****.*

(2) *As a left module, $\widehat{R} \cong {}_R R$.*

(3) *As a right module, $\widehat{R} \cong R_R$.*

Example 1.2.1. *The ring $\mathbb{Z}_p$, where p is an integer is a Frobenius ring. The direct product of the two rings $\mathbb{Z}_n$ and $\mathbb{Z}_m$, where n and m are integers, is a Frobenius ring. For example, the ring $\mathbb{Z}_{16}$ is a Frobenius ring of order 16. The ring $\mathbb{Z}_8 \times \mathbb{Z}_2$ is a Frobenius ring of order 16.*

Definition 14. *([12]) Let R be a Frobenius ring. Let $\phi : R \to \widehat{R}$ be the module isomorphism. Set $\chi = \phi(1)$ so that $\phi(r) = \chi^r$ for $r \in R$. We call this character χ a* ***generating character*** *for $\widehat{R}$.*

Theorem 3. *([12]) The finite commutative ring R is Frobenius if and only if $\widehat{R}$ has a generating character.*

Theorem 4. *([12]) Let χ be a character of a finite commutative ring R. Then χ is a generating character if and only if ker (χ) contains no non-zero ideals of R.*

Example 1.2.2. *Consider the following Frobenius ring $\mathbb{Z}_{16}$ of order 16. Its generating character is given by $\chi(a) = \zeta^a$ where $\zeta = e^{\frac{2\pi i}{16}}$.*

We now give the basic definitions on codes over finite commutative Frobenius rings. We study codes specifically over this family of rings since both MacWilliams theorems for codes over finite fields extend to Frobenius rings. We now state these two fundamental theorems.

Theorem 5. *([60]) Let $\mathcal{C}$ be a linear code over a finite field $\mathbb{F}$, then every Hamming isometry $\mathcal{C} \to \mathbb{F}^n$ can be extended to a monomial transformation.*

This theorem allows us to define an equivalence on codes effectively as codes where one can be transformed into the other via a monomial tranformation. In general, we want to study codes up to this equivalence.

Theorem 6. *([60]) Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$ then*

$$W_{\mathcal{C}^\perp}(x, y) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(x + (q-1)y, x - y).$$

With this theorem, we are able to give the weight enumerator of the orthogonal of a code from the weight enumerator of a linear code.

In [64], J. Wood showed that the above two very important theorem for codes over finite fields extend to codes over commutative Frobenius rings. This is why in this thesis, we restrict our attention to this family of rings. Please see [12] for a very detailed explanation of the two MacWilliams theorems. From now on, unless otherwise stated, we use R to represent a finite commutative Frobenius ring.

Definition 15. *([12]) A* ***code*** *$\mathcal{C}$ over R of length n is a subset of R^n. If the code is a submodule of R^n, then we say that the code is* ***linear****. If a code is a k-dimensional submodule of R^n, then the code is denoted as an $[n, k]$ linear code over R, where n is the length of the code and k is the number of rows. The rows of the code $\mathcal{C}$ are called* ***codewords****.*

Definition 16. *([12]) Let $\mathcal{C}$ be a linear code over R. Then, the* ***orthogonal*** *of $\mathcal{C}$ is defined as:*

$$\mathcal{C}^\perp = \{\mathbf{v} \in R^n \mid [\mathbf{v}, \mathbf{w}] = 0, \ \forall \mathbf{w} \in \mathcal{C}\},$$

where $[\mathbf{v}, \mathbf{w}] = \sum v_i w_i$ is the Euclidean inner-product.

Definition 17. *([12]) A code $\mathcal{C}$ is said to be* ***self-orthogonal*** *if $\mathcal{C} \subseteq \mathcal{C}^\perp$ and* ***self-dual*** *if $\mathcal{C} = \mathcal{C}^\perp$.*

Definition 18. *([12]) Two codes $\mathcal{C}$ and $\mathcal{C}'$ are **equivalent** if $\mathcal{C}'$ can be formed from $\mathcal{C}$ by permuting the coordinates of $\mathcal{C}$.*

Definition 19. *([12]) The **automorphism group** of a code $\mathcal{C}$, denoted $Aut(G)$, consists of all permutations of the coordinates of the code that fix the code.*

Definition 20. *([12]) The **Hamming weight** of a vector $\mathbf{v} \in R^n$ defined as*

$$wt_H(\mathbf{v}), \tag{1.1}$$

is the number of non-zero entries of $\mathbf{v}$. The minimum Hamming weight of a code $\mathcal{C}$ is $min\{wt_H(\mathbf{v}) \mid \mathbf{v} \in C, \mathbf{v} \neq \mathbf{0}\}$, where $\mathbf{0}$ is the all-zero vector.

Definition 21. *([50]) A self-dual code $\mathcal{C}$ for which all the codewords have Hamming weight divisible by four is called a **Type II** or **doubly-even** code. Otherwise $\mathcal{C}$ is called a **Type I** or **singly-even** code.*

Definition 22. *([12]) The **minimum distance** d of a code $\mathcal{C}$ over R is the minimum of all the Hamming weights.*

An $[n, k, d]$-code over R is an $[n, k]$-code over R with minimum distance d.

Definition 23. *([50]) A **generator matrix** for an $[n, k]$-code $\mathcal{C}$ is any $k \times n$ matrix G whose rows form basis for $\mathcal{C}$.*

Since in this work, we present a number of generator matrices for binary self-dual codes, we now recall the well-known upper bounds on the minimum Hamming distance of such codes.

Theorem 7. *([62]) Let $d_I(n)$ and $d_{II}(n)$ be the minimum distances of a Type I and Type II binary self-dual code of length n, respectively. Then*

$$d_{II}(n) \leq 4\lfloor\frac{n}{24}\rfloor + 4$$

and

$$d_I(n) \leq \begin{cases} 4\lfloor\frac{n}{24}\rfloor + 4 & if\ n \not\equiv 22 \pmod{24} \\ 4\lfloor\frac{n}{24}\rfloor + 6 & if\ n \equiv 22 \pmod{24}. \end{cases}$$

Definition 24. *([50]) Self-dual codes meeting these bounds are called **extremal**. Self-dual codes with the largest d for a specific length n are said to be **optimal**. Extremal codes are necessarily optimal but optimal codes are not necessarily extremal.*

Definition 25. *([12]) Let $\mathcal{C}$ be a code over $R = \{a_0, a_1, \ldots, a_{r-1}\}$. The **complete weight enumerator** for the code $\mathcal{C}$ is defined as:*

$$cwe_{\mathcal{C}}(x_{a_0}, x_{a_1}, \ldots, x_{a_{r-1}}) = \sum_{\mathbf{c}\in\mathcal{C}} \prod_{i=0}^{r-1} x_{a_i}^{n_i(\mathbf{c})}, \tag{1.2}$$

where there are $n_i(\mathbf{c})$ occurrences of a_i in the vector $\mathbf{c}$.

Definition 26. *([12]) A **Gray map** is a distance preserving map to the binary Hamming space.*

The Gray images of codes over rings tend to have a rich automorphism group which arises from the algebraic structure of the rings. This means that one can construct codes over a family of rings whose binary images are codes with parameters that can not be obtained from other classical techniques. For example, in [24] and [26], it is shown that the binary images of self-dual codes over a certain family of rings have automorphism groups whose orders are multiples of 2^k, please see [24] and [26] for details.

Corollary 1.2.1. *([12]) If $\mathcal{C}$ is a linear code over a finite commutative Frobenius ring R, with $|R| = r$, then $|\mathcal{C}||\mathcal{C}^{\perp}| = |R^n|$.*

We notice that the above corollary generalises the theorem which states that for linear codes over fields $dim(\mathcal{C}) + dim(\mathcal{C}^{\perp}) = n$, where n is the dimension of the ambient space - this is one of the main differences between linear codes over finite fields and finite commutative Frobenius rings. That is, for linear codes over finite fields we can employ the results from vector spaces while for linear codes over Frobenius rings we need results from ring and module theory. Please see [12] for a detailed description of the differences. The differences between self-dual codes over finite fields and Frobenius rings are that they have applications in different areas of Mathematics. For example, self-dual codes over fields can be used to produce interesting designs (please see [2] for details) while self-dual codes over Frobenius rings can produce optimal unimodular lattices (please see [3] for details).

1.2.1 Codes over the Rings $R_1 = \mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$

In some of the later chapters, we obtain codes over some particular families of commutative Frobenius rings of characteristic 2, known in the literature. For this reason, in this section, we recall the definitions and key results on these families of rings. We start with the family of rings that were defined in [24] and [26].

Definition 27. *([24]) Define the ring R_k for $k \geq 1$ as*

$$R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle u_i^2 = 0, u_i u_j = u_j u_i \rangle. \tag{1.3}$$

These rings are commutative Frobenius rings of characteristics 2 and $|R_k| = 2^{2^k}$.

When $k = 0$, then $R_0 = \mathbb{F}_2$. When $k = 1$, then $R_1 = \mathbb{F}_2 + u_1\mathbb{F}_2$ or just $R_1 = \mathbb{F}_2 + u\mathbb{F}_2$. When $k = 2$, then $R_2 = \mathbb{F}_2 + u_1\mathbb{F}_2 + u_2\mathbb{F}_2 + u_1u_2\mathbb{F}_2$, and so on.

Lemma 1.2.2. *([24]) An element γ of R_k that is a unit satisfies $\gamma^2 = 1$. An element α of R_k that is a non-unit satisfies $\alpha^2 = 0$.*

We now define the Gray map associated to R_k.

Definition 28. *([24]) Let $c \in R_k$, then c can be written as $c = a + bu_{k-1}$, where $a, b \in R_{k-1}$. The Gray map $\phi_k : R_k \to \mathbb{F}_2^{2^k}$ is defined as:*

$$\phi_k(c) = (\phi_{k-1}(b), \phi_{k-1}(a+b)). \tag{1.4}$$

This map is a distance preserving map.

Theorem 8. *([26]) Let $\mathcal{C}$ be a self-dual code over R_k, then $\phi_k(\mathcal{C})$ is a binary self-dual code of length $2^k n$.*

We now recall the basic definitions and results on the ring $\mathbb{F}_4 + u\mathbb{F}_4$.

Definition 29. *([58]) Let $\mathbb{F}_4 = \mathbb{F}_2(\omega)$ be the quadratic field extension of $\mathbb{F}_2$, where $\omega^2 + \omega + 1 = 0$. The ring*

$$\mathbb{F}_4 + u\mathbb{F}_4 = \mathbb{F}_4[u]/\langle u^2 = 0 \rangle, \tag{1.5}$$

is a commutative Frobenius ring of size 16 and characteristic 2. Moreover, it is isomorphic to $\mathbb{F}_2[\omega, u]/\langle u^2 = 0, \omega^2 + \omega + 1 = 0 \rangle$.

The ring $\mathbb{F}_4 + u\mathbb{F}_4$ can be viewed as an extension of the ring $\mathbb{F}_2 + u\mathbb{F}_2$ and so we can express any element of $\mathbb{F}_4 + u\mathbb{F}_4$ in the form $a\omega + b\overline{\omega}$ uniquely, where $a, b \in \mathbb{F}_2 + u\mathbb{F}_2$ and $\overline{\omega} = \omega^2$.

We now give the Gray maps for the ring $\mathbb{F}_4 + u\mathbb{F}_4$. The following two maps were defined and studied in [13, 34].

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

In [58], the above maps were generalized to the following:

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

It was also shown in [58] that the above Gray maps preserve orthogonality in their respective alphabets. Combining the results from [34] and [58] we have that if $\mathcal{C} \subseteq (\mathbb{F}_4 + u\mathbb{F}_4)^n$, then the binary codes: $\varphi_{\mathbb{F}_2 + u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4 + u\mathbb{F}_4}(\mathcal{C})$ and $\psi_{\mathbb{F}_4} \circ \varphi_{\mathbb{F}_4 + u\mathbb{F}_4}(\mathcal{C})$ are equivalent to each other.

Definition 30. *([58]) The **Lee weight** of an element in $\mathbb{F}_4 + u\mathbb{F}_4$ is defined to be the Hamming weight of its binary image.*

Definition 31. *([58]) Let $\mathbf{c}$ and $\mathbf{c}'$ be two codewords in $(\mathbb{F}_4 + u\mathbb{F}_4)^n$. The **Lee distance** of two codewords $\mathbf{c}$ and $\mathbf{c}'$ is the Lee weight of $\mathbf{c} - \mathbf{c}'$.*

Proposition 1.2.3. *([58]) Let $\mathcal{C}$ be a code over $\mathbb{F}_4 + u\mathbb{F}_4$. If $\mathcal{C}$ is self-orthogonal, then so are $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$ and $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$. The code $\mathcal{C}$ is a Type I (resp. Type II) code over $\mathbb{F}_4 + u\mathbb{F}_4$ if and only if $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$ is a Type I (resp. Type II) $\mathbb{F}_4$-code, if and only if $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$ is a Type I (resp. Type II) $\mathbb{F}_2 + u\mathbb{F}_2$-code. Furthermore, the minimum Lee weight of $\mathcal{C}$ is the same as the minimum Lee weight of $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$ and $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$.*

The next corollary follows immediately from the proposition and we will use this result in some of the later chapters to produce binary self-dual codes.

Corollary 1.2.4. *([58]) Suppose that $\mathcal{C}$ is a self-dual code over $\mathbb{F}_4 + u\mathbb{F}_4$ of length n and minimum Lee distance d. Then $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$ is a binary $[4n, 2n, d]$ self-dual code. Moreover, the Lee weight enumerator of $\mathcal{C}$ is equal to the Hamming weight enumerator of $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$. If $\mathcal{C}$ is Type I (Type II), then so is $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(\mathcal{C})$.*

Throughout this work, we use the following notation for the elements of $\mathbb{F}_4 + u\mathbb{F}_4$:

$$0 \leftrightarrow 0000, 1 \leftrightarrow 0001, 2 \leftrightarrow 0010, 3 \leftrightarrow 0011,$$

$$4 \leftrightarrow 0100, 5 \leftrightarrow 0101, 6 \leftrightarrow 0110, 7 \leftrightarrow 0111,$$

$$8 \leftrightarrow 1000, 9 \leftrightarrow 1001, A \leftrightarrow 1010, B \leftrightarrow 1011,$$

$$C \leftrightarrow 1100, D \leftrightarrow 1101, E \leftrightarrow 1110, F \leftrightarrow 1111.$$

We use the ordered basis $\{u\omega, \omega, u, 1\}$ to express the elements of $\mathbb{F}_4 + u\mathbb{F}_4$. For instance, $1 + u\omega$ corresponds to 1001, which is represented by the hexadecimal 9.

We finish this section by recalling some well-known techniques for obtaining self-dual codes. We employ these techniques in some of the later chapters.

Theorem 9. *([28]) Let $\mathcal{C}$ be a self-dual code of length n over 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 $n + 2$.

Definition 32. *([37]) Two binary self-dual codes of length $2k$ are said to be **neighbours** if their intersection has dimension $k - 1$. Let $\mathcal{C}$ be a binary self-dual code of length $2k$ and $x \in \mathbb{F}_2^{2k} - \mathcal{C}$ then $\mathcal{D} = \left\langle \langle x\rangle^{\perp} \cap \mathcal{C}, x \right\rangle$ is a neighbour of $\mathcal{C}$.*

The above definition was extended in [37] to the following.

Definition 33. *([37]) Let $\mathcal{N}_{(0)}$ be a binary self-dual code of length $2n$. Let $x_0 \in \mathbb{F}_2^{2n} - \mathcal{N}_{(0)}$. The the i^{th}**-range neighbour** is defined as:*

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

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

1.2.2 Codes over Formal Power Series Rings and Finite Chain Rings

We recall the definitions and properties of a finite chain ring R and the formal power series ring R_∞.

Definition 34. *([30, 31]) A ring is called a **chain ring** if its ideals are linearly ordered by inclusion. In particular, this means that any finite chain ring has a unique maximal ideal. Let R be a finite chain ring. Denote the unique maximal ideal of R by $\mathfrak{m}$, and let $\tilde{\gamma}$ be the generator of the unique maximal ideal $\mathfrak{m}$. This gives that $\mathfrak{m} = \langle \tilde{\gamma} \rangle = R\tilde{\gamma}$, where $R\tilde{\gamma} = \langle \tilde{\gamma} \rangle = \{\beta\tilde{\gamma} \mid \beta \in R\}$. We have the following chain of ideals:*

$$R = \langle \tilde{\gamma}^0 \rangle \supseteq \langle \tilde{\gamma}^1 \rangle \supseteq \cdots \supseteq \langle \tilde{\gamma}^i \rangle \supseteq \cdots . \tag{1.6}$$

The chain in (1.6) can not be infinite, since R is finite. Therefore, there exists i such that $\langle \tilde{\gamma}^i \rangle = \{0\}$. Let e be the minimal number such that $\langle \tilde{\gamma}^e \rangle = \{0\}$. The number e is called the nilpotency index of $\tilde{\gamma}$. This gives that for a finite chain ring we have the following:

$$R = \langle \tilde{\gamma}^0 \rangle \supseteq \langle \tilde{\gamma}^1 \rangle \supseteq \cdots \supseteq \langle \tilde{\gamma}^e \rangle. \tag{1.7}$$

If the ring R is infinite then the chain in Equation (1.6) is also infinite.

Lemma 1.2.5. *([30, 31]) Let $R^\times$ denote the multiplicative group of all units in the ring R. Let $\mathbb{F} = R/\mathfrak{m} = R/\langle \tilde{\gamma} \rangle$ be the residue field with characteristic p, where p is a prime number, then $|\mathbb{F}| = q = p^r$ for some integers q and r. We know that $|\mathbb{F}^\times| = p^r - 1$.*

Lemma 1.2.6. *([59]) For any $0 \neq r \in R$ there is a unique integer i, $0 \leq i < e$, where e is the nilpotency index of $\tilde{\gamma}$, such that $r = \mu\tilde{\gamma}^i$, with μ a unit. The unit μ is unique modulo $\tilde{\gamma}^{e-i}$.*

Lemma 1.2.7. *([59]) Let R be a finite chain ring with maximal ideal $\mathfrak{m} = \langle \tilde{\gamma} \rangle$, where $\tilde{\gamma}$ is a generator of $\mathfrak{m}$ with nilpotency index e. Let $V \subseteq R$ be a set of representatives for the equivalence classes of R under congruence modulo $\tilde{\gamma}$. Then*

(i) for all $r \in R$ there are unique $r_0, \cdots, r_{e-1} \in V$ such that $r = \sum_{i=0}^{e-1} r_i\tilde{\gamma}^i$;

(ii) $|V| = |\mathbb{F}|$;

(iii) $|\langle \tilde{\gamma}^j \rangle| = |\mathbb{F}|^{r-j}$ *for* $0 \leq j \leq e-1$.

From Lemma 1.2.7, we know that any element $\tilde{a}$ of R can be written uniquely as

$$\tilde{a} = a_0 + a_1\tilde{\gamma} + \cdots + a_{e-1}\tilde{\gamma}^{e-1},$$

where the a_i can be viewed as elements in the field $\mathbb{F}$.

In the next definitions, γ will indicate the generator of the ideal of a chain ring, not necessarily the maximal ideal.

Definition 35. *([30, 31]) The ring R_∞ is defined as a* ***formal power series ring****:*

$$R_\infty = \mathbb{F}[[\gamma]] = \{\sum_{l=0}^{\infty} a_l\gamma^l | a_l \in \mathbb{F}\}.$$

Let i be an arbitrary positive integer. The rings R_i are defined as follows:

$$R_i = \{a_0 + a_1\gamma + \cdots + a_{i-1}\gamma^{i-1} | a_i \in \mathbb{F}\},$$

where $\gamma^{i-1} \neq 0$, but $\gamma^i = 0$ in R_i. If i is finite or infinite then the operations over R_i are defined as follows:

$$\sum_{l=0}^{i-1} a_l\gamma^l + \sum_{l=0}^{i-1} b_l\gamma^l = \sum_{l=0}^{i-1}(a_l + b_l)\gamma^l \tag{1.8}$$

$$\sum_{l=0}^{i-1} a_l\gamma^l \cdot \sum_{l'=0}^{i-1} b_{l'}\gamma^l = \sum_{s=0}^{i-1}(\sum_{l+l'=s} a_l b_{l'})\gamma^s. \tag{1.9}$$

We note that if $i = 1$ then $R_1 = \mathbb{F}$ and if $i = e$ then $R_e \cong R$.

Lemma 1.2.8. *([30, 31])*

1. *The ring R_i is a chain ring with the maximal ideal $\langle\gamma\rangle$ for all $i < \infty$.*

2. *The multiplicative group $R_\infty^\times = \{\sum_{j=0}^{\infty} a_j\gamma^j | a_0 \neq 0\}$.*

3. *The ring R_∞ is a principal ideal domain.*

We note that the ring R_∞ is an infinite ring whereas each R_i is a finite ring.

Lemma 1.2.9. *([30, 31]) It is well-known that the generator matrix for a code $\mathcal{C}$ over a finite chain ring R_i, where $i < \infty$ is permutation equivalent to a matrix of the following* *form:*

$$G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & & & A_{0,e} \\ & \gamma I_{k_1} & \gamma A_{1,2} & \gamma A_{1,3} & & & \gamma A_{1,e} \\ & & \gamma^2 I_{k_2} & \gamma^2 A_{2,3} & & & \gamma^2 A_{2,e} \\ & & & \ddots & \ddots & & \\ & & & & \ddots & \ddots & \\ & & & & & \gamma^{e-1} I_{k_{e-1}} & \gamma^{e-1} A_{e-1,e} \end{pmatrix}, \tag{1.10}$$

where e is the nilpotency index of γ. This matrix G is called the standard generator matrix of the code $\mathcal{C}$. In this case, the code $\mathcal{C}$ is said to have type

$$1^{k_0}\gamma^{k_1}(\gamma^2)^{k_2}\ldots(\gamma^{e-1})^{k_{e-1}}. \tag{1.11}$$

For linear codes over R_∞, the situation is a little different.

Lemma 1.2.10. *([30, 31]) Let $\mathcal{C}$ be a finitely generated, nonzero linear code over R_∞ of length n, then any generator matrix of $\mathcal{C}$ is permutation equivalent to a matrix of the following form:*

$$G = \begin{pmatrix} \gamma^{m_0} I_{k_0} & \gamma^{m_0} A_{0,1} & \gamma^{m_0} A_{0,2} & \gamma^{m_0} A_{0,3} & & & \gamma^{m_0} A_{0,r} \\ & \gamma^{m_1} I_{k_1} & \gamma^{m_1} A_{1,2} & \gamma^{m_1} A_{1,3} & & & \gamma^{m_1} A_{1,r} \\ & & \gamma^{m_2} I_{k_2} & \gamma^{m_2} A_{2,3} & & & \gamma^{m_2} A_{2,r} \\ & & & \ddots & \ddots & & \\ & & & & \ddots & \ddots & \\ & & & & & \gamma^{m_{r-1}} I_{k_{r-1}} & \gamma^{m_{r-1}} A_{r-1,r} \end{pmatrix}, \tag{1.12}$$

where $0 \leq m_0 < m_1 < \cdots < m_{r-1}$ for some integer r. The column blocks have sizes $k_0, k_1, \ldots, k_r$ and k_i are nonnegative integers adding to n. A code $\mathcal{C}$ with generator matrix of the form given in Equation (1.12) is said to be of type

$$(\gamma^{m_0})^{k_0}(\gamma^{m_1})^{k_1}\ldots(\gamma^{m_{r-1}})^{k_{r-1}},$$

where $k = k_0 + k_1 + \cdots + k_{r-1}$ is called its rank and $k_r = n - k$.

Definition 36. *([30, 31]) A code $\mathcal{C}$ of length n with rank k over R_∞ is called a γ-**adic** $[n, k]$ code. We call k the dimension of $\mathcal{C}$ and denote the dimension by dim $\mathcal{C} = k$.*

Definition 37. *([30, 31]) Let i, j be two integers with $i \leq j$, we define a map*

$$\Psi_i^j : R_j \to R_i, \tag{1.13}$$

$$\sum_{l=0}^{j-1} a_l\gamma^l \mapsto \sum_{l=0}^{i-1} a_l\gamma^l. \tag{1.14}$$

If we replace R_j with R_∞ then we obtain a map Ψ_i^∞. For convenience, we denote it by Ψ_i. Since both, Ψ_i^j and Ψ_i are projection maps, it is easy to show that Ψ_i^j and Ψ_i are ring homomorphisms. Let a, b be two arbitrary elements in R_j. It is easy to get that

$$\Psi_i^j(a+b) = \Psi_i^j(a) + \Psi_i^j(b),\ \Psi_i^j(ab) = \Psi_i^j(a)\Psi_i^j(b). \tag{1.15}$$

If $a, b \in R_\infty$, we have that

$$\Psi_i(a+b) = \Psi_i(a) + \Psi_i(b),\ \Psi_i(ab) = \Psi_i(a)\Psi_i(b). \tag{1.16}$$

Note that the map Ψ_i^j and Ψ_i can be extended naturally from R_j^n to R_i^n and R_∞^n to R_i^n.

1.3 Weight Enumerators of Binary Self-Dual Codes

In some of the later chapters in this work, we construct many Type I, extremal binary self-dual codes of lengths 64 and 68 of which some have parameters in their weight enumerators that have not been known in the literature before. We focus on this particular length, since there are still many Type I unknown codes of this length. Recently, much work has been done to find new, extremal, Type I binary self-dual codes of length 68, see [14, 19, 20, 22, 36] for some examples. In this work, we construct new binary self-dual codes of length 68 with very rare parameters that were not found before. We recall the weight enumerators of these codes.

1.3.1 Type I Binary $[64, 32, 12]$ Self-Dual Codes

There are two possible forms for the weight enumerator of binary $[64, 32, 12]$ self-dual codes ([10]):

$$W_{64,1} = 1 + (1312 + 16\beta)y^{12} + (22016 - 64\beta)y^{14} + \dots,\ 14 \le \beta \le 284,$$
$$W_{64,2} = 1 + (1312 + 16\beta)y^{12} + (23040 - 64\beta)y^{14} + \dots,\ 0 \le \beta \le 277,$$

where β is an integer.

Examples of many codes constructed for both weight enumerators with different values of the parameter β can be found in [36, 54, 65].

1.3.2 Type I Binary $[68, 34, 12]$ Self-Dual Codes

There are two possible forms for the weight enumerator of binary $[68, 34, 12]$ self-dual codes ([6, 47]):

$$W_{68,1} = 1 + (442 + 4\beta)y^{12} + (10864 - 8\beta)y^{14} + \dots, 104 \le \beta \le 1358,$$

$$W_{68,2} = 1 + (442 + 4\beta)y^{12} + (14960 - 8\beta - 256\gamma)y^{14} + \ldots,$$

where β and γ are integers with $0 \leq \gamma \leq 9$.

Examples of many codes constructed for both weight enumerators with different values of the parameters β and γ can be found in [14, 19, 22, 36, 37, 66, 67]. In [67], the authors constructed the first examples of codes with $\gamma = 7$ in $W_{68,2}$. In [37], the authors constructed the first examples of codes with $\gamma = 8, 9$ in $W_{68,2}$.

In Chapters 2 and 5, we construct many codes with different values of the parameter β for $\gamma = 1, 2, 3, 5, 6, 7, 8, 9$ that were not known in the literature before.

1.4 Special Matrices, Group Rings, the Map $\sigma(v)$ and Group Codes

In later chapters of this work, we present generator matrices in which we employ a well-known map that sends an element from a group ring to some $n \times n$ matrix with coefficients from the ring R. We also study codes, group codes in particular, over finite commutative Frobenius rings generated by this map. Moreover, in Chapter 4, we extend this well-known map. For that reason, we now recall the definitions on group rings, the well-known map that sends an element from a group ring to an $n \times n$ matrix over the ring R and the definition of group codes.

1.4.1 Special Matrices

In order to understand the map that sends an element from a group ring to an $n \times n$ matrix over the ring R and to understand some of the constructions we present later in this work, we now recall the definitions of some special matrices.

Definition 38. *([1]) The $n \times n$ **identity** matrix, denoted I_n, is the diagonal matrix with $a_{ii} = 1$.*

Definition 39. *([50]) A **circulant** matrix is one where each row is shifted one element to the right relative to the preceding row. We label the circulant matrix as $A = circ(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n)$ where α_i are ring elements.*

Definition 40. *([53]) A **block-circulant** matrix is one where each row consists of blocks which are square matrices. The rows of the block matrix are defined by shifting one block to the right relative to the preceding row. We label the block-circulant matrix as $CIRC(A_1, A_2, \ldots, A_n)$, where A_i are the $k \times k$ matrices over the ring R.*

Definition 41. *([50]) A **reverse circulant** matrix is one where each row is shifted one element to the left relative to the preceding row. We label the reverse circulant matrix as $A = revcirc(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n)$ where α_i are ring elements.*

Definition 42. *([1]) The **transpose** of a matrix A, denoted by A^T, is a matrix whose rows are the columns of A, i.e., $(A_{ij})^T = A_{ji}$.*

Definition 43. *([1]) A **symmetric** matrix is a square matrix that is equal to its transpose.*

Definition 44. *([63]) An $n \times n$ matrix $A = (a_{ij})$ is called a **bisymmetric** matrix if $a_{ij} = a_{ji}$ and $a_{ij} = a_{n+1-j,n+1-i}$ where $(i, j = 1, 2, \ldots, n)$.*

Definition 45. *([48]) The **determinant** of a square matrix A is a function, $det(A) : A \to \mathbb{R}$ such that the square matrix A is **non-singular** if and only if $det(A) \neq 0$. If $det(A) = 0$ then we say that A is **singular**.*

Definition 46. *([11]) A **Latin square** is an $n \times n$ matrix containing of n different elements, each occurring exactly once in each row and exactly once in each column.*

1.4.2 Group Rings

In this section, we give the standard definition of a group ring.

Definition 47. *([61]) Let R be a ring and let G be a group, then the **group ring** RG of G over R is given as:*

$$RG = \left\{ \sum_{g \in G} a_g g \mid a_g \in R \right\}.$$

We define the sum of two elements in RG componentwise:

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g.$$

Additionally, given two elements $\alpha = \sum_{g \in G} a_g g$ and $\beta = \sum_{h \in G} b_h h$, we define their product as

$$\alpha\beta = \sum_{g,h \in G} a_g b_h gh.$$

Definition 48. *([61]) The **canonical involution** $* : RG \to RG$ on a group ring RG is given by*

$$v^* = \sum_{g \in G} a_g g^{-1} \text{ for } v = \sum_{g \in G} a_g g \in RG.$$

*If v satisfies $vv^* = 1$, then we say that v is a **unitary unit** in RG.*

1.4.3 An Established Isomorphism

Here, we recall the map that sends a group ring element to an $n \times n$ matrix over R, described in [51]. We also recall some properties of this map.

Definition 49. *([51]) Let $\{g_1, g_2, g_3, \dots, g_n\}$ be a fixed listing of the elements of the group G. Then the matrix of G (relative to this listing) is defined as:*

$$M(G) = \begin{pmatrix} g_1^{-1}g_1 & g_1^{-1}g_2 & g_1^{-1}g_3 & \dots & g_1^{-1}g_n \\ g_2^{-1}g_1 & g_2^{-1}g_2 & g_2^{-1}g_3 & \dots & g_2^{-1}g_n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g_n^{-1}g_1 & g_n^{-1}g_2 & g_n^{-1}g_3 & \dots & g_n^{-1}g_n \end{pmatrix}. \tag{1.17}$$

Next we define the matrix that corresponds to a group ring element.

Definition 50. *([51]) Let $G = \{g_1, g_2, \dots, g_n\}$ be a group of order n. Let R be a ring. 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*

$$\sigma(v) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \alpha_{g_1^{-1}g_3} & \dots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \alpha_{g_2^{-1}g_3} & \dots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \alpha_{g_n^{-1}g_3} & \dots & \alpha_{g_n^{-1}g_n} \end{pmatrix}. \tag{1.18}$$

The elements $g_1^{-1}, g_2^{-2}, \dots, g_n^{-1}$ are simply the elements of the group G in some order. The matrix $\sigma(v)$ is in $M_n(R)$.

Theorem 10. *([51]) Let $v \in RG$, then the map $\sigma : v \to M_n(R)$ is a ring isomorphism from RG to a subring of $M_n(R)$.*

Theorem 11. *([51]) Suppose R has an identity. Then $v \in RG$ is a unit in RG if and only if $\sigma(v)$ is a unit in $M_n(R)$.*

Corollary 1.4.1. *([51]) When R is commutative, v is a unit in RG if and only if $\sigma(v)$ is a unit in $M_n(R)$ if and only if $det(\sigma(v))$ is a unit in R.*

Corollary 1.4.2. *([51]) The element v is a zero-divisor in RG if and only if $\sigma(v)$ is a zero-divisor in $M_n(R)$.*

In [39], the authors showed that there is a connection between v^* and v when we take their images under the σ map:

$$\sigma(v^*) = \sigma(v)^T. \tag{1.19}$$

An interesting and the most important property of the matrix $\sigma(v)$ is that it takes different form for different groups G. For example, for the cyclic group of order n, the matrix $\sigma(v)$ is a circulant matrix of order n, for the dihedral group D_{2n}, the matrix $\sigma(v)$ takes one of the following forms (these forms depend on how we list the elements of the group D_{2n}):

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

where A is a circulant matrix and B is a reverse circulant matrix, both with entries from the ring R, or

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

where both matrices, A and B are circulant with the entries from the ring R. Of course, there are many different groups of different orders that one can consider to obtain interesting $n \times n$ matrices over the ring R under the map σ.

1.4.4 Group Codes

In this section, we give the definition and some results on group codes generated by the group ring elements. This family of codes was described and studied over finite commutative Frobenius rings in [23].

Definition 51. *([23]) Let R be a finite commutative Frobenius ring. For a given element $v \in RG$, a* ***group code*** *or a G-code, over the ring R is defined as:*

$$\mathcal{C}(v) = \langle \sigma(v) \rangle, \tag{1.20}$$

where $\sigma(v)$ is the matrix defined in Section 1.4.3. Namely, the code is formed by taking the row space of $\sigma(v)$ over the ring R. Moreover, the code $\mathcal{C}(v)$ is a linear code since it is the row space of a generator matrix.

It is not possible to determine the size of the code (or the dimension if R is a field) immediately from the matrix, i.e., the rows of the matrix $\sigma(v)$ are not necessarily linearly independent.

We now recall some important results on G-codes over finite commutative Frobenius rings.

Theorem 12. *([23]) Let R be a finite commutative Frobenius ring and G a finite group of order n. Let $v \in RG$ and let $\mathcal{C}(v)$ be the corresponding code in R^n. Let $I(v)$ be the set of elements of RG such that $\sum \alpha_i g_i \in I(v)$ if and only if $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathcal{C}(v)$. Then $I(v)$ is a left ideal in RG.*

Corollary 1.4.3. *([23]) Let R be a finite commutative Frobenius ring and G a finite group of order n. Let $v \in RG$ and let $\mathcal{C}(v)$ be the corresponding code in R^n. Then the automorphism group of $\mathcal{C}(v)$ has a subgroup isomorphic to G.*

Chapter 2

Self-Dual Codes using Bisymmetric Matrices and Group Rings

A very well known and probably the most common technique for producing self-dual codes over rings is to consider standard generator matrices of the form $(I_n \mid A)$, where A is some $n \times n$ matrix over the ring R, fully defined by the elements appearing in the first row, for example, a circulant or reverse-circulant matrix. Please see [41, 42, 43, 44, 55] for some examples. Such generator matrices have to satisfy one condition, namely, $AA^T = -I_n$.

One of the main reasons why A is a matrix fully defined by the first row is that it reduces the search field significantly. For instance, if we were to consider a square matrix with n^2 independent variables, then if we searched for self-dual codes over the finite field $\mathbb{F}_2$ the search field would be 2^{n^2} which is very impractical. For square matrices that are fully defined by the elements appearing in the first row the search field reduces to 2^n when we search for self-dual codes over the field $\mathbb{F}_2$.

Recently in [39], the authors considered generator matrices of the form $(I_n \mid \sigma(v))$, where $\sigma(v)$ is the matrix defined in Equation (1.18). The advantage of this generator matrix is that one can obtain many different $n \times n$ matrices, fully defined by the first row, over the ring R. The number of these matrices depends on the number of groups of a particular order n. This technique allows to find codes with parameters that could not be obtained from the standard generator matrices.

In this chapter, we consider a generator matrix in which the identity matrix is replaced with a block matrix, where the blocks are fully defined by the elements appearing in the first row, and the matrix A is replaced with the 4×4 bisymmetric block matrix, where each block is a matrix of the form $\sigma(v)$. The 4×4 bisymmetric block matrix allows us to have a block matrix which does not have to be fully defined by the blocks appearing in the first row.

We present the construction and show under what conditions it produces self-dual codes over a finite commutative Frobenius ring of characteristic 2. We also employ our generator matrix together with the well-known extension and neighbour techniques to obtain new extremal binary self-dual codes of length 68. This chapter is joint work and the results are published in [35].

2.1 The Construction

In this section, we present the main construction of this chapter. As mentioned previously, we combine together the idea of a bisymmetric matrix and matrices that come from group rings.

Let $v_i \in RG$, where $1 \leq i \leq 6$, R be a finite commutative Frobenius ring of characteristic 2 and G be a finite group of order n. Additionally, let $B_1 = circ(\alpha_1, \underbrace{\alpha_2, \ldots, \alpha_2}_{n-1})$ and $B_2 = circ(\underbrace{\alpha_3, \ldots, \alpha_3}_{n})$ where $\alpha_i \in R$. Define the following matrix:

$$M_\sigma = \left[\begin{array}{cc|cc|cccc} B_1 & B_2 & \multicolumn{2}{c|}{\multirow{2}{*}{I_{2n}}} & \sigma(v_1) & \sigma(v_2) & \sigma(v_3) & \sigma(v_4) \\ B_2 & B_1 & & & \sigma(v_2) & \sigma(v_5) & \sigma(v_6) & \sigma(v_3) \\ \hline \multicolumn{2}{c|}{\multirow{2}{*}{I_{2n}}} & B_1 & B_2 & \sigma(v_3) & \sigma(v_6) & \sigma(v_5) & \sigma(v_2) \\ & & B_2 & B_1 & \sigma(v_4) & \sigma(v_3) & \sigma(v_2) & \sigma(v_1) \end{array}\right]. \tag{2.1}$$

Let $\mathcal{C}_\sigma$ be the code that is generated by the matrix M_σ. Then, the code $\mathcal{C}_\sigma$ has length $8n$.

As mentioned earlier, the standard generator matrix of a self-dual code is of the form $(I_n \mid A)$, where I_n is the $n \times n$ identity matrix. In the above construction, we replaced the identity matrix with a block matrix dependant on three variables. The reason for doing this, is that we want to increase our chances of constructing binary self-dual codes with parameters that could not be obtained from the standard generator matrix. By increasing the search field (by having more independent variables) we can consider more possibilities for different entries in the above construction - this may lead to finding new self-dual codes.

We now give the main theorem of this chapter.

Theorem 2.1.1. *Let R be a finite commutative Frobenius ring of characteristic 2 and let G be a finite group of order n. Then $\mathcal{C}_\sigma$ is a self-dual code of length $8n$ if and only if*

1. $1 + \alpha_1^2 = 0,$
2. $n\alpha_2^2 + n\alpha_3^2 = 0,$
3. $v_1v_1^* + v_2v_2^* + v_3v_3^* + v_4v_4^* = 0,$
4. $v_1v_2^* + v_2v_5^* + v_3v_6^* + v_4v_3^* = 0,$
5. $v_1v_3^* + v_2v_6^* + v_3v_5^* + v_4v_2^* = 0,$

6. $v_1v_4^* + v_2v_3^* + v_3v_2^* + v_4v_1^* = 0,$

7. $v_2v_2^* + v_5v_5^* + v_6v_6^* + v_3v_3^* = 0,$

8. $v_2v_3^* + v_5v_6^* + v_6v_5^* + v_3v_2^* = 0$

and

$$rank\begin{pmatrix}\sigma(v_7) & \sigma(v_8) & \sigma(v_9) & \sigma(v_{10})\\ \sigma(v_{11}) & \sigma(v_{12}) & \sigma(v_{13}) & \sigma(v_{14})\end{pmatrix} = 2n,$$

where

$$\begin{array}{rlrl} v_7 = & v_3+\alpha_1v_1+w(\alpha_2v_1+\alpha_3v_2), & v_8 = & v_6+\alpha_1v_2+w(\alpha_2v_2+\alpha_3v_5),\\ v_9 = & v_5+\alpha_1v_3+w(\alpha_2v_3+\alpha_3v_6), & v_{10} = & v_2+\alpha_1v_4+w(\alpha_2v_4+\alpha_3v_3),\\ v_{11} = & v_4+\alpha_1v_2+w(\alpha_3v_1+\alpha_2v_2), & v_{12} = & v_3+\alpha_1v_5+w(\alpha_3v_2+\alpha_2v_5),\\ v_{13} = & v_2+\alpha_1v_6+w(\alpha_3v_3+\alpha_2v_6), & v_{14} = & v_1+\alpha_1v_3+w(\alpha_3v_4+\alpha_2v_3) \end{array}$$

and $w = \sum_{g\in G} g \in RG$.

Proof. Let $M_\sigma = \begin{pmatrix} M_1 & M_2\end{pmatrix}$ where

$$M_1 = \begin{pmatrix} B_1 & B_2 & I_n & 0\\ B_2 & B_1 & 0 & I_n\\ I_n & 0 & B_1 & B_2\\ 0 & I_n & B_2 & B_1\end{pmatrix} \text{ and } M_2 = \begin{pmatrix}\sigma(v_1) & \sigma(v_2) & \sigma(v_3) & \sigma(v_4)\\ \sigma(v_2) & \sigma(v_5) & \sigma(v_6) & \sigma(v_3)\\ \sigma(v_3) & \sigma(v_6) & \sigma(v_5) & \sigma(v_2)\\ \sigma(v_4) & \sigma(v_3) & \sigma(v_2) & \sigma(v_1)\end{pmatrix},$$

$B_1 = \alpha_1 I_n + \sigma(\alpha_2 w)$, $B_2 = \sigma(\alpha_3 w)$ and $w = \sum_{g\in G} g \in RG$. Clearly, $M_\sigma M_\sigma^T = M_1M_1^T + M_2M_2^T$. It is well known that w is contained in the center of the group ring RG. Clearly for any square matrices A and B of the same size over the ring R, $(A+B)^2 = A^2 + B^2$ if and only if $AB = BA$. We now have

$$
\begin{aligned}
M_1M_1^T &= \begin{pmatrix} \alpha_1 I_n + \sigma(\alpha_2 w) & \sigma(\alpha_3 w) & I_n & 0 \\ \sigma(\alpha_3 w) & \alpha_1 I_n + \sigma(\alpha_2 w) & 0 & I_n \\ I_n & 0 & \alpha_1 I_n + \sigma(\alpha_2 w) & \sigma(\alpha_3 w) \\ 0 & I_n & \sigma(\alpha_3 w) & \alpha_1 I_n + \sigma(\alpha_2 w) \end{pmatrix}^2 \\
&= \left(\alpha_1 I_{4n} + \begin{pmatrix} \sigma(\alpha_2 w) & \sigma(\alpha_3 w) & I_n & 0 \\ \sigma(\alpha_3 w) & \sigma(\alpha_2 w) & 0 & I_n \\ I_n & 0 & \sigma(\alpha_2 w) & \sigma(\alpha_3 w) \\ 0 & I_n & \sigma(\alpha_3 w) & \sigma(\alpha_2 w) \end{pmatrix} \right)^2 \\
&= \alpha_1^2 I_{4n} + \begin{pmatrix} \sigma(\alpha_2 w) & \sigma(\alpha_3 w) & I_n & 0 \\ \sigma(\alpha_3 w) & \sigma(\alpha_2 w) & 0 & I_n \\ I_n & 0 & \sigma(\alpha_2 w) & \sigma(\alpha_3 w) \\ 0 & I_n & \sigma(\alpha_3 w) & \sigma(\alpha_2 w) \end{pmatrix}^2
\end{aligned}
$$

since I_{4n} commutes with any $4n \times 4n$-matrix. Moreover

$$
M_1M_1^T = \alpha_1^2 I_{4n} + I_{4n} + \begin{pmatrix} \sigma(\alpha_2 w) & \sigma(\alpha_3 w) & 0 & 0 \\ \sigma(\alpha_3 w) & \sigma(\alpha_2 w) & 0 & 0 \\ 0 & 0 & \sigma(\alpha_2 w) & \sigma(\alpha_3 w) \\ 0 & 0 & \sigma(\alpha_3 w) & \sigma(\alpha_2 w) \end{pmatrix}^2
$$

since $\left(\begin{smallmatrix} 0 & I_{2n} \\ I_{2n} & 0 \end{smallmatrix}\right)^2 = I_{4n}$ and $\left(\begin{smallmatrix} 0 & I_{2n} \\ I_{2n} & 0 \end{smallmatrix}\right)$ commutes with any $4n \times 4n$-matrix of the form $\left(\begin{smallmatrix} B & 0 \\ 0 & B \end{smallmatrix}\right)$. Clearly $\sigma(w)^2 = n\sigma(w)$. So

$$
\begin{aligned}
M_1M_1^T &= (1+\alpha_1^2) I_{4n} + CIRC\left(\begin{pmatrix} \sigma(n(\alpha_2^2+\alpha_3^2)w) & \sigma(2n\alpha_2\alpha_3 w) \\ \sigma(2n\alpha_2\alpha_3 w) & \sigma(n(\alpha_2^2+\alpha_3^2)w) \end{pmatrix}, 0 \right) \\
&= (1+\alpha_1^2) I_{4n} + CIRC(\sigma(n(\alpha_2^2+\alpha_3^2)w), 0, 0, 0).
\end{aligned}
$$

Additionally,

$$
M_2M_2^T = \begin{pmatrix} \sigma(v_1) & \sigma(v_2) & \sigma(v_3) & \sigma(v_4) \\ \sigma(v_2) & \sigma(v_5) & \sigma(v_6) & \sigma(v_3) \\ \sigma(v_3) & \sigma(v_6) & \sigma(v_5) & \sigma(v_2) \\ \sigma(v_4) & \sigma(v_3) & \sigma(v_2) & \sigma(v_1) \end{pmatrix} \begin{pmatrix} \sigma(v_1^*) & \sigma(v_2^*) & \sigma(v_3^*) & \sigma(v_4^*) \\ \sigma(v_2^*) & \sigma(v_5^*) & \sigma(v_6^*) & \sigma(v_3^*) \\ \sigma(v_3^*) & \sigma(v_6^*) & \sigma(v_5^*) & \sigma(v_2^*) \\ \sigma(v_4^*) & \sigma(v_3^*) & \sigma(v_2^*) & \sigma(v_1^*) \end{pmatrix}
$$

$$
= \begin{pmatrix} \sigma(v_1v_1^*+v_2v_2^*+v_3v_3^*+v_4v_4^*) & \sigma(v_1v_2^*+v_2v_5^*+v_3v_6^*+v_4v_3^*) & \sigma(v_1v_3^*+v_2v_6^*+v_3v_5^*+v_4v_2^*) & \sigma(v_1v_4^*+v_2v_3^*+v_3v_2^*+v_4v_1^*) \\ \sigma(v_2v_1^*+v_5v_2^*+v_6v_3^*+v_3v_4^*) & \sigma(v_2v_2^*+v_5v_5^*+v_6v_6^*+v_3v_3^*) & \sigma(v_2v_3^*+v_5v_6^*+v_6v_5^*+v_3v_2^*) & \sigma(v_2v_4^*+v_5v_3^*+v_6v_2^*+v_3v_1^*) \\ \sigma(v_3v_1^*+v_6v_2^*+v_5v_3^*+v_2v_4^*) & \sigma(v_3v_2^*+v_6v_5^*+v_5v_6^*+v_2v_3^*) & \sigma(v_3v_3^*+v_6v_6^*+v_5v_5^*+v_2v_2^*) & \sigma(v_3v_4^*+v_6v_3^*+v_5v_2^*+v_2v_1^*) \\ \sigma(v_4v_1^*+v_3v_2^*+v_2v_3^*+v_1v_4^*) & \sigma(v_4v_2^*+v_3v_5^*+v_2v_6^*+v_1v_3^*) & \sigma(v_4v_3^*+v_3v_6^*+v_2v_5^*+v_1v_2^*) & \sigma(v_4v_4^*+v_3v_3^*+v_2v_2^*+v_1v_1^*) \end{pmatrix}.
$$

Clearly, $\mathcal{C}_\sigma$ is self-orthogonal if and only if $1+\alpha_1^2 = 0$, $n\alpha_2^2 + n\alpha_3^2 = 0$, $v_1v_1^* + v_2v_2^* + v_3v_3^* + v_4v_4^* = 0$, $v_1v_2^* + v_2v_5^* + v_3v_6^* + v_4v_3^* = 0$, $v_1v_3^* + v_2v_6^* + v_3v_5^* + v_4v_2^* = 0$, $v_1v_4^* +$

$v_2v_3^* + v_3v_2^* + v_4v_1^* = 0$, $v_2v_2^* + v_5v_5^* + v_6v_6^* + v_3v_3^* = 0$, $v_2v_3^* + v_5v_6^* + v_6v_5^* + v_3v_2^* = 0$, $v_2v_4^* + v_5v_3^* + v_6v_2^* + v_3v_1^* = 0$ and $v_3v_4^* + v_6v_3^* + v_5v_2^* + v_2v_1^* = 0$. We note here that the last two conditions are the result of the fifth and fourth conditions respectively. Namely, $v_1v_3^* + v_2v_6^* + v_3v_5^* + v_4v_2^* = 0 \implies v_2v_4^* + v_5v_3^* + v_6v_2^* + v_3v_1^* = 0$, that is $0 = 0^* = (v_1v_3^* + v_2v_6^* + v_3v_5^* + v_4v_2^*)^* = v_3v_1^* + v_6v_2^* + v_5v_3^* + v_2v_4^* = v_2v_4^* + v_5v_3^* + v_6v_2^* + v_3v_1^*$ and similarly $v_1v_2^* + v_2v_5^* + v_3v_6^* + v_4v_3^* = 0 \implies v_3v_4^* + v_6v_3^* + v_5v_2^* + v_2v_1^* = 0$, that is $0 = 0^* = (v_1v_2^* + v_2v_5^* + v_3v_6^* + v_4v_3^*)^* = v_2v_1^* + v_5v_2^* + v_6v_3^* + v_3v_4^* = v_3v_4^* + v_6v_3^* + v_5v_2^* + v_2v_1^*$. Now,

$$\begin{aligned}
B_1^2 + B_2^2 + I_n &= (\alpha_1 I_n + \sigma(\alpha_2 w))^2 + (\sigma(\alpha_3 w))^2 + I_n \\
&= \alpha_1^2 I_n + \sigma((\alpha_2 w)^2) + \sigma((\alpha_3 w)^2) + I_n \\
&= \alpha_1^2 I_n + \sigma(\alpha_2^2 w^2 + \alpha_3^2 w^2) + I_n \\
&= \alpha_1^2 I_n + \sigma(\alpha_2^2 (nw) + \alpha_3^2 (nw)) + I_n \\
&= \alpha_1^2 I_n + \sigma((n\alpha_2^2 + n\alpha_3^2) w) + I_n \\
&= (1) I_n + \sigma((0) w) + I_n \\
&= 2I_n + \sigma(0) \\
&= 0.
\end{aligned}$$

Consequently,

$$\begin{aligned}
M_1 \begin{pmatrix} I_n & 0 & 0 & 0 \\ 0 & I_n & 0 & 0 \\ B_1 & B_2 & I_n & 0 \\ B_2 & B_1 & 0 & I_n \end{pmatrix} &= \begin{pmatrix} B_1 & B_2 & I_n & 0 \\ B_2 & B_1 & 0 & I_n \\ I_n & 0 & B_1 & B_2 \\ 0 & I_n & B_2 & B_1 \end{pmatrix} \begin{pmatrix} I_n & 0 & 0 & 0 \\ 0 & I_n & 0 & 0 \\ B_1 & B_2 & I_n & 0 \\ B_2 & B_1 & 0 & I_n \end{pmatrix} \\
&= \begin{pmatrix} 2B_1 & 2B_2 & I_n & 0 \\ 2B_2 & 2B_1 & 0 & I_n \\ B_1^2 + B_2^2 + I_n & 2B_1B_2 & B_1 & B_2 \\ 2B_1B_2 & B_2^2 + B_1^2 + I_n & B_2 & B_1 \end{pmatrix} \\
&= \begin{pmatrix} 0 & 0 & I_n & 0 \\ 0 & 0 & 0 & I_n \\ 0 & 0 & B_1 & B_2 \\ 0 & 0 & B_2 & B_1 \end{pmatrix}
\end{aligned}$$

and

$$\text{rank} M_\sigma = \text{rank} \begin{pmatrix} I_n & 0 & \sigma(v_1) & \sigma(v_2) & \sigma(v_3) & \sigma(v_4) \\ 0 & I_n & \sigma(v_2) & \sigma(v_5) & \sigma(v_6) & \sigma(v_3) \\ B_1 & B_2 & \sigma(v_3) & \sigma(v_6) & \sigma(v_5) & \sigma(v_2) \\ B_2 & B_1 & \sigma(v_4) & \sigma(v_3) & \sigma(v_2) & \sigma(v_1) \end{pmatrix}.$$

It is interesting to note that $B_1 = \alpha_1 I_n + \sigma(\alpha_2 w) = \sigma(\alpha_1 e + \alpha_2 w)$ as $I_n = \sigma(e)$, where e is the identity element of the group G. Additionally,

$$\text{rank}M_\sigma = \text{rank}\begin{pmatrix} \sigma(e) & 0 & \sigma(v_1) & \sigma(v_2) & \sigma(v_3) & \sigma(v_4) \\ 0 & \sigma(e) & \sigma(v_2) & \sigma(v_5) & \sigma(v_6) & \sigma(v_3) \\ \sigma(\alpha_1 e+\alpha_2 w) & \sigma(\alpha_3 w) & \sigma(v_3) & \sigma(v_6) & \sigma(v_5) & \sigma(v_2) \\ \sigma(\alpha_3 w) & \sigma(\alpha_1 e+\alpha_2 w) & \sigma(v_4) & \sigma(v_3) & \sigma(v_2) & \sigma(v_1) \end{pmatrix} =$$

$$\text{rank}\left[\begin{pmatrix} I_n & 0 & 0 & 0 \\ 0 & I_n & 0 & 0 \\ \sigma(\alpha_1 e+\alpha_2 w) & \sigma(\alpha_3 w) & I_n & 0 \\ \sigma(\alpha_3 w) & \sigma(\alpha_1 e+\alpha_2 w) & 0 & I_n \end{pmatrix} \times \right.$$

$$\left.\begin{pmatrix} \sigma(e) & 0 & \sigma(v_1) & \sigma(v_2) & \sigma(v_3) & \sigma(v_4) \\ 0 & \sigma(e) & \sigma(v_2) & \sigma(v_5) & \sigma(v_6) & \sigma(v_3) \\ \sigma(\alpha_1 e+\alpha_2 w) & \sigma(\alpha_3 w) & \sigma(v_3) & \sigma(v_6) & \sigma(v_5) & \sigma(v_2) \\ \sigma(\alpha_3 w) & \sigma(\alpha_1 e+\alpha_2 w) & \sigma(v_4) & \sigma(v_3) & \sigma(v_2) & \sigma(v_1) \end{pmatrix}\right] =$$

$$\text{rank}\begin{pmatrix} \sigma(e) & 0 & \sigma(v_1) & \sigma(v_2) & \sigma(v_3) & \sigma(v_4) \\ 0 & \sigma(e) & \sigma(v_2) & \sigma(v_5) & \sigma(v_6) & \sigma(v_3) \\ 0 & 0 & \sigma(v_7) & \sigma(v_8) & \sigma(v_9) & \sigma(v_{10}) \\ 0 & 0 & \sigma(v_{11}) & \sigma(v_{12}) & \sigma(v_{13}) & \sigma(v_{14}) \end{pmatrix},$$

where

$$\begin{aligned} v_7 = {}& v_3+\alpha_1 v_1+w(\alpha_2 v_1+\alpha_3 v_2), & v_8 = {}& v_6+\alpha_1 v_2+w(\alpha_2 v_2+\alpha_3 v_5), \\ v_9 = {}& v_5+\alpha_1 v_3+w(\alpha_2 v_3+\alpha_3 v_6), & v_{10} = {}& v_2+\alpha_1 v_4+w(\alpha_2 v_4+\alpha_3 v_3), \\ v_{11} = {}& v_4+\alpha_1 v_2+w(\alpha_3 v_1+\alpha_2 v_2), & v_{12} = {}& v_3+\alpha_1 v_5+w(\alpha_3 v_2+\alpha_2 v_5), \\ v_{13} = {}& v_2+\alpha_1 v_6+w(\alpha_3 v_3+\alpha_2 v_6), & v_{14} = {}& v_1+\alpha_1 v_3+w(\alpha_3 v_4+\alpha_2 v_3). \end{aligned}$$

Hence,

$$\text{rank}M_\sigma = 2n+\text{rank}\begin{pmatrix} \sigma(v_7) & \sigma(v_8) & \sigma(v_9) & \sigma(v_{10}) \\ \sigma(v_{11}) & \sigma(v_{12}) & \sigma(v_{13}) & \sigma(v_{14}) \end{pmatrix}.$$

Finally, the self-orthogonal code $\mathcal{C}_\sigma$ is self-dual if and only if

$$\text{rank}\begin{pmatrix} \sigma(v_7) & \sigma(v_8) & \sigma(v_9) & \sigma(v_{10}) \\ \sigma(v_{11}) & \sigma(v_{12}) & \sigma(v_{13}) & \sigma(v_{14}) \end{pmatrix} = 2n.$$

□

If we assume that the group G is Abelian, we get the following result.

Corollary 2.1.2. *Let R be a finite commutative Frobenius ring of characteristic 2 and let G be an Abelian finite group of order n. Then $\mathcal{C}_\sigma$ is a self-dual code of length $8n$ if and only if*

1. $1 + \alpha_1^2 = 0$,

2. $n\alpha_2^2 + n\alpha_3^2 = 0$,

3. $v_1^2 + v_2^2 + v_3^2 + v_4^2 = 0$,

4. $v_1v_3 + v_2v_4 + v_3v_5 + v_2v_6 = 0$,

5. $(v_2 + v_3)(v_1 + v_4 + v_5 + v_6) = 0$,

6. $(v_1 + v_4 + v_5 + v_6)^2 = 0$.

Proof. From Theorem 2.1.1 we have the first two conditions. Since G is Abelian then $v^* = v$ for any $v \in RG$. The equations $(3) - (8)$ in Theorem 2.1.1 are equivalent to

$$v_1^2 + v_2^2 + v_3^2 + v_4^2 = 0,$$

$$v_1v_2 + v_2v_5 + v_3v_6 + v_3v_4 = 0,$$

$$v_1v_3 + v_2v_4 + v_2v_6 + v_3v_5 = 0,$$

$$v_1v_4 + v_1v_4 + v_2v_3 + v_2v_3 = 0,$$

$$v_2^2 + v_5^2 + v_6^2 + v_3^2 = 0,$$

$$v_2v_3 + v_2v_3 + v_5v_6 + v_5v_6 = 0,$$

or

$$v_1^2 + v_2^2 + v_3^2 + v_4^2 = 0,$$

$$v_1v_2 + v_2v_5 + v_3v_6 + v_3v_4 = 0,$$

$$v_1v_3 + v_2v_4 + v_2v_6 + v_3v_5 = 0,$$

$$0 = 0,$$

$$v_2^2 + v_5^2 + v_6^2 + v_3^2 = 0,$$

$$0 = 0.$$

Adding the 5th equation to the 1st one, the 2nd equation to the third one, we obtain the required equations:

$$v_1^2 + v_2^2 + v_3^2 + v_4^2 = 0,$$

$$v_1v_2 + v_2v_5 + v_3v_6 + v_3v_4 = 0,$$

$$(v_2 + v_3)(v_1 + v_4 + v_5 + v_6) = 0,$$

$$v_1^2 + v_4^2 + v_5^2 + v_6^2 = 0.$$

□

We can clearly see that the search field is greater in our construction than in the standard generator matrix of the form $(I_n|A)$, where I_n is the identity matrix and A is a matrix that is fully defined by the elements in the first row. Also, $\sigma(v_i)$ represent matrices that come from group rings - this means that we can create many different M_σ matrices by considering different groups in the group rings. We next apply the above matrix to search for extremal self-dual codes.

2.2 Numerical Results

In this section, we apply the matrix defined in Equation (2.1) to the ring $\mathbb{F}_4 + u\mathbb{F}_4$ to obtain self-dual codes whose binary images have parameters $[64, 32, 12]$. We specifically consider the matrix M_σ for the group $G = C_2$, that is, the cyclic group of order 2. Next, we extend these codes to obtain new self-dual codes of length 68. We finally consider their possible neighbours and find more new self-dual codes of length 68. We implement the search of self-dual codes over the alphabets using the software *MAGMA* ([4]).

2.2.1 Single-Even, Binary $[64, 32, 12]$ Self-Dual Codes

We now employ the matrix M_σ with $G = C_2$ over $\mathbb{F}_4 + u\mathbb{F}_4$. As a result, we obtain many codes whose binary images are the extremal codes of length 64. To save space, we only list two. These codes in turn are used to find new codes of length 68. Recall that the above construction involves $v_i \in RC_2$ for $i \in \{1, \ldots, 6\}$. Instead of listing each v_i separately, we list $(v_1, \ldots, v_6)$ as one vector. We also list the parameters of the corresponding binary images.

Table 2.1: Codes of length 64 via Theorem 2.1.1 over the ring $\mathbb{F}_4 + u\mathbb{F}_4$

$\mathcal{C}_i$	$(\alpha_1, \alpha_2, \alpha_3)$	$(v_1, \ldots, v_6)$	$\lvert Aut(\mathcal{C}_i)\rvert$	$W_{64,2}$	$\mathcal{C}_i$	$(\alpha_1, \alpha_2, \alpha_3)$	$(v_1, \ldots, v_6)$	$\lvert Aut(\mathcal{C}_i)\rvert$	$W_{64,2}$
1	$(0, 4, 2)$	$(A, 1, 0, 0, 4, 4, 1, 7, A, 1, 7, 1)$	2^5	$\beta = 0$	2	$(0, E, 2)$	$(A, 3, 0, 1, 4, 7, 5, 3, 4, 3, 4, 4)$	$2^4 \cdot 3$	$\beta = 64$

2.2.2 New Extremal Self-Dual Binary Codes of Length 68 from $\mathbb{F}_2 + u\mathbb{F}_2$ Extensions

In this section, we apply Theorem 9 to the $\psi_{\mathbb{F}_4+u\mathbb{F}_4}$-images of the codes in Table 2.1. The results are tabulated in Table 2.2, where $1 + u$ in $\mathbb{F}_2 + u\mathbb{F}_2$ is denoted as 3.

Table 2.2: New codes of length 68 from Theorem 9

$\mathcal{C}_{68,i}$	$\mathcal{C}_i$	c	X	γ	β	$\mathcal{C}_{68,i}$	$\mathcal{C}_i$	c	X	γ	β
$\mathcal{C}_{68,1}$	2	1	$(133u330310100uu130u0313311110u03)$	**1**	**173**	$\mathcal{C}_{68,2}$	2	1	$(331031u1101uuu01100033311133uuu1)$	**1**	**177**
$\mathcal{C}_{68,3}$	2	1	$(313u31031u1000u1100u33311131u001)$	**1**	**181**	$\mathcal{C}_{68,4}$	2	1	$(1010u113u3u3011u1u3uuu13u33uu1u1)$	**2**	**167**
$\mathcal{C}_{68,5}$	2	1	$(11u033013u3uu0u0u0003110013133u0)$	**2**	**175**	$\mathcal{C}_{68,6}$	2	3	$(00u11333330uu00uu30130100300u311)$	**2**	**177**
$\mathcal{C}_{68,7}$	2	3	$(331u33uu10u000u1303uu03u0033u0u3)$	**2**	**179**	$\mathcal{C}_{68,8}$	2	1	$(013u331u0uu1uu3u3uu33u033101333u)$	**2**	**181**
$\mathcal{C}_{68,9}$	2	3	$(0003uu3u1u03013u30000301331111u0)$	**2**	**183**	$\mathcal{C}_{68,10}$	2	1	$(u0u3u03u3uu1011010u0010131111100)$	**2**	**187**
$\mathcal{C}_{68,11}$	2	1	$(31u11u133u10013011u01103u033u110)$	**2**	**191**	$\mathcal{C}_{68,12}$	2	1	$(0uu1uu1u3003011u10u0u301113331u0)$	**2**	**197**
$\mathcal{C}_{68,13}$	1	3	$(1u33u331u33330u10u130310u130u0uu)$	**3**	**74**	$\mathcal{C}_{68,14}$	2	1	$(uu01003u01003u30113131uuuu00330u)$	**3**	**157**
$\mathcal{C}_{68,15}$	2	3	$(11130u0u11013333u0u31uu3133uuuuu)$	**3**	**181**	$\mathcal{C}_{68,16}$	2	3	$(33u11u11303uu310110u310100110110)$	**3**	**183**
$\mathcal{C}_{68,17}$	2	1	$(u31u31300001uu303003100311033310)$	**3**	**185**	$\mathcal{C}_{68,18}$	2	1	$(13330u13u311011131u113u3u3u300u3)$	**3**	**187**
$\mathcal{C}_{68,19}$	2	1	$(01301130uu030u1010u31u033103331u)$	**3**	**195**	$\mathcal{C}_{68,20}$	2	1	$(031u3330uu01001010u3300131011330)$	**3**	**197**
$\mathcal{C}_{68,21}$	2	1	$(131100110111u311130313u3u1030uu3)$	**3**	**199**	$\mathcal{C}_{68,22}$	2	1	$(1131001101330331110311u301010003)$	**3**	**201**
$\mathcal{C}_{68,23}$	2	1	$(u310313uuuu1003u10u31u0111011130)$	**3**	**203**	$\mathcal{C}_{68,24}$	2	1	$(u1303310u003uu1u30u13uu131u3311u)$	**3**	**217**
$\mathcal{C}_{68,25}$	2	1	$(u31u111uuu010u1u10u130u11301111u)$	**5**	**205**	$\mathcal{C}_{68,26}$	2	1	$(011u113uu0u3001u10u3300333u1311u)$	**5**	**213**

2.2.3 New Codes of length 68 from Neighbours

In this section, we employ Definition 32 to investigate the possible neighbours of the codes in Table 2.2. As a result, we obtain 15 more new binary self-dual codes with parameters $[64, 32, 12]$ as neighbours of the codes $\mathcal{C}_{15}$ and $\mathcal{C}_{16}$. It turns out the neighbours have trivial automorphism. We set the first 34 entries of x to be 0, the rest of the vectors are listed in Table 2.3.

Table 2.3: New codes of length 68 as neighbours

$\mathcal{N}_{68,27}$	$\mathcal{C}_{68,26}$	$(0101111000110001011111010111110111)$	**5**	**183**	$\mathcal{N}_{68,28}$	$\mathcal{C}_{68,25}$	$(0101110001000111011110011010101100)$	**5**	**184**
$\mathcal{N}_{68,29}$	$\mathcal{C}_{68,25}$	$(0110100011110111100100000100100000)$	**5**	**185**	$\mathcal{N}_{68,30}$	$\mathcal{C}_{68,25}$	$(1010011011100010001000100110011101)$	**5**	**186**
$\mathcal{N}_{68,31}$	$\mathcal{C}_{68,26}$	$(0000010000111110000110011000101101)$	**5**	**188**	$\mathcal{N}_{68,32}$	$\mathcal{C}_{68,25}$	$(1101101010010110101001001001000110)$	**5**	**190**
$\mathcal{N}_{68,33}$	$\mathcal{C}_{68,25}$	$(0101111110111000000110101000101101)$	**5**	**192**	$\mathcal{N}_{68,34}$	$\mathcal{C}_{68,26}$	$(1111111111101001001001100111000001)$	**5**	**194**
$\mathcal{N}_{68,35}$	$\mathcal{C}_{68,26}$	$(1111001001100001110100111100000111)$	**5**	**196**	$\mathcal{N}_{68,36}$	$\mathcal{C}_{68,26}$	$(1000011011000101011111111110000010)$	**5**	**197**
$\mathcal{N}_{68,37}$	$\mathcal{C}_{68,26}$	$(0011101000101101011101110001011001)$	**5**	**199**	$\mathcal{N}_{68,38}$	$\mathcal{C}_{68,26}$	$(1101001011110010100010010010010011)$	**5**	**203**
$\mathcal{N}_{68,39}$	$\mathcal{C}_{68,26}$	$(1010110101000110100110101111100001)$	**5**	**204**	$\mathcal{N}_{68,40}$	$\mathcal{C}_{68,26}$	$(0010001101000001010100010101011011)$	**6**	**192**
$\mathcal{N}_{68,41}$	$\mathcal{C}_{68,26}$	$(1010011000111100101001111000001100)$	**6**	**210**					

The codes constructed in this chapter and the ones constructed in later chapters, could potentially be used in design theory to produce some new t-designs. It is well know that some of the binary self-dual codes have been used before to produce particular t-designs by the Assmus-Mattson Theorem from [2]. For example, the binary self-dual $[24, 12, 8]$ extended Golay code hold 5-designs. Please see [2] for details on the Assmus-Mattson Theorem and its connections to binary self-dual codes with interesting examples, like the one about the binary self-dual $[24, 12, 8]$ extended Golay code.

Chapter 3

G-Codes, Self-Dual G-Codes and Reversible G-Codes over the Ring $\mathcal{B}_{j,k}$

In this chapter, we study a new family of rings, $\mathcal{B}_{j,k}$, whose base field is the finite field $\mathbb{F}_{p^r}$. We study the structure of this family of rings and show that each member of the family is a commutative Frobenius ring. We define a Gray map for the new family of rings, study G-codes, self-dual G-codes, and reversible G-codes over this family. In particular, we show that the projection of a G-code over $\mathcal{B}_{j,k}$ to a code over $\mathcal{B}_{l,m}$ is also a G-code and the image under the Gray map of a self-dual G-code is also a self-dual G-code when the characteristic of the base field is 2. Moreover, we show that the image of a reversible G-code under the Gray map is also a reversible $G^{2^{j+k}}$-code. The Gray images of these codes are shown to have a rich automorphism group which arises from the algebraic structure of the rings and the groups. Finally, we show that quasi-G codes, which are the images of G-codes under the Gray map, are also G^s-codes for some s.

One desirable property of codes over this new family of rings is that one can obtain codes with a rich automorphism group via the algebraic structure of the ring through the Gray map. In this construction, one can find codes that might have been missed by more classical construction techniques, for example, one may find extremal binary self-dual codes with new weight enumerators or with different orders of the automorphism group. The new family of commutative Frobenius rings $\mathcal{B}_{j,k}$, introduced in this chapter, is an extension of the family of commutative Frobenius rings $\mathcal{F}_{j,k}$, given in [9]. In there, the authors consider a finite field of order 4 as a base field, that is, the finite field $\mathbb{F}_4$. In this chapter, our base field is a finite field $\mathbb{F}_{p^r}$ of order p^r. There is an extensive literature on different families of codes over rings, please see [13, 24, 25, 32] for some examples.

3.1 The ring $\mathcal{B}_{j,k}$

We begin by describing the family of rings $\mathcal{B}_{j,k}$. Set

$$\mathcal{B}_{j,k} = \mathbb{F}_{p^r}[v_1, v_2, \ldots, v_j, u_1, u_2, \ldots, u_k]/\langle v_i^2 - v_i, u_i^2 \rangle.$$

The above family of rings generalises the definition of $\mathcal{F}_{j,k}$ in [9] as well as the rings $R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle u_i^2 = 0 \rangle$ from Definition 27, the rings $A_k = \mathbb{F}_2[v_1, v_2, \ldots, v_k]/\langle v_i^2 = v_i \rangle$ in [8] and the rings $\mathbb{F}_{p^r}[v_1, v_2, \ldots, v_k]/\langle v_i^2 - v_i, v_iv_j - v_jv_i \rangle$ given in [52].

In essence, all of the families of rings were studied together with Gray maps to ambient spaces over finite fields. They use the algebraic structure of the family of rings to obtain desirable properties for the codes over finite fields. One desirable property is that one can obtain codes with a rich automorphism group via the algebraic structure of the ring through the Gray map.

We now look at the algebraic structure of the ring $\mathcal{B}_{j,k}$.

For $A \subseteq [j] = \{1, 2, 3, \ldots, j\}$ and $B \subseteq [k] = \{1, 2, 3, \ldots, k\}$, we denote

$$v_A := \prod_{i \in A} v_i \quad \text{and} \quad u_B := \prod_{i \in B} u_i,$$

with $u_\emptyset = 1$ and $v_\emptyset = 1$. Every element in the ring can be written as

$$\sum_{\substack{A \subseteq [j] \\ B \subseteq [k]}} c_{A,B} v_A u_B, \tag{3.1}$$

where $c_{A,B} \in \mathbb{F}_{p^r}$.

It is immediate that

$$u_A u_{A'} = \begin{cases} 0 & if \quad A \cap A' \neq \emptyset, \\ u_{A \cup A'} & if \quad A \cap A' = \emptyset. \end{cases} \tag{3.2}$$

Similarly, we have

$$v_A v_{A'} = v_{A \cup A'}. \tag{3.3}$$

By using Equation (3.2) and Equation (3.3), multiplication of two elements in $\mathcal{B}_{j,k}$ is given by:

$$\left(\sum_{A,B} c_{A,B} v_A u_B \right) \left(\sum_{A',B'} c_{A',B'} v_{A'} u_{B'} \right) = \sum_{\substack{A, B, A', B' \\ B \cap B' = \emptyset}} (c_{A,B} c_{A',B'}) v_{A \cup A'} u_{B \cup B'}, \tag{3.4}$$

where A, A' are subsets of $[j]$ and B, B' are subsets of $[k]$.

Lemma 3.1.1. *The commutative ring $\mathcal{B}_{j,k}$ has characteristic p, and $|\mathcal{B}_{j,k}| = (p^r)^{2^{j+k}}$.*

Proof. The commutativity of the ring follows from the fact that $\mathbb{F}_{p^r}$ is commutative and that the variables commute. Since the characteristic of $\mathbb{F}_{p^r}$ is p, then $\mathcal{B}_{j,k}$ has characteristic p. When we look at the representation of elements of $\mathcal{B}_{j,k}$ given in Equation (3.1), we see that there are $2^j 2^k = 2^{j+k}$ subsets and p^r choices for each coefficient $c_{A,B}$. This gives that $\mathcal{B}_{j,k}$ has cardinality $(p^r)^{2^{j+k}}$. □

We now give some structural theorems about the family of rings.

Theorem 13. *Let j and k be non-negative integers.*

1. *The ring $\mathcal{B}_{j,k}$ is isomorphic to $\oplus_{i=1}^{2^j}\mathcal{B}_{0,k}$.*
2. *An element a is a unit in $\mathcal{B}_{j,k}$ if and only if the projection to each component of $\oplus_{i=1}^{2^j}\mathcal{B}_{0,k}$ is a unit.*

Proof. The ideals $\langle v_j \rangle$ and $\langle 1 + v_j \rangle$ are relatively prime ideals. By Lemma 2.3 in [12], we have that $\mathcal{B}_{j,k} \cong \mathcal{B}_{j-1,k} \times \mathcal{B}_{j-1,k}$. Then, by induction on j, we have the first result.

The second result follows immediately from the isomorphisms in the first. □

Since $\mathcal{B}_{j,k}$ is isomorphic to $\oplus_{i=1}^{2^j}\mathcal{B}_{0,k}$, it is natural to look at the structure of the ring $\mathcal{B}_{0,k} = \mathbb{F}_{p^r}[u_1, u_2, \dots, u_k]/\langle u_i^2 \rangle$ to understand the structure of $\mathcal{B}_{j,k}$.

Lemma 3.1.2. *Let $\sum_{A\subseteq[k]} c_A u_A \in \mathcal{B}_{0,k}$, with $c_\emptyset = 0$, then*

$$(\sum_{A\subseteq[k]} c_A u_A)^p = 0$$

where p is the characteristic of $\mathcal{B}_{0,k}$.

Proof. First, we note that if $A \neq \emptyset$, then $u_A^2 = 0$. Then, we see that the coefficient of any monomial in this expansion, other than the first or the last is divisible by p and hence 0. Therefore, all of the terms are 0. □

Lemma 3.1.3. *An element a of the ring $\mathcal{B}_{0,k}$ is a unit if and only if $c_\emptyset \neq 0$.*

Proof. We write an element in $\mathcal{B}_{0,k}$ as $c_\emptyset + \sum_{A\subset[k]} c_A u_A$ by hypothesis, with $c_\emptyset \neq 0$. Since the ring has characteristic p and by Lemma 3.1.2, the inverse of $c_\emptyset + \sum_{A\subset[k]} c_A u_A$ is:

$$\sum_{i=0}^{p-1} \binom{p-1}{i} (c_\emptyset^{-1})^{i+1} (\sum_{A\subseteq[k]} c_A u_A)^i.$$

The term $c_\emptyset^{-1}$ exists if and only if $c_\emptyset \neq 0$. □

Theorem 14. *An element a of the ring $\mathcal{B}_{0,k}$ is a zero-divisor if and only if $c_\emptyset = 0$. The set of all non-units form a maximal ideal and the cardinality of this maximal ideal is $(p^r)^{2^k-1}$ and therefore the ring $\mathcal{B}_{0,k}$ is local.*

Proof. For the first statement, we know by Lemma 3.1.2 that

$$(\sum_{A\subseteq[k]} c_A u_A)(\sum_{A\subseteq[k]} c_A u_A)^{p-1} = 0,$$

when $c_\emptyset = 0$. Therefore it is a zero-divisor. Lemma 3.1.3 gives the other direction.

Next, let $\mathfrak{m} = \langle u_1, u_2, \ldots, u_k\rangle$. Elements of this ideal are all of the form, $c_\emptyset + \sum_{A\subset[k]} c_A u_A$ where $c_\emptyset = 0$. This is necessarily all non-units and is therefore the unique maximal ideal. □

Theorem 15. *The ring $\mathcal{B}_{j,k}$ is not local for non-zero j.*

Proof. The ring $\mathcal{B}_{j,k}$ is isomorphic to $\oplus_{i=1}^{2^j} \mathcal{B}_{0,k}$ by Theorem 13. Then each ideal corresponding to the sum of $(k-1)$ zero-ideals with one copy of $\mathcal{B}_{0,k}$ is a maximal ideal. Therefore, the ring is not local. □

As an example of this, consider the ring $\mathcal{B}_{1,0} = \mathbb{F}_p[v_1]/\langle v_1^2 - v_1\rangle$. The ring is isomorphic via Theorem 13 to $\mathbb{F}_p \times \mathbb{F}_p$. This ring has two maximal ideals corresponding to $\mathbb{F}_p \times \{0\}$ and to $\{0\} \times \mathbb{F}_p$. Therefore, the ring is not local.

Given the definition of inner-product and the fact that the ring is commutative it is easy to see that for any ideal I, $Ann(I) = I^\perp$. We use this result in the following theorem.

Theorem 16. *Let $I_1 = \langle u_{i_1} u_{i_2} \cdots u_{i_s}\rangle$ and $I_2 = \langle u_{i_1}, u_{i_2}, \ldots, u_{i_s}\rangle$ be ideals of $\mathcal{B}_{0,k}$, where $i_\ell \neq i_{\ell'}$, when $\ell \neq \ell'$. Then $|I_1| = (p^r)^{2^{k-s}}$ and $|I_2| = (p^r)^{2^k - 2^{k-s}}$.*

Proof. Elements of I_1 are in the form of

$$\sum_{A\subseteq[k]} c_A u_A,\ c_A \in \mathbb{F}_{p^r},$$

where $u_\emptyset = 1$. It is clear that every u_A must have $\{i_1, i_2, \ldots, i_s\} \subseteq A$. Then there are 2^{k-s} such subsets of $[k]$. Hence $|I_1| = (p^r)^{2^{k-s}}$.

For the second statement, elements of I_2 are in the same form. But this time, the subsets of $[k]$ differ. More precisely, subsets must have at least one of $\{i_1, i_2, \ldots, i_s\}$. It can be easily obtained that there are $2^k - 2^{k-s}$ such subsets. Hence $|I_2| = (p^r)^{2^k - 2^{k-s}}$. □

Theorem 17. *Let $I_1 = \langle u_{i_1} u_{i_2} \ldots u_{i_s}\rangle$ and $I_2 = \langle u_{i_1}, u_{i_2}, \ldots u_{i_s}\rangle$ be ideals of $\mathcal{B}_{0,k}$. Then $I_2^\perp = I_1$.*

Proof. We have $I_2^\perp \subseteq I_1$ by the fact that $u_{i_j} u_A = 0$ where $A = \{i_1, i_2, \ldots, i_s\}$ and $u_{i_j} \in A$. Equality follows from Theorem 16 by using the fact that $\mathcal{B}_{0,k}$ is a Frobenius ring and examining the cardinalities. □

Corollary 3.1.4. *The ideal $\langle u_i\rangle$ is a self dual code of length 1 for $1 \leq i \leq k$.*

Proof. Follows from Theorem 17. □

3.1.1 Gray maps

Gray maps have been one of the most important aspects of codes over rings. In essence, they are a map from the n fold product of the ring to an ambient space where the finite field is the alphabet. This map emanates from the map that sends elements of the ring to elements in the the s fold product of the finite field, where s is determined by the ring. This map, in general, preserves weight and its intention is to create interesting codes over the finite field from codes over the ring.

In this section, we define a Gray map $\Theta : \mathcal{B}_{j,k} \to \mathbb{F}_{p^r}^{2^{j+k}}$. The map we give is a generalization of the map given in [9] as well as those given in [8], [24], [25], [26], and [27].

We can view $\mathcal{B}_{j,k}$ as $\mathcal{B}_{j,k-1} + u_k\mathcal{B}_{j,k-1}$ and write each element of $\mathcal{B}_{j,k}$ as $a + bu_k$. Then we can define the map $\Phi : \mathcal{B}_{j,k} \to \mathcal{B}_{j,k-1}^2$ as follows:

$$\Phi(a + bu_k) = (b, a + b). \tag{3.5}$$

We can view $\mathcal{B}_{j,k}$ as $\mathcal{B}_{j-1,k} + v_j\mathcal{B}_{j-1,k}$ and write each element of $\mathcal{B}_{j,k}$ as $a + bv_j$. Then we can define the following map $\Psi : \mathcal{B}_{j,k} \to \mathcal{B}_{j-1,k}^2$ as follows:

$$\Psi(a + bv_j) = (a, a + b). \tag{3.6}$$

We now define the map $\Theta : \mathcal{B}_{j,k} \to \mathbb{F}_{p^r}^{2^{j+k}}$ as follows:

$$\Theta(a) = \Psi^j(\Phi^k(a)). \tag{3.7}$$

Lemma 3.1.5. *Let $\mathcal{C}$ be a linear code over $\mathcal{B}_{j,k}$ of length n. Then $\Theta(\mathcal{C})$ is a linear code of length $n(2^{j+k})$.*

Proof. First, we shall show that the map Φ is linear. We have that

$$\begin{aligned}
\Phi((a + bu_k) + (a' + b'u_k)) &= \Phi((a + a') + (b + b')u_k) \\
&= (b + b', a + a' + b + b') \\
&= (b, a + b) + (b', a' + b') \\
&= \Phi(a + bu_k) + \Phi(a' + b'u_k).
\end{aligned}$$

Then if $c \in \mathcal{B}_{j,k-1}$ we have that

$$\begin{aligned}
\Phi(c(a + bu_k)) &= \Phi(ca + cbu_k) \\
&= (cb, ca + cb) \\
&= c(b, a + b) = c\Phi(a + bu_k).
\end{aligned}$$

This gives that Φ is linear.

Now, we show that the map Ψ is also linear. We have

$$\begin{array}{rcl} \Psi((a+bv_j)+(a'+b'v_j)) & = & \Psi((a+a')+(b+b')v_j) \\ & = & (a+a', a+a'+b+b') \\ & = & (a, a+b)+(a', a'+b') \\ & = & \Psi(a+bv_j)+\Psi(a'+b'v_j). \end{array}$$

If $c \in \mathcal{B}_{j-1,k}$ we have

$$\begin{array}{rcl} \Psi(c(a+bv_j)) & = & \Psi(ca+cbv_j) \\ & = & (ca, ca+cb) \\ & = & c(a, a+b) = c\Psi(a+bv_j). \end{array}$$

This gives that Ψ is linear.

Then the map Θ is the composition of $j+k$ linear maps and therefore the map Θ is a linear map. □

Define the swap maps $\sigma_1, \sigma_2, \ldots, \sigma_k$ that act on $\mathbb{F}_{p^r}^{2^{j+k}}$ as follows:

$$\sigma_k(\mathbf{c}_1, \mathbf{c}_2) = (\mathbf{c}_2, \mathbf{c}_1),\ \forall \mathbf{c}_1, \mathbf{c}_2 \in \mathbb{F}_{p^r}^{2^{j+k-1}},$$

$$\sigma_{k-1}(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4) = (\mathbf{c}_2, \mathbf{c}_1, \mathbf{c}_4, \mathbf{c}_3),\ \forall \mathbf{c}_i \in \mathbb{F}_{p^r}^{2^{j+k-2}}$$

continuing to

$$\sigma_1(\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_{2^{j+k}-1}, \mathbf{c}_{2^{j+k}}) = (\mathbf{c}_2, \mathbf{c}_1, \mathbf{c}_4, \mathbf{c}_3, \ldots, \mathbf{c}_{2^{j+k}}, \mathbf{c}_{2^{j+k}-1}),\ \forall \mathbf{c}_i \in \mathbb{F}_{p^r}^{2^j}.$$

The next theorem shows that the map Θ gives some automorphisms in the image under certain conditions.

Theorem 18. *If the base field of $\mathcal{B}_{j,k}$ has characteristic 2 and $\mathcal{C}$ is a linear code over $\mathcal{B}_{j,k}$, then $\Theta(\mathcal{C})$ has k swap maps, $\sigma_1, \sigma_2, \ldots, \sigma_k$ in their automorphism group.*

Proof. Given an element $a+bu_k$, multiplication by $1+u_k$ gives $(1+u_k)(a+bu_k) = a+(a+b)u_k$. We see that $\Phi(a+bu_k) = (b, a+b)$ and $\Phi(a+(a+b)u_k) = (a+b, 2a+b)$. Therefore, if the characteristic of the finite field is 2, then $\Phi(a+(a+b)u_k) = (a+b, b)$. This gives that for characteristic 2, multiplication by the unit $1+u_i$, for each i induces an automorphism of order 2 in the image that corresponds to a swap map. Finally, let σ_i denote the induced by multiplication by $1+u_i$. This gives the result. □

We now generalize two results from [8] and [24] respectively, where it is shown that for the maps defined in (3.5) and (3.6), the following two

$$\Phi(\mathcal{C}^{\perp}) = (\Phi(\mathcal{C}))^{\perp}$$

and

$$\Psi(\mathcal{C}^{\perp}) = (\Psi(\mathcal{C}))^{\perp}$$

hold when the base field of the ring is $\mathbb{F}_2$. We now show that the two hold for the ring $\mathcal{B}_{j,k}$ only when the base field is $\mathbb{F}_{2^r}$.

Lemma 3.1.6. *Let $\mathcal{C}$ be a code over $\mathcal{B}_{j,k}$. Let $\Phi : \mathcal{B}_{j,k} \to \mathcal{B}^2_{j,k-1}$ be defined as:*

$$\Phi(a + bu_k) = (b, a + b),$$

and let $\Psi : \mathcal{B}_{j,k} \to \mathcal{B}^2_{j-1,k}$ be defined as:

$$\Psi(a + bv_j) = (a, a + b).$$

Then $\Phi(\mathcal{C}^{\perp}) = (\Phi(\mathcal{C}))^{\perp}$ and $\Psi(\mathcal{C}^{\perp}) = (\Psi(\mathcal{C}))^{\perp}$ if and only if the characteristic of the ring $\mathcal{B}_{j,k}$ is 2.

Proof. We prove the result for Φ. The proof for Ψ is similar.

Let $\mathbf{v}_1 + \mathbf{w}_1 u_k$ and $\mathbf{v}_2 + \mathbf{w}_2 u_k$ be two orthogonal vectors in $\mathcal{B}_{j,k}$, where $\mathbf{v}_i, \mathbf{w}_i$ are vectors in $\mathcal{B}^n_{j,k-1}$. Then

$$[\mathbf{v}_1 + \mathbf{w}_1 u_k, \mathbf{v}_2 + \mathbf{w}_2 u_k] = [\mathbf{v}_1, \mathbf{v}_2] + ([\mathbf{v}_1, \mathbf{w}_2] + [\mathbf{v}_2, \mathbf{w}_1])u_k = 0.$$

Moreover, we have that $[\mathbf{v}_1, \mathbf{v}_2] = 0$ and $[\mathbf{v}_1, \mathbf{w}_2] + [\mathbf{v}_2, \mathbf{w}_1] = 0$.

The images of the vectors have the following inner-product:

$$[\Phi(\mathbf{v}_1 + \mathbf{w}_1 u_k), \Phi(\mathbf{v}_2 + \mathbf{w}_2 u_k)] = [(\mathbf{w}_1, \mathbf{v}_1 + \mathbf{w}_1), (\mathbf{w}_2, \mathbf{v}_2 + \mathbf{w}_2)] =$$

$$= [\mathbf{v}_1, \mathbf{v}_2] + [\mathbf{v}_1, \mathbf{w}_2] + [\mathbf{v}_2, \mathbf{w}_1] + 2[\mathbf{w}_1, \mathbf{w}_2] = 2[\mathbf{w}_1, \mathbf{w}_2].$$

This will only be zero if the characteristic of the ring $\mathcal{B}_{j,k}$ is 2, i.e., the base field is $\mathbb{F}_{2^r}$. Assuming that the characteristic of the ring $\mathcal{B}_{j,k}$ is 2 gives that $\Phi(\mathcal{C}^{\perp}) \subseteq (\Phi(\mathcal{C}))^{\perp}$. Since Φ is a bijection we have $\Phi(\mathcal{C}^{\perp}) = (\Phi(\mathcal{C}))^{\perp}$. □

We now have the following result.

Theorem 19. *Let $\mathcal{C}$ be a linear code over*

$$\mathcal{B}_{j,k} = \mathbb{F}_{2^r}[v_1, v_2, \ldots, v_j, u_1, u_2, \ldots, u_k]/\langle v_i^2 - v_i, u_i^2 \rangle.$$

Then $\Theta(\mathcal{C}^{\perp}) = \Theta(\mathcal{C})^{\perp}$.

Proof. Follows from Lemma 3.1.6. □

Corollary 3.1.7. *Let $\mathcal{C}$ be a self-dual code over*

$$\mathcal{B}_{j,k} = \mathbb{F}_{2^r}[v_1, v_2, \ldots, v_j, u_1, u_2, \ldots, u_k]/\langle v_i^2 - v_i, u_i^2 \rangle$$

of length n, then $\Theta(\mathcal{C})$ is a self-dual code over $\mathbb{F}_{2^r}$ of length $n(2^{j+k})$.

Proof. Follows from Theorem 19 and Lemma 3.1.5. □

3.1.2 Characters

In this section, we show that the ring $\mathcal{B}_{j,k}$ is a Frobenius ring by showing that there is a generating character for the associated character module.

In the present situation, we have that the ring $\mathcal{B}_{j,k}$ is isomorphic to $\oplus_{i=1}^{2^j}\mathcal{B}_{0,k}$. We only need to find a generating character for $\mathcal{B}_{0,k}$ then if $\chi_{\mathcal{B}_{0,k}}$ is the generating character for $\mathcal{B}_{0,k}$, we have that the character χ for R defined by

$$\chi(a) = \prod \chi_{\mathcal{B}_{0,k}}(a_i) \tag{3.8}$$

where a corresponds to $(a_1, a_2, \ldots, a_s)$ via the isomorphism, is a generating character for $\mathcal{B}_{j,k}$. To do this, we recall that any finite field of order p^e can be written as $\mathbb{F}_p(\xi)$ where ξ is a root of the irreducible polynomial $q(x)$ of degree e. That is $\mathbb{F}_p(\xi) \cong \mathbb{F}_p[x]/\langle q(x)\rangle$. Then each element in $\mathbb{F}_{p^e}$ can be written as $\sum a_i\xi^i$ where $a_i \in \mathbb{F}_p$. This leads immediately to the following lemma.

Lemma 3.1.8. *The ring $\mathcal{B}_{0,k} \cong \mathbb{F}_p[\xi, u_1, u_2, \ldots, u_k]/\langle q(x), u_i^2\rangle$, where all of the indeterminates commute and $q(x)$ is an irreducible polynomial of degree e. Each element in $\mathcal{B}_{0,k}$ can be written as $\sum_{s=0}^{e-1}\sum_{A\subseteq[k]}\xi^s(d_s)_A u_A$, where $d_S \in \mathbb{F}_p$. Let η be a complex primitive root of p-th root of unity. The generating character for $\mathcal{B}_{0,k}$ is given by $(\eta)^{\sum_{s=0}^{e-1}\sum_{A\subseteq[k]}(d_s)_A}$ showing that the ring is Frobenius.*

Proof. We have already explained why each element can be written in that form.

The unique minimal ideal of $\mathcal{B}_{0,k}$ is the orthogonal of the unique maximal ideal. Therefore, the minimal ideal is $\mathfrak{a} = \langle u_1u_2\cdots u_k\rangle$. It follows that any ideal that is contained in $ker(\chi)$ must contain the ideal $\mathfrak{a}$. But we have that $\chi(u_1u_2\cdots u_k) = \eta$ which gives that $ker(\chi)$ contains no non-trivial ideal. It follows that the map is a generating character and then the ring $\mathcal{B}_{0,k}$ is a Frobenius ring. □

The next theorem follows from the fact that the ring decomposes by the Chinese Remainder Theorem.

Theorem 20. *Let*

$$\chi_i(\sum_{s=0}^{e-1}\sum_{A\subseteq[k]}\xi^s(d_s)_A u_A) = (\eta)^{\sum_{s=0}^{e-1}\sum_{A\subseteq[k]}(d_s)_A}.$$

The ring $\mathcal{B}_{j,k} \cong \oplus_{i=1}^{2^j}\mathcal{B}_{0,k}$ has a generating character of the form:

$$\chi = \prod_{i=1}^{2^j}\chi_i,$$

giving that the ring $\mathcal{B}_{j,k}$ is a Frobenius ring.

Proof. We have that $\mathcal{B}_{j,k}$ is isomorphic to $\oplus_{i=1}^{2^j}\mathcal{B}_{0,k}$. It follows that the generating character is χ from Lemma 3.1.8.

Then the ring is Frobenius since it has a generating character. □

Let T be a square $(p^r)^{2^{j+k}}$ by $(p^r)^{2^{j+k}}$ matrix indexed by the elements of $\mathcal{B}_{j,k}$ and let

$$T_{a,b} = \chi_a(b) = \chi(ab), \tag{3.9}$$

where χ is the generating character of $\widehat{\mathcal{B}_{j,k}}$.

From Definition 25 we know that the complete weight enumerator of a code $\mathcal{C}$ is defined as

$$cwe_{\mathcal{C}}(x_{a_0}, x_{a_1}, \dots, x_{a_{r-1}}) = \sum_{\mathbf{c}\in\mathcal{C}} \prod_{i=0}^{r-1} x_{a_i}^{n_i(\mathbf{c})}, \tag{3.10}$$

where there are $n_i(\mathbf{c})$ occurrences of a_i in the vector $\mathbf{c}$.

It follows that if $\mathcal{C}$ is a linear code over $\mathcal{B}_{j,k}$, then

$$cwe_{\mathcal{C}^\perp} = \frac{1}{|\mathcal{C}|} cwe_{\mathcal{C}}(T \cdot (x_0, x_1, \dots, x_{r-1})). \tag{3.11}$$

By collapsing T as in [64], we get that if $\mathcal{C}$ is a linear code over $\mathcal{B}_{j,k}$, then

$$W_{\mathcal{C}^\perp}(x, y) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(x + (|\mathcal{B}_{j,k}| - 1)y, x - y),$$

where $W_{\mathcal{C}}(x, y)$ denotes the Hamming weight enumerator of $\mathcal{C}$.

Now recall that the Lee weight enumerator of a code $\mathcal{C}$ is defined as:

$$L_{\mathcal{C}}(x, y) = \sum_{\mathbf{c}\in\mathcal{C}} x^{N - wt_L(\mathbf{c})} y^{wt_L(\mathbf{c})} \tag{3.12}$$

where N is the length of $\Theta(\mathcal{C})$.

From Section 3.1, we know that when the characteristic of the finite field is 2, then $\Theta(\mathcal{C}^\perp) = \Theta(\mathcal{C})^\perp$ which allows us to find the MacWilliams identities for the Lee weight enumerators of codes over

$$\mathcal{B}_{j,k} = \mathbb{F}_{2^r}[v_1, v_2, \dots, v_j, u_1, u_2, \dots, u_k]/\langle v_i^2 - v_i, u_i^2\rangle$$

in the following way:

$$Lee_{\mathcal{C}^\perp}(z) = W_{\Theta(\mathcal{C}^\perp)}(z) = W_{\Theta(\mathcal{C})^\perp}(z)$$

where $Lee_{\mathcal{C}}(z)$ is the Lee weight enumerator and W denotes the Hamming weight enumerator. This leads to the following theorem.

Theorem 21. *Let $\mathcal{C}$ be a code of length n over*

$$\mathcal{B}_{j,k} = \mathbb{F}_{2^r}[v_1, v_2, \dots, v_j, u_1, u_2, \dots, u_k]/\langle v_i^2 - v_i, u_i^2\rangle$$

then

$$Lee_{\mathcal{C}^\perp}(z) = \frac{1}{|\mathcal{C}|}(1+z)^{2^{j+k}n} Lee_{\mathcal{C}}\left(\frac{1-z}{1+z}\right). \tag{3.13}$$

3.2 G-Codes over $\mathcal{B}_{j,k}$

In this section, we study group codes over the ring $\mathcal{B}_{j,k}$. We recall the following definitions from [29] that we apply in our setting:

- Let $\mathcal{B}_{j,k}$ be a local Frobenius ring with unique maximal ideal $\mathfrak{m}_i$, and let $\mathbf{w}_1, \dots, \mathbf{w}_s$ be vectors in $\mathcal{B}_{j,k}^n$. Then $\mathbf{w}_1, \dots, \mathbf{w}_s$ are modular independent if and only if $\sum \alpha_j \mathbf{w}_j = \mathbf{0}$ implies that $\alpha_j \in \mathfrak{m}_i$ for all j.

- Let $\mathbf{w}_1, \dots, \mathbf{w}_s$ be non-zero vectors in $\mathcal{B}_{j,k}^n$. Then $\mathbf{w}_1, \dots, \mathbf{w}_s$ are independent if $\sum \alpha_j \mathbf{w}_j = \mathbf{0}$ implies that $\alpha_j \mathbf{w}_j = \mathbf{0}$ for all j.

In [29], it is shown that if the ring is local, then any modular independent set is a minimal generating set and that if the ring is not local then any set that is both modular independent and independent is a minimal generating set. We shall call such a set a basis for the code.

In [23], it is shown that G-codes are linear codes in R^n if and only if they are left ideals in a group ring. Specifically, let $v \in \mathcal{B}_{j,k}G$ and let $\mathcal{C}(v)$ be the corresponding code in $\mathcal{B}_{j,k}^n$. Let $I(v)$ be the set of elements of $\mathcal{B}_{j,k}G$ 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 $\mathcal{B}_{j,k}G$.

The following is immediate from these results.

Lemma 3.2.1. *Let $v \in RG$, where R is a finite ring and G is a finite group. Then $Aut(\mathcal{C}(v))$ contains G as a subgroup.*

Proof. This follows from the fact that the action of G on the coordinates of $\mathcal{C}(v)$ necessarily holds the code invariant, since it corresponds to an ideal in the group ring. □

It is also shown in [23] that for a commutative Frobenius ring R, if $\mathcal{C}$ is a G-code for some G then its orthogonal $\mathcal{C}^\perp$ is also a G-code.

The following definition is given in [23].

Definition 52. *Let G be a finite group of order n and R a finite Frobenius commutative ring. Let $\mathcal{D}$ 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 $\mathcal{D}$ is held invariant by the action of multiplying the coordinate set marker by every element of G then the code $\mathcal{D}$ is called a quasi-group code of index s.*

The following is immediate from the definition.

Lemma 3.2.2. *Let $\mathcal{C}$ be a linear G-code over $B_{j,k}$, then $\Theta(\mathcal{C})$ is a quasi-G code of index 2^{j+k} in $\mathbb{F}_{p^r}^{n2^{j+k}}$.*

Lemma 3.2.3. *Let G be a finite group of order n and R a finite Frobenius commutative ring. A quasi-G code of index s in R^{sn} is equivalent to a group code under the action of the finite group G^s.*

Proof. Consider a quasi-G code of index s in R^{ns}. Reorder the coordinates of R^{ns} so that the n coordinates in the orbit of a coordinate under the action of group G are grouped together. Then the coordinates in R^{ns} are arranged into s copies of n coordinates where the code is held invariant by the action of the group G on each block of n coordinates. This gives the result. □

These two lemmas lead to the following important theorem.

Theorem 22. *Let $\mathcal{C}$ be a linear G-code over $B_{j,k}$, then $\Theta(\mathcal{C})$ is a $G^{2^{j+k}}$ code over $\mathbb{F}_{p^r}$, which gives that $Aut(\mathcal{C})$ necessarily contains $G^{2^{j+k}}$ as a subgroup.*

Proof. Lemma 3.2.2 gives that $\Theta(\mathcal{C})$ is a quasi-G code of index 2^{j+k}, then Lemma 3.2.3 gives that $\Theta(\mathcal{C})$ is a $G^{2^{j+k}}$ code. Finally Lemma 3.2.1 gives that $Aut(\mathcal{C})$ necessarily contains $G^{2^{j+k}}$ as a subgroup. □

This theorem can be extended even further in the case when the base field has even order.

Corollary 3.2.4. *Let $\mathcal{C}$ be a linear G-code over $B_{j,k}$, where the base field is $\mathbb{F}_{2^r}$. Then $Aut(\mathcal{C})$ necessarily contains $G^{2^{j+k}}$ and k swap maps which generate an additional subgroup.*

Proof. Theorem 22 gives the first part and Corollary 3.1.7 gives the second part. □

3.3 Projections and lifts of self-dual G-codes over $\mathcal{B}_{j,k}$

Define $\pi_{k,m} : \mathcal{B}_{j,k} \to \mathcal{B}_{j,m}$ by $\pi_{k,m}(u_i) = 0$ if $i > m$ and the identity elsewhere. That is, $\pi_{k,m}$ is the projection of $\mathcal{B}_{j,k}$ to $\mathcal{B}_{j,m}$. Note that if $k \leq m$, then $\pi_{k,m}$ is the identity map on $\mathcal{B}_{j,k}$. Also define $\pi_{j,l} : \mathcal{B}_{j,k} \to \mathcal{B}_{l,k}$ by $\pi_{j,l}(v_i) = 0$ if $i > l$ and the identity elsewhere. That is, $\pi_{j,l}$ is the projection of $\mathcal{B}_{j,k}$ to $\mathcal{B}_{l,k}$. Note that if $j \leq l$, then $\pi_{j,l}$ is the identity map on $\mathcal{B}_{j,k}$. Now, let $a \in \mathcal{B}_{j,k}$ and define

$$\Pi_{(j,k),(l,m)} : \mathcal{B}_{j,k} \to \mathcal{B}_{l,m}$$

by

$$\Pi_{(j,k),(l,m)}(a) = \pi_{j,l}(\pi_{k,m}(a)).$$

That is, $\Pi_{(j,k),(l,m)}$ is the projection of $\mathcal{B}_{j,k}$ to $\mathcal{B}_{l,m}$.

Example 3.3.1. *Let $\mathcal{B}_{1,1} = \mathbb{F}_3[v_1, u_1]/\langle v_1^2 - v_1, u_1^2\rangle$. Consider the projection of $a = 2 + v_1 + 2u_1 + 2v_1u_1$ from $\mathcal{B}_{1,1}$ to $\mathcal{B}_{0,0} = \mathbb{F}_3$. By the above definition we have that $\Pi_{(1,1),(0,0)}(2 + v_1 + 2u_1 + 2v_1u_1) = \pi_{1,0}(\pi_{1,0}(2 + v_1 + 2u_1 + 2v_1u_1)) = \pi_{1,0}(2 + v_1) = 2$.*

We allow j and k to be ∞ as well and denote this map as $\Pi_{(\infty,\infty),(l,m)}$. In this case the ring $B_{\infty,\infty}$ is an infinite ring. If $\mathcal{C} = \Pi_{(j,k),(l,m)}(\mathcal{C}')$ for some $\mathcal{C}'$ and $j > l, k > m$, then $\mathcal{C}'$ is said to be a lift of $\mathcal{C}$.

Theorem 23. *Let $\mathcal{C}(v)$ be a self-dual G-code over $\mathcal{B}_{j,k}$. Then $\Pi_{(j,k),(l,m)}(\mathcal{C}(v))$ is a self-orthogonal G-code over $\mathcal{B}_{l,m}$.*

Proof. We first show that $\Pi_{(j,k),(l,m)}(\mathcal{C}(v))$ is a self-orthogonal code over $\mathcal{B}_{l,m}$. Let $\mathbf{w} = (w_1, w_2, \ldots, w_n)$ and $\mathbf{z} = (z_1, z_2, \ldots, z_n)$ be vectors in $\mathcal{C}(v)$. We have that

$$\Pi_{(j,k),(l,m)}(\sum w_i z_i) = \sum (\Pi_{(j,k),(l,m)}(w_i)\Pi_{(j,k),(l,m)}(z_i)).$$

If $\sum w_i z_i = 0$ in $\mathcal{B}_{j,k}$ then $\Pi_{(j,k),(l,m)}(0) = 0$ so

$$\langle \Pi_{(j,k),(l,m)}(w), \Pi_{(j,k),(l,m)}(z)\rangle_{(l,m)} = 0.$$

Therefore $\Pi_{(j,k),(l,m)}(\mathcal{C}(v))$ is self-orthogonal.

To show that $\Pi_{(j,k),(l,m)}(\mathcal{C}(v))$ is also a G-code, we notice that the projection $\Pi_{(j,k),(l,m)}(\mathcal{C}(v)) = \Pi_{(j,k),(l,m)}(\langle\sigma(v)\rangle)$ corresponds to $\Pi_{(j,k),(l,m)}(v) = \Pi_{(j,k),(l,m)}(\alpha_{g_1})g_1 + \Pi_{(j,k),(l,m)}(\alpha_{g_2})g_2 + \cdots + \Pi_{(j,k),(l,m)}(\alpha_{g_n})g_n$, where $\alpha_{g_i} \in \mathcal{B}_{j,k}$. Thus $\Pi_{(j,k),(l,m)}(\mathcal{C}(v))$ is a G-code over $\mathcal{B}_{j,k}$. □

Theorem 24. *Let $w \in \mathcal{B}_{l,m}G$ generate a self-dual G-code over $\mathcal{B}_{l,m}$. Then w generates a self-dual code over $\mathcal{B}_{j,k}$ for all $j > l$ and $k > m$. Moreover, the self-dual code over $\mathcal{B}_{j,k}$ is also a G-code.*

Proof. Let $\mathcal{C}_{j,k}$ be the code generated by $w \in \mathcal{B}_{j,k}G$. We proceed by induction. We know $\mathcal{C}_{l,m}$ is a self-dual G-code by assumption.

Assume $\mathcal{C}_{j,k}$ is a self-dual G-code. We have that $\mathcal{C}_{j,k} = \langle\sigma(w)\rangle$, where $w \in \mathcal{B}_{j,k}G$, $\mathcal{C}_{j+1,k} = \mathcal{C}_{j,k} \oplus v_{j+1}\mathcal{C}_{j,k}$, where $\mathcal{C}_{j,k} \cap v_{j+1}\mathcal{C}_{j,k} = \emptyset$ and $\mathcal{C}_{j,k+1} = \mathcal{C}_{j,k} + u_{k+1}\mathcal{C}_{j,k}$, where $\mathcal{C}_{j,k} \cap u_{k+1}\mathcal{C}_{j,k} = \emptyset$. Then we have that $\mathcal{C}_{j+1,k} = \langle\sigma(w)\rangle \oplus v_{j+1}\langle\sigma(w)\rangle$, $\mathcal{C}_{j,k+1} = \langle\sigma(w)\rangle \oplus u_{k+1}\langle\sigma(w)\rangle$ and $|\mathcal{C}_{j+1,k}| = |\mathcal{C}_{j,k}||\mathcal{C}_{j,k}| = \sqrt{(p^r)^{2^{j+k}}}\sqrt{(p^r)^{2^{j+k}}} = \sqrt{(p^r)^{2^{j+k+1}}} = |\mathcal{C}_{j,k+1}|$. Then for vectors $\mathbf{w}, \mathbf{z}, \mathbf{w}', \mathbf{z}' \in \mathcal{C}_{j,k}$ we have (since $\mathcal{C}_{j,k}$ is self-dual by assumption),

$$\begin{aligned}[\mathbf{w} + v_{j+1}\mathbf{w}', \mathbf{z} + v_{j+1}\mathbf{z}']_{j+1} &= [\mathbf{w}, \mathbf{z}]_j + v_{j+1}[\mathbf{w}, \mathbf{z}']_j \\ &+ v_{j+1}[\mathbf{w}', \mathbf{z}]_j + v_{j+1}^2[\mathbf{w}', \mathbf{z}']_j = 0\end{aligned}$$

and

$$\begin{aligned}[\mathbf{w} + u_{k+1}\mathbf{w}', \mathbf{z} + u_{k+1}\mathbf{z}']_{k+1} &= [\mathbf{w}, \mathbf{z}]_k + u_{k+1}[\mathbf{w}, \mathbf{z}']_k \\ &+ u_{k+1}[\mathbf{w}', \mathbf{z}]_k + u_{k+1}^2[\mathbf{w}', \mathbf{z}']_k = 0.\end{aligned}$$

Hence $\mathcal{C}_{j+1,k}$ and $\mathcal{C}_{j,k+1}$ are self-dual codes since both are self-orthogonal and both have the proper cardinality. Therefore by mathematical induction $\mathcal{C}_{j,k}$ is a self-dual code for all finite j and k.

Next we prove that $\mathcal{C}_{\infty,\infty}$ is self-dual. If $\mathbf{z}, \mathbf{w} \in \mathcal{C}_{\infty,\infty}$ then there exist j and k with $\mathbf{z}, \mathbf{w} \in \mathcal{C}_{j,k}$ and hence $[\mathbf{z}, \mathbf{w}]_j = [\mathbf{z}, \mathbf{w}]_k = 0$ which implies $[\mathbf{z}, \mathbf{w}]_\infty = 0$. If $\mathbf{w} \in \mathcal{C}_{\infty,\infty}^\perp$ then $\mathbf{w} \in \mathcal{C}_{j,k}^\perp$ for some j and k which gives that $\mathbf{w} \in \mathcal{C}_{j,k}$ and hence in $\mathcal{C}_{\infty,\infty}$. Therefore $\mathcal{C}_{\infty,\infty}$ is self-dual.

To show that $\mathcal{C}_{j,k}$ is also a G-code, let $w = \alpha_{g_1}g_1 + \alpha_{g_2}g_2 + \cdots + \alpha_{g_n}g_n$, where $\alpha_{g_i} \in \mathcal{B}_{l,m}$. Then we see that $\mathcal{C}_{j+1,k} = \langle \sigma(w) \rangle \oplus v_{j+1} \langle \sigma(w) \rangle$ corresponds to $w + v_{j+1}w = (\alpha_{g_1} + v_{j+1}\alpha_{g_1})g_1 + (\alpha_{g_2} + v_{j+1}\alpha_{g_2})g_2 + \cdots + (\alpha_{g_n} + v_{j+1}\alpha_{g_n})g_n$ in $\mathcal{B}_{j+1,k}G$. Similarly, $\mathcal{C}_{j,k+1} = \langle \sigma(w) \rangle \oplus u_{k+1} \langle \sigma(w) \rangle$ corresponds to $w + u_{k+1}w = (\alpha_{g_1} + u_{k+1}\alpha_{g_1})g_1 + (\alpha_{g_2} + u_{k+1}\alpha_{g_2})g_2 + \cdots + (\alpha_{g_n} + u_{k+1}\alpha_{g_n})g_n$ in $\mathcal{B}_{j,k+1}G$. Thus $\mathcal{C}_{j,k}$ is a G-code. □

As a consequence of the above theorem, we have the following result.

Corollary 3.3.1. *If $\mathcal{C}$ is a self-dual G-code over $\mathcal{B}_{l,m}$ then there exists a self-dual code $\mathcal{C}'$ over $\mathcal{B}_{j,k}$, for $j > l$ and $k > m$ with $\Pi_{(j,k),(l,m)}(\mathcal{C}') = \mathcal{C}$.*

3.4 The Gray image of G-codes over $\mathcal{B}_{j,k}$

In this section, we restrict our attention to the ring $\mathcal{B}_{j,k} = \mathbb{F}_{2^r}[v_1, v_2, \ldots, v_j, u_1, u_2, \ldots, u_k]/\langle v_i^2 - v_i, u_i^2 \rangle$ and employ the Gray map defined in Section 3.1. We extend the Gray map Θ linearly to all of $\mathcal{B}_{j,k}$ and define the Lee weight of an element in $\mathcal{B}_{j,k}$ to be the Hamming weight of its image. We get a linear distance preserving map from $\mathcal{B}_{j,k}^n$ to $\mathbb{F}_{2^r}^{2^{j+k}n}$.

From Theorem 19 we know that for any linear code over $\mathcal{B}_{j,k}$ we have $\Theta(\mathcal{C}^\perp) = \Theta(\mathcal{C})^\perp$. As a consequence of this, we get the following result.

Corollary 3.4.1. *Let $\mathcal{C}$ be a G-code over $\mathcal{B}_{j,k}$. Then $\Theta(\mathcal{C}^\perp) = \Theta(\mathcal{C})^\perp$.*

Proof. From the definition of a G-code, we know that $\mathcal{C}$ is linear. The rest follows from Theorem 19. □

Theorem 25. *If $\mathcal{C}$ is a self-dual G-code of length n over $\mathcal{B}_{j,k}$, then $\Theta(\mathcal{C})$ is a self-dual G-code of length $n(2^{j+k})$ over $\mathbb{F}_{2^r}$.*

Proof. If $\mathcal{C} = \mathcal{C}^\perp$, then $\Theta(\mathcal{C}) = \Theta(\mathcal{C}^\perp) = \Theta(\mathcal{C})^\perp$ and we have that $\Theta(\mathcal{C})$ is self-dual. To show that $\Theta(\mathcal{C})$ is also a G-code, we see that $\Theta(\mathcal{C}) = \Theta(\langle \sigma(v) \rangle)$ corresponds to $\Theta(v) = \Theta(\alpha_{g_1})g_1 + \Theta(\alpha_{g_2})g_2 + \cdots + \Theta(\alpha_{g_n})g_n$ in $\mathbb{F}_{2^r}G$. Thus, $\Theta(\mathcal{C})$ is a G-code. □

Theorem 26. *Let $\mathcal{C}$ be a self-dual G-code over $\mathcal{B}_{j,k}$ of length n, then $\Theta(\mathcal{C})$ is a self-dual G^n-code of length $n(2^{j+k})$ over $\mathbb{F}_{2^r}$. If the base field is the binary field and the Lee weight of every codeword is* $0 \pmod 4$*, then $\Theta(\mathcal{C})$ is a Type II binary code.*

Proof. If $\mathcal{C} = \mathcal{C}^\perp$ then by Corollary 3.4.1, $\Theta(\mathcal{C}^\perp) = \Theta(\mathcal{C})^\perp$. □

Since Θ is distance preserving, the following corollary immediately follows from the bounds given in [62]. Note that for $j \geq 1$ and $k \geq 1$, the length of the binary image of a code over $\mathcal{B}_{j,k}$ will always be divisible by 4, hence the case $n \equiv 22 \pmod{24}$ is not possible for the image of an $\mathcal{B}_{j,k}$ code.

Corollary 3.4.2. *Let $d_L(n, I)$ and $d_L(n, II)$ denote the minimum distance of a Type I and Type II G-code over $\mathcal{B}_{j,k}$ of length n, respectively, where the base field is $\mathbb{F}_2$. Then, for $j \geq 1$ and $k \geq 1$, we have*

$$d_L(n, I), d_L(n, II) \leq 4 \left\lfloor \frac{2^{(j-1)+(k-1)}n}{6} \right\rfloor + 4.$$

3.5 Reversible G-codes over $\mathcal{B}_{j,k}$

Lastly in this chapter, we extend some results from [9] on reversible G-codes. Reversible codes have applications in DNA computing. The desirable property of a DNA code is that the reverse of a codeword with respect to a base of length 2^k is necessarily in the code. For a detailed description of DNA codes and their applications, please see [9]. In [9], it is also shown that with a particular listing of the elements of the finite group G of even order, the well-established isomorphism given in Equation (1.18) gives a reversible code. In this section, we extend some of the results from [9] over to our new ring $\mathcal{B}_{j,k}$. We start with a definition.

Definition 53. *A code $\mathcal{C}$ is said to be reversible of index α if $\mathbf{a}_i$ is a vector of length α and $\mathbf{c}^\alpha = (\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_{s-1}) \in \mathcal{C}$ implies that $(\mathbf{c}^\alpha)^r = (\mathbf{a}_{s-1}, \mathbf{a}_{s-2}, \ldots, \mathbf{a}_1, \mathbf{a}_0) \in \mathcal{C}$.*

For the remainder of this section, we fix the listing of the group elements as follows. Let G be a finite group of order $n = 2l$ and let $H = \{e, h_1, h_2, \ldots, h_{l-1}\}$ be a subgroup of index 2 in G. Let $\beta \notin H$ be an element in G, with $\beta^{-1} = \beta$. We list the elements of $G = \{g_1, g_2, \ldots, g_n\}$ as follows:

$$\{e, h_1, \ldots, h_{l-1}, \beta h_{l-1}, \beta h_{l-2}, \ldots, \beta h_2, \beta h_1, \beta\}. \tag{3.14}$$

In [9], the following is proven.

Theorem 27. *Let R be a finite ring. Let G be a finite group of order $n = 2l$ and let $H = \{e, h_1, h_2, \ldots, h_{l-1}\}$ be a subgroup of index 2 in G. Let $\beta \notin H$ be an element in G with $\beta^{-1} = \beta$. List the elements of G as in (3.14), then any linear G-code in R^n (a left ideal in RG) is a reversible code of index 1.*

We now employ the map defined in Section 3.1 and prove the following result.

Theorem 28. *Let G be a finite group of order $n = 2l$ and let $H = \{e, h_1, h_2, \ldots, h_{l-1}\}$ be a subgroup of index 2 in G. Let $\beta \notin H$ be an element in G with $\beta^{-1} = \beta$ and list the elements* *of G as in (3.14). If C is a linear G-code in $\mathcal{B}_{j,k}$ (a left ideal in $\mathcal{B}_{j,k}G$), then $\Theta(\mathcal{C})$ is a reversible $G^{2^{j+k}}$-code over $\mathbb{F}_{p^r}$.*

Proof. By Theorem 27, we have that $\mathcal{C}$ is a reversible code. Therefore, if $(c_0, c_1, \dots, c_{n-1}) \in \mathcal{C}$ we have that $(c_{n-1}, c_{n-2}, \dots, c_1, c_0) \in \mathcal{C}$, where $c_i \in \mathcal{B}_{j,k}$. Then $\Theta(c_i)$ is a vector of length 2^{j+k}. This gives that

$$(\Theta(c_0), \Theta(c_1), \dots, \Theta(c_{n-1})) \in \Theta(\mathcal{C})$$

and then

$$(\Theta(c_{n-1}), \Theta(c_{n-2}), \dots, \Theta(c_1), \Theta(c_0)) \in \Theta(\mathcal{C}).$$

This gives the first part of the result.

The last statement comes from Theorem 22.

□

The following result can also be found in [9].

Theorem 29. *Let R be a finite ring. Let $G_1, G_2, \dots, G_n$ be finite groups, each of order 2ℓ and let $H_1, H_2, \dots, H_n$, where $H_i = \{e_i, h_{i_1}, h_{i_2}, \dots, h_{i_{\ell-1}}\}$, be subgroups of index 2 in $G_1, G_2, \dots, G_n$ respectively. Let $\beta_i \notin H_i$ be an element in G_i with $\beta_i^{-1} = \beta_i$. List the elements of G_i as*

$$e_i, h_{i_1}, h_{i_2}, \dots, h_{i_{\ell-1}}, \beta_i h_{i_{\ell-1}}, \beta_i h_{i_{\ell-2}}, \dots, \beta_i h_{i_2}, \beta_i h_{i_1}, \beta_i. \tag{3.15}$$

Then any linear code D generated by the matrix

$$M = \begin{bmatrix} \sigma(v_1) & \sigma(v_2) & \sigma(v_3) & \dots & \sigma(v_n) \\ \sigma(v_n) & \sigma(v_{n-1}) & \sigma(v_{n-2}) & \dots & \sigma(v_1) \end{bmatrix},$$

where $v_i \in RG_i$, is a reversible code of index 1.

With the above theorem, our ring $\mathcal{B}_{j,k}$ and the Gray map from Section 3.1, we have the following result.

Theorem 30. *Let R be a finite ring. Let $G_1, G_2, \dots, G_n$ be finite groups, each of order 2ℓ and let $H_1, H_2, \dots, H_n$, where $H_i = \{e_i, h_{i_1}, h_{i_2}, \dots, h_{i_{\ell-1}}\}$, be subgroups of index 2 in $G_1, G_2, \dots, G_n$ respectively. Let $\beta_i \notin H_i$ be an element in G_i with $\beta_i^{-1} = \beta_i$. List the elements of G_i as*

$$e_i, h_{i_1}, h_{i_2}, \dots, h_{i_{\ell-1}}, \beta_i h_{i_{\ell-1}}, \beta_i h_{i_{\ell-2}}, \dots, \beta_i h_{i_2}, \beta_i h_{i_1}, \beta_i. \tag{3.16}$$

If $\mathcal{D}$ is a linear code in $\mathcal{B}_{j,k}^n$ generated by the matrix

$$M = \begin{bmatrix} \sigma(v_1) & \sigma(v_2) & \sigma(v_3) & \dots & \sigma(v_n) \\ \sigma(v_n) & \sigma(v_{n-1}) & \sigma(v_{n-2}) & \dots & \sigma(v_1) \end{bmatrix},$$

where $v_i \in \mathcal{B}_{j,k}G_i$, then $\Theta(\mathcal{D})$ is a reversible code over $\mathbb{F}_{p^r}$ of index 2^{j+k}.

Proof. By Theorem 29, we have that $\mathcal{D}$ is a reversible code of index 1. Therefore, if

$$((a_0^1, a_1^1, \ldots, a_{2\ell-1}^1), (a_0^2, a_1^2, \ldots, a_{2\ell-1}^2), \ldots, (a_0^n, a_1^n, \ldots, a_{2\ell-1}^n)) \in \mathcal{D}$$

we have that

$$((a_{2\ell-1}^n, a_{2\ell-2}^n, \ldots, a_0^n), (a_{2\ell-1}^{n-1}, a_{2\ell-2}^{n-1}, \ldots, a_0^{n-1}), \ldots, (a_{2\ell-1}^1, a_{2\ell-2}^1, \ldots, a_0^1)) \in \mathcal{D},$$

where $a_i^m \in \mathcal{B}_{j,k}$ with $i \in \{0, 1, 2, \ldots, 2\ell - 1\}$ and $m \in \{1, 2, 3, \ldots, n\}$. Then $\Theta(a_i^m)$ is a vector of length 2^{j+k}. This gives that

$$((\Theta(a_0^1), \Theta(a_1^1), \ldots, \Theta(a_{2\ell-1}^1)), (\Theta(a_0^2), \Theta(a_1^2), \ldots, \Theta(a_{2\ell-1}^2)), \ldots,$$

$$(\Theta(a_0^n), \Theta(a_1^n), \ldots, \Theta(a_{2\ell-1}^n))) \in \Theta(\mathcal{D})$$

then

$$((\Theta(a_{2\ell-1}^n), \Theta(a_{2\ell-2}^n), \ldots, \Theta(a_0^n)), \Theta((a_{2\ell-1}^{n-1}), \Theta(a_{2\ell-2}^{n-1}), \ldots, \Theta(a_0^{n-1})), \ldots,$$

$$(\Theta(a_{2\ell-1}^1), \Theta(a_{2\ell-2}^1), \ldots, \Theta(a_0^1))) \in \Theta(\mathcal{D}).$$

This proves the result. □

Chapter 4

Extending an Established Isomorphism between Group Rings and a Subring of the $n \times n$ Matrices

In this chapter, we extend the isomorphism given in Section 1.4.3. As we have mentioned earlier, the map σ gives different $n \times n$ matrices for different choices of the group G. These matrices are fully defined by the elements appearing in the first row - this property can be used in algebraic coding theory and specifically in constructing generator matrices so that the search field can be minimised but new codes can still be obtained. We presented an example in Chapter 2. In fact, there is an extensive research on constructing generator matrices with the use of the map σ, please see [14, 15, 16, 38, 40] for some interesting examples.

We want to continue in this direction, namely, we want to be able to construct more $n \times n$ matrices over the ring R that are fully defined by the elements appearing in the first row and cannot be obtained from the map σ. We therefore present an extension of the isomorphism given in [51]. Our extension enables one to construct many interesting, complex $n \times n$ matrices over the ring R that are fully defined by the elements appearing in the first row. We present our extend isomorphism and show when our matrices are not equivalent to the matrices obtained from the map σ. This chapter is joint work and the results are published in [18].

4.0.1 Extending the $M(G)$ Matrix

In this section, we extend the matrix $M(G)$ given in Equation (1.17). This matrix consists of entries which are the elements of the group G. In our extension, this is also the case, the matrices will consist of the elements of the group G but in a different order. We now extend the matrix $M(G)$.

Let $\{g_1, g_2, \ldots, g_n\}$ be a fixed listing of the elements of G. Let $\{h_1, h_2, \ldots, h_r\}$ be a fixed listing of the elements of H, where H is a group of order r. Here, 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 map:

$$\begin{array}{ccc} \multicolumn{3}{c}{\phi : H \mapsto G_r} \\ h_1 & \overset{\phi}{\to} & g_1 \\ h_2 & \overset{\phi}{\to} & g_2 \\ \vdots & \vdots & \vdots \\ h_r & \overset{\phi}{\to} & g_r. \end{array}$$

This map sends r distinct elements of the group H to r distinct elements of the group G.

Corollary 4.0.1. *The map ϕ is a bijection.*

Proof. The domain of ϕ consists of r distinct elements of H. The codomain of ϕ consists of r distinct elements of G. It is then clear from the above diagram that ϕ is bijective. □

Now, let $M(G)$ be the corresponding matrix of G. By partitioning $M(G)$ into an $\frac{n}{r} \times \frac{n}{r}$ block matrix, in which each block has order r and by applying the map ϕ in individual blocks we can form the following matrix:

$$\begin{pmatrix} A_1 & A_2 & A_3 & \ldots & A_{\frac{n}{r}} \\ A_{\frac{n}{r}+1} & A_{\frac{n}{r}+2} & A_{\frac{n}{r}+3} & \ldots & A_{\frac{2n}{r}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ A_{\frac{(r-1)n}{r}+1} & A_{\frac{(r-1)n}{r}+2} & A_{\frac{(r-1)n}{r}+3} & \ldots & A_{\frac{n^2}{r^2}} \end{pmatrix},$$

where each block has one of the two following forms:

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

or

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

where $l = \{1, 2, 3, \ldots, \frac{n^2}{r^2}\}$

and where:

$$\begin{array}{ccc} & \phi_l : H_i \mapsto G_r & \\ (h_i)_1 & \xrightarrow{\phi_l} & g_j^{-1}g_k \\ (h_i)_2 & \xrightarrow{\phi_l} & g_j^{-1}g_{k+1} \\ \vdots & \vdots & \vdots \\ (h_i)_r & \xrightarrow{\phi_l} & g_j^{-1}g_{k+(r-1)}. \end{array}$$

Here we have that when $l = 1$ then $j = 1, k = 1$, when $l = 2$ then $j = 1, k = r + 1$, when $l = 3$ then $j = 1, k = 2r + 1, \ldots$ 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 $j = r + 1, k = 2r + 1, \ldots$ when $l = \frac{2n}{r}$ then $j = r + 1, k = n - r + 1, \ldots,$ and so on.

By splitting $M(G)$ into an $\frac{n}{r} \times \frac{n}{r}$ block matrix we have that in each block, the first row consists of r distinct elements of G - this is because $M(G)$ is a Latin square. Thus, since we can apply the map ϕ in individual blocks, it allows us to employ different groups of order r in different blocks, i.e., we could employ $\frac{n^2}{r^2}$ different groups of order r. In the above, A'_l means we apply the map ϕ_l in this specific block. Now, $l \in \{1, 2, 3, \ldots, \frac{n^2}{r^2}\}$, which means we can employ $\frac{n^2}{r^2}$ different maps ϕ_l. We note that the map ϕ in the above matrix determines the order of the r distinct elements of G (which appear in the first row of a block) in the next rows. Thus a block of the A'_l form is fully determined by the elements appearing in the first row of that block. We call the above matrix the composite construction or for simplicity the composite matrix of G and $H_1, H_2, \ldots, H_{\frac{n^2}{r^2}}$ (depending on how many groups of order r we use) relative to these listings and denote it by $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$. We note that if the composite matrix consists of blocks which are of the A_l form only then it is equivalent to the matrix $M(G)$. We therefore, from now on assume that the composite matrix $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ consists of at least one block of the A'_l form.

Corollary 4.0.2. *Let G be a group of order n, such that $n \neq 1$. Let H_i be a group of order r such that r is a factor of n with $n > r$ and $r \neq 1$. We can then form a composite matrix $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ if and only if the order of the group G is not a prime number.*

Proof. Assume the order of the group G is n, where n is a prime number. We know from the above definition that to form a composite matrix there has to be a group of order r such that r is a factor of n with $n > r$ and $n, r \neq 1$. Since the order of the group G is prime, the only factors of n are n itself and 1, which does not satisfy the definition. This concludes the proof. □

We now present an example of a composite matrix. As stated above, the matrix will consist of the elements of the group G.

Example 4.0.1. *Let $G = \langle x, y \mid x^4 = y^2 = 1, x^y = x^{-1}\rangle \cong D_8$. Let $H_1 = \langle a, b \mid a^2 = b^2 = 1, ab = ba\rangle \cong C_2 \times C_2$. Let $H_2 = \langle c \mid c^4 = 1\rangle \cong C_4$. We now define the composite matrix as:*

$$M(G, H_1, H_2) = \begin{pmatrix} A'_1 & A'_2 \\ A'_3 & A'_4 \end{pmatrix},$$

where:

$$\begin{pmatrix} A'_1 & A'_2 \\ A'_3 & A'_4 \end{pmatrix} =$$

$$\left(\begin{array}{cccc|cccc}
g_1^{-1}g_1 & g_1^{-1}g_2 & g_1^{-1}g_3 & g_1^{-1}g_4 & g_1^{-1}g_5 & g_1^{-1}g_6 & g_1^{-1}g_7 & g_1^{-1}g_8 \\
\phi_1((h_1)_2^{-1}(h_1)_1) & \phi_1((h_1)_2^{-1}(h_1)_2) & \phi_1((h_1)_2^{-1}(h_1)_3) & \phi_1((h_1)_2^{-1}(h_1)_4) & \phi_2((h_2)_2^{-1}(h_2)_1) & \phi_2((h_2)_2^{-1}(h_2)_2) & \phi_2((h_2)_2^{-1}(h_2)_3) & \phi_2((h_2)_2^{-1}(h_2)_4) \\
\phi_1((h_1)_3^{-1}(h_1)_1) & \phi_1((h_1)_3^{-1}(h_1)_2) & \phi_1(h_1)_3^{-1}(h_1)_3) & \phi_1((h_1)_3^{-1}(h_1)_4) & \phi_2((h_2)_3^{-1}(h_2)_1) & \phi_2((h_2)_3^{-1}(h_2)_2) & \phi_2((h_2)_3^{-1}(h_2)_3) & \phi_2((h_2)_3^{-1}(h_2)_4) \\
\phi_1((h_1)_4^{-1}(h_1)_1) & \phi_1((h_1)_4^{-1}(h_1)_2) & \phi_1(h_1)_4^{-1}(h_1)_3) & \phi_1((h_1)_4^{-1}(h_1)_4) & \phi_2((h_2)_4^{-1}(h_2)_1) & \phi_2((h_2)_4^{-1}(h_2)_2) & \phi_2((h_2)_4^{-1}(h_2)_3) & \phi_2((h_2)_4^{-1}(h_2)_4) \\
\hline
g_5^{-1}g_1 & g_5^{-1}g_2 & g_5^{-1}g_3 & g_5^{-1}g_4 & g_5^{-1}g_5 & g_5^{-1}g_6 & g_5^{-1}g_7 & g_5^{-1}g_8 \\
\phi_3((h_2)_2^{-1}(h_2)_1) & \phi_3((h_2)_2^{-1}(h_2)_2) & \phi_3((h_2)_2^{-1}(h_2)_3) & \phi_3((h_2)_2^{-1}(h_2)_4) & \phi_4((h_1)_2^{-1}(h_1)_1) & \phi_4((h_1)_2^{-1}(h_1)_2) & \phi_4((h_1)_2^{-1}(h_1)_3) & \phi_4((h_1)_2^{-1}(h_1)_4) \\
\phi_3((h_2)_3^{-1}(h_2)_1) & \phi_3((h_2)_3^{-1}(h_2)_2) & \phi_3((h_2)_3^{-1}(h_2)_3) & \phi_3((h_2)_3^{-1}(h_2)_4) & \phi_4((h_1)_3^{-1}(h_1)_1) & \phi_4((h_1)_3^{-1}(h_1)_2) & \phi_4((h_1)_3^{-1}(h_1)_3) & \phi_4((h_1)_3^{-1}(h_1)_4) \\
\phi_3((h_2)_4^{-1}(h_2)_1) & \phi_3((h_2)_4^{-1}(h_2)_2) & \phi_3((h_2)_4^{-1}(h_2)_3) & \phi_3((h_2)_4^{-1}(h_2)_4) & \phi_4((h_1)_4^{-1}(h_1)_1) & \phi_4((h_1)_4^{-1}(h_1)_2) & \phi_4((h_1)_4^{-1}(h_1)_3) & \phi_4((h_1)_4^{-1}(h_1)_4)
\end{array}\right),$$

and where:

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

$$\phi_3 : \begin{array}{c} (h_2)_i \xrightarrow{\phi_3} g_5^{-1}g_i \\ \text{for } i = \{1, 2, 3, 4\} \end{array} \qquad \phi_4 : \begin{array}{c} (h_1)_i \xrightarrow{\phi_4} g_5^{-1}g_j \\ \text{for when } \{i = 1, j = 5, i = 2, j = 6, i = 3, j = 7, i = 4, j = 8\}. \end{array}$$

This results in the following composite matrix

$$\begin{pmatrix} A'_1 & A'_2 \\ A'_3 & A'_4 \end{pmatrix} = \left(\begin{array}{cccc|cccc}
1 & x & x^2 & x^3 & y & xy & x^2y & x^3y \\
x & 1 & x^3 & x^2 & x^3y & y & xy & x^2y \\
x^2 & x^3 & 1 & x & x^2y & x^3y & y & xy \\
x^3 & x^2 & x & 1 & xy & x^2y & x^3y & y \\
\hline
y & x^3y & x^2y & xy & 1 & x^3 & x^2 & x \\
xy & y & x^3y & x^2y & x^3 & 1 & x & x^2 \\
x^2y & xy & y & x^3y & x^2 & x & 1 & x^3 \\
x^3y & x^2y & xy & y & x & x^2 & x^3 & 1
\end{array}\right).$$

In the above example, all four blocks have the A'_l form. We observe that in the resulting composite matrix, all four blocks are Latin squares and the composite matrix itself is a Latin square.

Example 4.0.2. *Let $G = \langle x \mid x^8 = 1\rangle \cong C_8$. 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:*

$$M(G, H_1) = \begin{pmatrix} A'_1 & A_2 \\ A_3 & A_4 \end{pmatrix} =$$

$$= \left(\begin{array}{cccc|cccc}
g_1^{-1}g_1 & g_1^{-1}g_2 & g_1^{-1}g_3 & g_1^{-1}g_4 & g_1^{-1}g_5 & g_1^{-1}g_6 & g_1^{-1}g_7 & g_1^{-1}g_8 \\
\phi_1((h_1)_2^{-1}(h_1)_1) & \phi_1((h_1)_2^{-1}(h_1)_2) & \phi_1((h_1)_2^{-1}(h_1)_3) & \phi_1((h_1)_2^{-1}(h_1)_4) & g_2^{-1}g_5 & g_2^{-1}g_6 & g_2^{-1}g_7 & g_2^{-1}g_8 \\
\phi_1((h_1)_3^{-1}(h_1)_1) & \phi_1((h_1)_3^{-1}(h_1)_2) & \phi_1((h_1)_3^{-1}(h_1)_3) & \phi_1((h_1)_3^{-1}(h_1)_4) & g_3^{-1}g_5 & g_3^{-1}g_6 & g_3^{-1}g_7 & g_3^{-1}g_8 \\
\phi_1((h_1)_4^{-1}(h_1)_1) & \phi_1((h_1)_4^{-1}(h_1)_2) & \phi_1((h_1)_4^{-1}(h_1)_3) & \phi_1((h_1)_4^{-1}(h_1)_4) & g_4^{-1}g_5 & g_4^{-1}g_6 & g_4^{-1}g_7 & g_4^{-1}g_8 \\
\hline
g_5^{-1}g_1 & g_5^{-1}g_2 & g_5^{-1}g_3 & g_5^{-1}g_4 & g_5^{-1}g_5 & g_5^{-1}g_6 & g_5^{-1}g_7 & g_5^{-1}g_8 \\
g_6^{-1}g_1 & g_6^{-1}g_2 & g_6^{-1}g_3 & g_6^{-1}g_4 & g_6^{-1}g_5 & g_6^{-1}g_6 & g_6^{-1}g_7 & g_6^{-1}g_8 \\
g_7^{-1}g_1 & g_7^{-1}g_2 & g_7^{-1}g_3 & g_7^{-1}g_4 & g_7^{-1}g_5 & g_7^{-1}g_6 & g_7^{-1}g_7 & g_7^{-1}g_8 \\
g_8^{-1}g_1 & g_8^{-1}g_2 & g_8^{-1}g_3 & g_8^{-1}g_4 & g_8^{-1}g_5 & g_8^{-1}g_6 & g_8^{-1}g_7 & g_8^{-1}g_8
\end{array}\right),$$

where:

$$\phi_1 : \begin{array}{ccc} (h_1)_i & \xrightarrow{\phi_1} & g_1^{-1}g_i \\ \text{for } i = \{1,2,3,4\} & & \end{array},$$

in A_1'. This results in the following composite matrix

$$\begin{pmatrix} A_1' & A_2 \\ A_3 & A_4 \end{pmatrix} = \left(\begin{array}{cccc|cccc}
1 & x & x^2 & x^3 & x^4 & x^5 & x^6 & x^7 \\
x & 1 & x^3 & x^2 & x^3 & x^4 & x^5 & x^6 \\
x^2 & x^3 & 1 & x & x^2 & x^3 & x^4 & x^5 \\
x^3 & x^2 & x & 1 & x & x^2 & x^3 & x^4 \\
\hline
x^4 & x^5 & x^6 & x^7 & 1 & x & x^2 & x^3 \\
x^3 & x^4 & x^5 & x^6 & x^7 & 1 & x & x^2 \\
x^2 & x^3 & x^4 & x^5 & x^6 & x^7 & 1 & x \\
x & x^2 & x^3 & x^4 & x^5 & x^6 & x^7 & 1
\end{array}\right).$$

We can see that in A_1' the 4 distinct elements of G appear exactly once in each row and exactly once in each column of that block. This is not the case in A_2, A_3 and A_4. Also the composite matrix itself is not a Latin square.

It is possible that the composite matrix $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ is a Latin square as we saw in Example 4.0.1. Before we prove when this is the case, we first look at the form of the composite matrix.

The rows of the matrix $M(G)$ from Equation (1.17) have the following form $g_j^{-1}g_1 \;\; g_j^{-1}g_2 \;\; \ldots \;\; g_j^{-1}g_n$ where j is the jth row of $M(G)$. This is not the case in the composite matrix $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$. We now look at an example.

Example 4.0.3. *Let $G = \langle x, y \mid x^4 = y^2 = 1, x^y = x^{-1} \rangle \cong D_8$. 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:*

$$M(G, H_1) = \begin{pmatrix} A_1' & A_2' \\ A_3 & A_4 \end{pmatrix} =$$

$$\left(\begin{array}{cccc|cccc}
g_1^{-1}g_1 & g_1^{-1}g_2 & g_1^{-1}g_3 & g_1^{-1}g_4 & g_1^{-1}g_5 & g_1^{-1}g_6 & g_1^{-1}g_7 & g_1^{-1}g_8 \\
\phi_1((h_1)_2^{-1}(h_1)_1) & \phi_1((h_1)_2^{-1}(h_1)_2) & \phi_1((h_1)_2^{-1}(h_1)_3) & \phi_1((h_1)_2^{-1}(h_1)_4) & \phi_2((h_1)_2^{-1}(h_1)_1) & \phi_2((h_1)_2^{-1}(h_1)_2) & \phi_2((h_1)_2^{-1}(h_1)_3) & \phi_2((h_1)_2^{-1}(h_1)_4) \\
\phi_1((h_1)_3^{-1}(h_1)_1) & \phi_1((h_1)_3^{-1}(h_1)_2) & \phi_1(h_1)_3^{-1}(h_1)_3) & \phi_1((h_1)_3^{-1}(h_1)_4) & \phi_2((h_1)_3^{-1}(h_1)_1) & \phi_2((h_1)_3^{-1}(h_1)_2) & \phi_2((h_1)_3^{-1}(h_1)_3) & \phi_2((h_1)_3^{-1}(h_1)_4) \\
\phi_1((h_1)_4^{-1}(h_1)_1) & \phi_1((h_1)_4^{-1}(h_1)_2) & \phi_1(h_1)_4^{-1}(h_1)_3) & \phi_1((h_1)_4^{-1}(h_1)_4) & \phi_2((h_1)_4^{-1}(h_1)_1) & \phi_2((h_1)_4^{-1}(h_1)_2) & \phi_2((h_1)_4^{-1}(h_1)_3) & \phi_2((h_1)_4^{-1}(h_1)_4) \\
\hline
g_5^{-1}g_1 & g_5^{-1}g_2 & g_5^{-1}g_3 & g_5^{-1}g_4 & g_5^{-1}g_5 & g_5^{-1}g_6 & g_5^{-1}g_7 & g_5^{-1}g_8 \\
g_6^{-1}g_1 & g_6^{-1}g_2 & g_6^{-1}g_3 & g_6^{-1}g_4 & g_6^{-1}g_5 & g_6^{-1}g_6 & g_6^{-1}g_7 & g_6^{-1}g_8 \\
g_7^{-1}g_1 & g_7^{-1}g_2 & g_7^{-1}g_3 & g_7^{-1}g_4 & g_7^{-1}g_5 & g_7^{-1}g_6 & g_7^{-1}g_7 & g_7^{-1}g_8 \\
g_8^{-1}g_1 & g_8^{-1}g_2 & g_8^{-1}g_3 & g_8^{-1}g_4 & g_8^{-1}g_5 & g_8^{-1}g_6 & g_8^{-1}g_7 & g_8^{-1}g_8
\end{array}\right),$$

where:

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

in A_1' and A_2'. This results in a composite matrix of the following form:

$$M(G, H_1) = \left(\begin{array}{cccc|cccc}
1 & x & x^2 & x^3 & y & xy & x^2y & x^3y \\
x & 1 & x^3 & x^2 & xy & y & x^3y & x^2y \\
x^2 & x^3 & 1 & x & x^2y & x^3y & y & xy \\
x^3 & x^2 & x & 1 & x^3y & x^2y & xy & y \\
\hline
y & x^3y & x^2y & xy & 1 & x^3 & x^2 & x \\
xy & y & x^3y & x^2y & x & 1 & x^3 & x^2 \\
x^2y & xy & y & x^3y & x^2 & x & 1 & x^3 \\
x^3y & x^2y & xy & y & x^3 & x^2 & x & 1
\end{array}\right).$$

We now look at the rows of $M(G, H_1)$. Let $r_1, r_2, \ldots, r_8$ be the rows of $M(G, H_1)$, then each row is formed by multiplying the elements $g_1, g_2, \ldots, g_n$ of G by some elements of G. These elements of G do not have to be the same but they can be. For example:

$$r_1 = (1)1 + (1)x + (1)x^2 + (1)x^3 + (1)y + (1)xy + (1)x^2y + (1)x^3y,$$

the first row of $M(G, H_1)$ is obtained by multiplying each element of G by the same group element of G, namely 1. Next,

$$r_2 = (x)1 + (x^3)x + (x)x^2 + (x^3)x^3 + (x)y + (x^3)xy + (x)x^2y + (x^3)x^3y,$$

the second row of $M(G, H_1)$ is obtained by multiplying each element of G by the group elements of G; x or x^3. Lastly,

$$r_8 = (x^3y)1 + (x^3y)x + (x^3y)x^2 + (x^3y)x^3 + (x^3y)y + (x^3y)xy + (x^3y)x^2y + (x^3y)x^3y,$$

the eighth row of $M(G, H_1)$ is obtained by multiplying each element of G by the same group element of G, namely x^3y.

The above example highlights the difference between the matrix $M(G)$ from Equation (1.17) and the composite matrix $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$. Namely, each row of $M(G)$ is of the form $g_j^{-1}g_1 \;\; g_j^{-1}g_2 \;\; \ldots \;\; g_j^{-1}g_n$ where j is the jth row of $M(G)$ (we multiply each element of G by the same group element of G). In the composite matrix $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$, some rows are formed by multiplying the elements of G by different group elements of G. Therefore, we can define the composite matrix $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ as:

$$M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}}) = \begin{pmatrix} g_{1_1}g_1 & g_{1_2}g_2 & g_{1_3}g_3 & \cdots & g_{1_n}g_n \\ g_{2_1}g_1 & g_{2_2}g_2 & g_{2_3}g_3 & \cdots & g_{2_n}g_n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g_{n_1}g_1 & g_{n_2}g_2 & g_{n_3}g_3 & \cdots & g_{n_n}g_n \end{pmatrix}, \tag{4.1}$$

where the elements g_{j_i} are simply the group elements G. Which elements of G these are, depends on how the composite matrix is defined, i.e., what groups of order r we employ and how we define the ϕ_l map in individual blocks.

This notation of the composite matrix $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ can be used to prove the following results.

Corollary 4.0.3. *The matrix $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ is equivalent to the matrix $M(G)$ if the group elements g_{j_i} in Equation (4.1) are the same for all $i \in \{1, 2, \ldots, n\}$.*

Proof. If $g_{j_1} = g_{j_2} = g_{j_3} = \cdots = g_{j_n}$ in Equation (4.1), then each row of $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ has the form $g_jg_1 \;\; g_jg_2 \;\; \ldots \;\; g_jg_n$ where g_j is an element of G. This is exactly what each row of $M(G)$ looks like. Thus $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ is equivalent to $M(G)$. □

Corollary 4.0.4. *Let $\{g_1, g_2, g_3, \ldots, g_n\}$ be a listing of the elements of the group G and let $M(G)$ be the corresponding matrix. Let $\{g_1', g_2', g_3', \ldots, g_n'\}$ be a different ordering of the elements of the group G and let $M'(G)$ be the corresponding matrix. Then $M'(G)$ is permutation equivalent to $M(G)$.*

Proof. Without loss of generality, let $\{g_3, g_2, g_1, g_n, g_{n-1}, g_{n-3}\}$ be a listing of the elements of the group G. Then

$$M'(G) = \begin{pmatrix} g_3^{-1}g_3 & g_3^{-1}g_2 & g_3^{-1}g_1 & g_3^{-1}g_n & g_3^{-1}g_{n-1} & \cdots & g_3^{-1}g_{n-3} \\ g_2^{-1}g_3 & g_2^{-1}g_2 & g_2^{-1}g_1 & g_2^{-1}g_n & g_2^{-1}g_{n-1} & \cdots & g_2^{-1}g_{n-3} \\ g_1^{-1}g_3 & g_1^{-1}g_2 & g_1^{-1}g_1 & g_1^{-1}g_n & g_1^{-1}g_{n-1} & \cdots & g_1^{-1}g_{n-3} \\ g_n^{-1}g_3 & g_n^{-1}g_2 & g_n^{-1}g_1 & g_n^{-1}g_n & g_n^{-1}g_{n-1} & \cdots & g_n^{-1}g_{n-3} \\ g_{n-1}^{-1}g_3 & g_{n-1}^{-1}g_2 & g_{n-1}^{-1}g_1 & g_{n-1}^{-1}g_n & g_{n-1}^{-1}g_{n-1} & \cdots & g_{n-1}^{-1}g_{n-3} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ g_{n-3}^{-1}g_3 & g_{n-3}^{-1}g_2 & g_{n-3}^{-1}g_1 & g_{n-3}^{-1}g_n & g_{n-3}^{-1}g_{n-1} & \cdots & g_{n-3}^{-1}g_{n-3} \end{pmatrix}.$$

It is clear that $M'(G)$ is row and column permutation equivalent to $M(G)$. This concludes the proof. □

We now show when the matrix $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ is not permutation equivalent to $M(G)$ for any arrangement of the elements of G.

Theorem 4.0.5. *Let $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ be a composite matrix such that at least one row of $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ has the following form*

$$g_{j_1}g_1 \quad g_{j_2}g_2 \quad g_{j_3}g_3 \quad \cdots \quad g_{j_n}g_n,$$

where g_{j_i} is not the same for all $i \in \{1, 2, \ldots, n\}$. Here, $g_i, g_{j_i} \in G$ and j is the jth row of the matrix $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$. Then $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ is not permutation equivalent to $M(G)$ for any arrangement of the elements of G.

Proof. Assume that the matrix $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ is permutation equivalent to the matrix $M(G)$ for some arrangements of the elements of G. This is equivalent to say that the matrix $M(G)$ is permutation equivalent to the matrix $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ for some specific arrangement of the elements of G. But we know from the previous corollary that for any arrangement of the elements of G, the corresponding matrix is permutation equivalent to $M(G)$. This implies that for any arrangement of the elements of G, the rows of the corresponding matrix will be of the form $g_jg_1 \quad g_jg_2 \quad g_jg_3 \quad \ldots \quad g_jg_n$ where g_j is any element of G. In other words, there will be no row of the form $g_{j_1}g_1 \quad g_{j_2}g_2 \quad g_{j_3}g_3 \quad \ldots \quad g_{j_n}g_n$, where g_{j_i} is not the same for all $i \in \{1, 2, \ldots, n\}$. Thus, $M(G)$ is not permutation equivalent to $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ for any arrangements of the elements of G. This contradicts our assumption. Therefore, the matrix $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ is not permutation equivalent to the matrix $M(G)$ for any arrangement of the elements of G. □

We now present another example of a composite matrix that is a Latin square and then prove when such matrices form Latin squares.

Example 4.0.4. *Let $G = \langle x, y \mid x^4 = y^2 = 1, x^y = x^{-1}\rangle \cong D_8$. 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:*

$$M(G, H_1) = \begin{pmatrix} A_1' & A_2 \\ A_3 & A_4 \end{pmatrix} =$$

$$= \left(\begin{array}{cccc|cccc}
g_1^{-1}g_1 & g_1^{-1}g_2 & g_1^{-1}g_3 & g_1^{-1}g_4 & g_1^{-1}g_5 & g_1^{-1}g_6 & g_1^{-1}g_7 & g_1^{-1}g_8 \\
\phi_1((h_1)_2^{-1}(h_1)_1) & \phi_1((h_1)_2^{-1}(h_1)_2) & \phi_1((h_1)_2^{-1}(h_1)_3) & \phi_1((h_1)_2^{-1}(h_1)_4) & g_2^{-1}g_5 & g_2^{-1}g_6 & g_2^{-1}g_7 & g_2^{-1}g_8 \\
\phi_1((h_1)_3^{-1}(h_1)_1) & \phi_1((h_1)_3^{-1}(h_1)_2) & \phi_1((h_1)_3^{-1}(h_1)_3) & \phi_1((h_1)_3^{-1}(h_1)_4) & g_3^{-1}g_5 & g_3^{-1}g_6 & g_3^{-1}g_7 & g_3^{-1}g_8 \\
\phi_1((h_1)_4^{-1}(h_1)_1) & \phi_1((h_1)_4^{-1}(h_1)_2) & \phi_1((h_1)_4^{-1}(h_1)_3) & \phi_1((h_1)_4^{-1}(h_1)_4) & g_4^{-1}g_5 & g_4^{-1}g_6 & g_4^{-1}g_7 & g_4^{-1}g_8 \\
\hline
g_5^{-1}g_1 & g_5^{-1}g_2 & g_5^{-1}g_3 & g_5^{-1}g_4 & g_5^{-1}g_5 & g_5^{-1}g_6 & g_5^{-1}g_7 & g_5^{-1}g_8 \\
g_6^{-1}g_1 & g_6^{-1}g_2 & g_6^{-1}g_3 & g_6^{-1}g_4 & g_6^{-1}g_5 & g_6^{-1}g_6 & g_6^{-1}g_7 & g_6^{-1}g_8 \\
g_7^{-1}g_1 & g_7^{-1}g_2 & g_7^{-1}g_3 & g_7^{-1}g_4 & g_7^{-1}g_5 & g_7^{-1}g_6 & g_7^{-1}g_7 & g_7^{-1}g_8 \\
g_8^{-1}g_1 & g_8^{-1}g_2 & g_8^{-1}g_3 & g_8^{-1}g_4 & g_8^{-1}g_5 & g_8^{-1}g_6 & g_8^{-1}g_7 & g_8^{-1}g_8
\end{array}\right),$$

where:

$$\phi_1 : \begin{array}{ccc} (h_1)_i & \xrightarrow{\phi_1} & g_1^{-1}g_i \\ \text{for } i = \{1,2,3,4\} & & \end{array},$$

in A_1'. This results in the following composite matrix

$$\begin{pmatrix} A_1' & A_2 \\ A_3 & A_4 \end{pmatrix} = \left(\begin{array}{cccc|cccc} 1 & x & x^2 & x^3 & y & xy & x^2y & x^3y \\ x & 1 & x^3 & x^2 & x^3y & y & xy & x^2y \\ x^2 & x^3 & 1 & x & x^2 & x^3y & y & xy \\ x^3 & x^2 & x & 1 & xy & x^2y & x^3y & y \\ \hline y & x^3y & x^2y & xy & 1 & x^3 & x^2 & x \\ xy & y & x^3y & x^2y & x & 1 & x^3 & x^2 \\ x^2y & xy & y & x^3y & x^2 & x & 1 & x^3 \\ x^3y & x^2y & xy & y & x^3 & x^2 & x & 1 \end{array}\right).$$

Here, each of the blocks; A_1', A_2, A_3 and A_4, is a Latin square. Also, the composite matrix itself is a Latin square.

Corollary 4.0.6. *The composite matrix $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ is a Latin square if the elements $g_{j_i}g_i$ of Equation (4.1), each appear exactly once in each row and exactly once in each column of $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$.*

Proof. Follows from the definition of a Latin square. □

The above corollary potentially opens up a new direction of research. Namely, since the composite matrix $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ can have a form of a Latin square, can one consider the possible groups G and H_i to establish exactly and for what groups the composite matrix is a Latin square? The classification of Latin squares of different lengths is an ongoing research problem so perhaps one could investigate the structure of the composite matrix $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ further to find out if this matrix construction can in any way help with classification and enumeration of Latin squares. Please see [11] for a very detailed explanation of Latin squares and open problems in this area.

The process of forming the composite matrix can be applied over again to individual blocks of $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$. Assume the block of $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ has an order r_1 such that r_1 is not prime and $r_1 > 1$. Assume also that there exists a group $(H_i)'$ of order r_2 such that r_2 is a factor of r_1 with $r_1 > r_2$ and $r_1, r_2 \neq 1$. Then we can split the block of $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ into an $\frac{r_1}{r_2} \times \frac{r_1}{r_2}$ block where each block has order r_2, where in at least one, we apply the bijective map $\phi_{l'}' : (H_i)' \mapsto G_{r_2}$, (here $l' \in \{1, 2, 3, \ldots, \frac{r_1^2}{r_2^2}\}$ where r_2 distinct elements of $(H_i)'$ get sent to r_2 distinct elements of G. We can repeat this process again if there exists a group $(H_i)''$ of order r_3 such that r_3 is a factor of r_2 with $r_2 > r_3$ and

$r_3 \neq 1$ and so on. We can therefore form a more complex composite construction. We now look at an example.

Example 4.0.5. *Let $G = \langle x, y \mid x^8 = y^2 = 1, x^y = x^{-1}\rangle \cong D_{16}$. Let $H_1 = \langle a, b \mid a^4 = b^2 = 1, ab = ba\rangle \cong C_4 \times C_2$. Let $(H_1)' = \langle c, d \mid c^2 = d^2 = 1, cd = dc\rangle \cong C_2 \times C_2$ We now define the composite matrix as:*

$$M'(G, H_1((H_1)')) = \begin{pmatrix} (A_1')' & A_2 \\ A_3 & A_4' \end{pmatrix},$$

where

$$A_1' = \begin{pmatrix}
g_1^{-1}g_1 & g_1^{-1}g_2 & g_1^{-1}g_3 & g_1^{-1}g_4 & g_1^{-1}g_5 & g_1^{-1}g_6 & g_1^{-1}g_7 & g_1^{-1}g_8 \\
\phi_1'((h_1')_2^{-1}(h_1')_1) & \phi_1'((h_1')_2^{-1}(h_1')_2) & \phi_1'((h_1')_2^{-1}(h_1')_3) & \phi_1'((h_1')_2^{-1}(h_1')_4) & \phi_2'((h_1')_2^{-1}(h_1')_1) & \phi_2'((h_1')_2^{-1}(h_1')_2) & \phi_2'((h_1')_2^{-1}(h_1')_3) & \phi_2'((h_1')_2^{-1}(h_1')_4) \\
\phi_1'((h_1')_3^{-1}(h_1')_1) & \phi_1'((h_1')_3^{-1}(h_1')_2) & \phi_1'((h_1')_3^{-1}(h_1')_3) & \phi_1'((h_1')_3^{-1}(h_1')_4) & \phi_2'((h_1')_3^{-1}(h_1')_1) & \phi_2'((h_1')_3^{-1}(h_1')_2) & \phi_2'((h_1')_3^{-1}(h_1')_3) & \phi_2'((h_1')_3^{-1}(h_1')_4) \\
\phi_1'((h_1')_4^{-1}(h_1')_1) & \phi_1'((h_1')_4^{-1}(h_1')_2) & \phi_1'((h_1')_4^{-1}(h_1')_3) & \phi_1'((h_1')_4^{-1}(h_1')_4) & \phi_2'((h_1')_4^{-1}(h_1')_1) & \phi_2'((h_1')_4^{-1}(h_1')_2) & \phi_2'((h_1')_4^{-1}(h_1')_3) & \phi_2'((h_1')_4^{-1}(h_1')_4) \\
\phi_1((h_1)_5^{-1}(h_1)_1) & \phi_1((h_1)_5^{-1}(h_1)_2) & \phi_1((h_1)_5^{-1}(h_1)_3) & \phi_1((h_1)_5^{-1}(h_1)_4) & \phi_1((h_1)_5^{-1}(h_1)_5) & \phi_1((h_1)_5^{-1}(h_1)_6) & \phi_1((h_1)_5^{-1}(h_1)_7) & \phi_1((h_1)_5^{-1}(h_1)_8) \\
\phi_3'((h_1')_2^{-1}(h_1')_1) & \phi_3'((h_1')_2^{-1}(h_1')_2) & \phi_3'((h_1')_2^{-1}(h_1')_3) & \phi_3'((h_1')_2^{-1}(h_1')_4) & \phi_4'((h_1')_2^{-1}(h_1')_1) & \phi_4'((h_1')_2^{-1}(h_1')_2) & \phi_4'((h_1')_2^{-1}(h_1')_3) & \phi_4'((h_1')_2^{-1}(h_1')_4) \\
\phi_3'((h_1')_3^{-1}(h_1')_1) & \phi_3'((h')_3^{-1}(h_1')_2) & \phi_3'((h_1')_3^{-1}(h_1')_3) & \phi_3'((h_1')_3^{-1}(h_1')_4) & \phi_4'((h_1')_3^{-1}(h_1')_1) & \phi_4'((h_1')_3^{-1}(h_1')_2) & \phi_4'((h_1')_3^{-1}(h_1')_3) & \phi_4'((h_1')_3^{-1}(h_1')_4) \\
\phi_3'((h_1')_4^{-1}(h_1')_1) & \phi_3'((h_1')_4^{-1}(h_1')_2) & \phi_3'((h_1')_4^{-1}(h_1')_3) & \phi_3'((h_1')_4^{-1}(h_1')_4) & \phi_4'((h_1')_4^{-1}(h_1')_1) & \phi_4'((h_1')_4^{-1}(h_1')_2) & \phi_4'((h_1')_4^{-1}(h_1')_3) & \phi_4'((h_1')_4^{-1}(h_1')_4)
\end{pmatrix},$$

$$A_2 = \begin{pmatrix}
g_1^{-1}g_9 & g_1^{-1}g_{10} & g_1^{-1}g_{11} & g_1^{-1}g_{12} & g_1^{-1}g_{13} & g_1^{-1}g_{14} & g_1^{-1}g_{15} & g_1^{-1}g_{16} \\
g_2^{-1}g_9 & g_2^{-1}g_{10} & g_2^{-1}g_{11} & g_2^{-1}g_{12} & g_2^{-1}g_{13} & g_2^{-1}g_{14} & g_2^{-1}g_{15} & g_2^{-1}g_{16} \\
g_3^{-1}g_9 & g_3^{-1}g_{10} & g_3^{-1}g_{11} & g_3^{-1}g_{12} & g_3^{-1}g_{13} & g_3^{-1}g_{14} & g_3^{-1}g_{15} & g_3^{-1}g_{16} \\
g_4^{-1}g_9 & g_4^{-1}g_{10} & g_4^{-1}g_{11} & g_4^{-1}g_{12} & g_4^{-1}g_{13} & g_4^{-1}g_{14} & g_4^{-1}g_{15} & g_4^{-1}g_{16} \\
g_5^{-1}g_9 & g_5^{-1}g_{10} & g_5^{-1}g_{11} & g_5^{-1}g_{12} & g_5^{-1}g_{13} & g_5^{-1}g_{14} & g_5^{-1}g_{15} & g_5^{-1}g_{16} \\
g_6^{-1}g_9 & g_6^{-1}g_{10} & g_6^{-1}g_{11} & g_6^{-1}g_{12} & g_6^{-1}g_{13} & g_6^{-1}g_{14} & g_6^{-1}g_{15} & g_6^{-1}g_{16} \\
g_7^{-1}g_9 & g_7^{-1}g_{10} & g_7^{-1}g_{11} & g_7^{-1}g_{12} & g_7^{-1}g_{13} & g_7^{-1}g_{14} & g_7^{-1}g_{15} & g_7^{-1}g_{16} \\
g_8^{-1}g_9 & g_8^{-1}g_{10} & g_8^{-1}g_{11} & g_8^{-1}g_{12} & g_8^{-1}g_{13} & g_8^{-1}g_{14} & g_8^{-1}g_{15} & g_8^{-1}g_{16}
\end{pmatrix}, A_3 = \begin{pmatrix}
g_9^{-1}g_1 & g_9^{-1}g_2 & g_9^{-1}g_3 & g_9^{-1}g_4 & g_9^{-1}g_5 & g_9^{-1}g_6 & g_9^{-1}g_7 & g_9^{-1}g_8 \\
g_{10}^{-1}g_1 & g_{10}^{-1}g_2 & g_{10}^{-1}g_3 & g_{10}^{-1}g_4 & g_{10}^{-1}g_5 & g_{10}^{-1}g_6 & g_{10}^{-1}g_7 & g_{10}^{-1}g_8 \\
g_{11}^{-1}g_1 & g_{11}^{-1}g_2 & g_{11}^{-1}g_3 & g_{11}^{-1}g_4 & g_{11}^{-1}g_5 & g_{11}^{-1}g_6 & g_{11}^{-1}g_7 & g_{11}^{-1}g_8 \\
g_{12}^{-1}g_1 & g_{12}^{-1}g_2 & g_{12}^{-1}g_3 & g_{12}^{-1}g_4 & g_{12}^{-1}g_5 & g_{12}^{-1}g_6 & g_{12}^{-1}g_7 & g_{12}^{-1}g_8 \\
g_{13}^{-1}g_1 & g_{13}^{-1}g_2 & g_{13}^{-1}g_3 & g_{13}^{-1}g_4 & g_{13}^{-1}g_5 & g_{13}^{-1}g_6 & g_{13}^{-1}g_7 & g_{13}^{-1}g_8 \\
g_{14}^{-1}g_1 & g_{14}^{-1}g_2 & g_{14}^{-1}g_3 & g_{14}^{-1}g_4 & g_{14}^{-1}g_5 & g_{14}^{-1}g_6 & g_{14}^{-1}g_7 & g_{14}^{-1}g_8 \\
g_{15}^{-1}g_1 & g_{15}^{-1}g_2 & g_{15}^{-1}g_3 & g_{15}^{-1}g_4 & g_{15}^{-1}g_5 & g_{15}^{-1}g_6 & g_{15}^{-1}g_7 & g_{15}^{-1}g_8 \\
g_{16}^{-1}g_1 & g_{16}^{-1}g_2 & g_{16}^{-1}g_3 & g_{16}^{-1}g_4 & g_{16}^{-1}g_5 & g_{16}^{-1}g_6 & g_{16}^{-1}g_7 & g_{16}^{-1}g_8
\end{pmatrix},$$

$$A_4 = \begin{pmatrix}
g_9^{-1}g_9 & g_9^{-1}g_{10} & g_9^{-1}g_{11} & g_9^{-1}g_{12} & g_9^{-1}g_{13} & g_9^{-1}g_{14} & g_9^{-1}g_{15} & g_9^{-1}g_{16} \\
\phi_4((h_1)_2^{-1}(h_1)_1) & \phi_4((h_1)_2^{-1}(h_1)_2) & \phi_4((h_1)_2^{-1}(h_1)_3) & \phi_4((h_1)_2^{-1}(h_1)_4) & \phi_4((h_1)_2^{-1}(h_1)_5) & \phi_4((h_1)_2^{-1}(h_1)_6) & \phi_4((h_1)_2^{-1}(h_1)_7) & \phi_4((h_1)_2^{-1}(h_1)_8) \\
\phi_4((h_1)_3^{-1}(h_1)_1) & \phi_4((h_1)_3^{-1}(h_1)_2) & \phi_4((h_1)_3^{-1}(h_1)_3) & \phi_4((h_1)_3^{-1}(h_1)_4) & \phi_4((h_1)_3^{-1}(h_1)_5) & \phi_4((h_1)_3^{-1}(h_1)_6) & \phi_4((h_1)_3^{-1}(h_1)_7) & \phi_4((h_1)_3^{-1}(h_1)_8) \\
\phi_4((h_1)_4^{-1}(h_1)_1) & \phi_4((h_1)_4^{-1}(h_1)_2) & \phi_4((h_1)_4^{-1}(h_1)_3) & \phi_4((h_1)_4^{-1}(h_1)_4) & \phi_4((h_1)_4^{-1}(h_1)_5) & \phi_4((h_1)_4^{-1}(h_1)_6) & \phi_4((h_1)_4^{-1}(h_1)_7) & \phi_4((h_1)_4^{-1}(h_1)_8) \\
\phi_4((h_1)_5^{-1}(h_1)_1) & \phi_4((h_1)_5^{-1}(h_1)_2) & \phi_4((h_1)_5^{-1}(h_1)_3) & \phi_4((h_1)_5^{-1}(h_1)_4) & \phi_4((h_1)_5^{-1}(h_1)_5) & \phi_4((h_1)_5^{-1}(h_1)_6) & \phi_4((h_1)_5^{-1}(h_1)_7) & \phi_4((h_1)_5^{-1}(h_1)_8) \\
\phi_4((h_1)_6^{-1}(h_1)_1) & \phi_4((h_1)_6^{-1}(h_1)_2) & \phi_4((h_1)_6^{-1}(h_1)_3) & \phi_4((h_1)_6^{-1}(h_1)_4) & \phi_4((h_1)_6^{-1}(h_1)_5) & \phi_4((h_1)_6^{-1}(h_1)_6) & \phi_4((h_1)_6^{-1}(h_1)_7) & \phi_4((h_1)_6^{-1}(h_1)_8) \\
\phi_4((h_1)_7^{-1}(h_1)_1) & \phi_4((h_1)_7^{-1}(h_1)_2) & \phi_4((h_1)_7^{-1}(h_1)_3) & \phi_4((h_1)_7^{-1}(h_1)_4) & \phi_4((h_1)_7^{-1}(h_1)_5) & \phi_4((h_1)_7^{-1}(h_1)_6) & \phi_4((h_1)_7^{-1}(h_1)_7) & \phi_4((h_1)_7^{-1}(h_1)_8) \\
\phi_4((h_1)_8^{-1}(h_1)_1) & \phi_4((h_1)_8^{-1}(h_1)_2) & \phi_4((h_1)_8^{-1}(h_1)_3) & \phi_4((h_1)_8^{-1}(h_1)_4) & \phi_4((h_1)_8^{-1}(h_1)_5) & \phi_4((h_1)_8^{-1}(h_1)_6) & \phi_4((h_1)_8^{-1}(h_1)_7) & \phi_4((h_1)_8^{-1}(h_1)_8)
\end{pmatrix}.$$

Here:

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

$$\phi_3' : \begin{array}{c} (h_1')_i \xrightarrow{\phi_3'} \phi_1((h_1)_5^{-1}(h_1)_i) \\ \text{for } i = \{1,2,3,4\} \end{array} \qquad \phi_4' : \begin{array}{c} (h_1')_i \xrightarrow{\phi_4'} \phi((h_1)_5^{-1}(h_1)_j) \\ \text{for when } \{i=1, j=5, i=2, j=6, i=3, j=7, i=4, j=8\}, \end{array}$$

in $(A_1')'$ and

$$\phi_4 : \begin{array}{c} (h_1)_i \xrightarrow{\phi_4} g_9^{-1}g_j \\ \text{for when } \{i=1, j=5, i=2, j=6, i=3, j=7, i=4, j=8, \ldots, i=8, j=16\} \end{array}$$

in A_4'.

This results in the following composite matrix

$$\begin{pmatrix} (A_1')' & A_2 \\ A_3 & A_4' \end{pmatrix} = \left(\begin{array}{c|c} \begin{array}{cc|cc} X_1 & Y_1 & X_2 & Y_2 \\ Y_1 & X_1 & Y_2 & X_2 \\ \hline X_2 & Y_2 & X_1 & Y_1 \\ Y_2 & X_2 & Y_1 & X_1 \end{array} & X_3 \\ \hline X_3^T & \begin{array}{c|c} X_4 & Y_4 \\ \hline Y_4 & X_4 \end{array} \end{array}\right),$$

where $X_1 = circ(1, x)$, $Y_1 = circ(x^2, x^3), X_2 = circ(x^4, x^5)$, $Y_2 = circ(x^6, x^7)$, $X_3 = circ(y, xy, x^2y, x^3y, x^4y, x^5y, x^6y, x^7y)$, $X_4 = circ(1, x^7, x^6, x^5)$ and $Y_4 = circ(x^4, x^3, x^2, x)$.

We finish this section with one more result.

Corollary 4.0.7. *Let $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r_1^2}})$ be a composite matrix. Here, G is a group of order n and H_i is a group of order r_1. Without loss of generality, assume A is an $\frac{n}{r_1} \times \frac{n}{r_1}$ block of the composite matrix $M(G, H_1, H_2, \ldots, H_{\frac{n^2}{r_1^2}})$. Now let $(H_i)'$ be a group of order r_2, $(H_i)''$ be a group of order r_3 and so on. Also, let r_1 be a factor of n, r_2 be a factor of r_1, r_3 be a factor of r_2 and so on, such that $n > r_1 > r_2 > r_3 > \ldots$ and $n, r_i \neq 1$. We can then keep repeating the process of forming the composite constructions on the block A until the divisor of $\frac{r_i}{r_{i+1}}$ is a prime number.*

Proof. If the divisor of $\frac{r_i}{r_{i+1}}$ is not a prime number then the resulting block matrix where each block has an order r_{i+1} can be split further into a more complex composite construction by considering a group of order less than r_{i+1} (not equal to 1) which is also a factor of r_{i+1}. If the divisor of $\frac{r_i}{r_{i+1}}$ is a prime number then the resulting composite construction has blocks of order r_{i+1} which is prime and the process can not be repeated again. This concludes the proof. □

4.0.2 Extending an Established Isomorphism

In this section, we extend the isomorphism given by T. Hurley in [51]. This isomorphism sends a group ring element of order n to an $n \times n$ matrix in which the entries are the elements of R. This is also the case in our extended isomorphism but with a significant difference. Namely, our extension allows us to construct more complex matrices over R. We will present some interesting examples. We now extend the well-known isomorphism.

Let $v = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \ldots, \alpha_{g_n} g_n \in RG$. We now form the $R(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$ matrix of v denoted by $M((G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}}), v)$ and define it as follows:

$$\begin{pmatrix} \alpha_{g_{1_1}g_1} & \alpha_{g_{1_2}g_2} & \alpha_{g_{1_3}g_3} & \dots & \alpha_{g_{1_n}g_n} \\ \alpha_{g_{2_1}g_1} & \alpha_{g_{2_2}g_2} & \alpha_{g_{2_3}g_3} & \dots & \alpha_{g_{2_n}g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_{n_1}g_1} & \alpha_{g_{n_2}g_2} & \alpha_{g_{n_3}g_3} & \dots & \alpha_{g_{n_n}g_n} \end{pmatrix}.$$

Thus $M((G, H_1, H_2, \dots, H_{\frac{n^2}{r^2}}), v)$ is in $R_{n\times n}$. Here, we assume that the order of the group G is not prime so that the above matrix is formed as the composite matrix in the previous section, i.e., the elements g_{j_i} are the group elements of G - which elements these are, depends again on how the composite matrix is defined.

If we label the first column of $M((G, H_1, H_2, \dots, H_{\frac{n^2}{r^2}}), v)$ as g_1, the second column by g_2, and so on, and if $b = \sum_{i=1}^{n} \beta_{g_1} g_i \in RG$ then the coefficient of g_i in the product $b * v$ is $(\beta_{g_1}, \beta_{g_2}, \dots, \beta_{g_n})$ times the $i-$th column of $M((G, H_1, H_2, \dots, H_{\frac{n^2}{r^2}}), v)$.

Given the listings of the elements of G and $H_1, H_2, \dots, H_{\frac{n^2}{r^2}}$, form the matrix $M(G, H_1, H_2, \dots, H_{\frac{n^2}{r^2}})$ relative to these listings. Then an $R(G, H_1, H_2, \dots, H_{\frac{n^2}{r^2}})$ matrix over R is a matrix obtained by substituting elements of R for elements of $M(G, H_1, H_2, \dots, H_{\frac{n^2}{r^2}})$, so that if two entries in $M(G, H_1, H_2, \dots, H_{\frac{n^2}{r^2}})$ are equal as group elements then the corresponding entries in the $R(G, H_1, H_2, \dots, H_{\frac{n^2}{r^2}})$ matrix are equal.

Given the entries of the first row of an $R(G, H_1, H_2, \dots, H_{\frac{n^2}{r^2}})$ matrix, the entries of the other rows are determined from the matrix $M(G, H_1, H_2, \dots, H_{\frac{n^2}{r^2}})$ of $G, H_1, H_2, \dots, H_{\frac{n^2}{r^2}}$; each row and each column consists of elements of the first row determined by the matrix of $G, H_1, H_2, \dots, H_{\frac{n^2}{r^2}}$.

We now extend two results from [51].

Theorem 4.0.8. *Let $M(G, H_1, H_2, \dots, H_{\frac{n^2}{r^2}})$ be a composite matrix. Then there is a bijective ring homomorphism between RG and the $n \times n$ $M(G, H_1, H_2, \dots, H_{\frac{n^2}{r^2}})$ - composite matrices over R. This bijective ring homomorphism is given by $\Omega : v \mapsto M((G, H_1, H_2, \dots, H_{\frac{n^2}{r^2}}), v)$.*

Proof. Let $G = \{g_1, g_2, \dots, g_n\}$ be the listing of the elements of G and let $H = \{h_1, h_2, \dots, h_r\}$ be the listing of the elements of H. Also, let M denote the set of $(G, H_1, H_2, \dots)$ - composite matrices relative to these listings. Now define mapping $\Omega : RG \to M$ as follows. Suppose $v = \sum_{i=1}^{n} \alpha_{g_i} g_i$. Then

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

This mapping is obviously additive, surjective and injective. It is thus sufficient to show that Ω is multiplicative. Consider $w = \sum_{i=1}^{n} \beta_{g_i} g_i$ and

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

Suppose $w * v = c$, where $c = \sum_{i=1}^{n} \gamma_{g_i} g_i$. Then

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

and this of course is $MG(RG, c) = \Omega(v * w)$ as required. □

We call the matrix $\Omega(v)$ a composite construction or a composite matrix over R. From now on Ω denotes the mapping Ω as in Theorem 4.0.8.

Theorem 4.0.9. *Suppose R has an identity. Then $v \in RG$ is a unit in RG if and only if $\Omega(v)$ is a unit in $M_n(R)$.*

Proof. Suppose v is a unit in RG and that w is its inverse. Then $v * w = 1_{RG}$ and hence $\Omega(v * w) = \Omega(1_{RG}) = I_n$, the identity matrix in $M_n(R)$. Thus $\Omega(v) * \Omega(w) = I_n$. Similarly $\Omega(w) * \Omega(v) = I_n$ and so $\Omega(v)$ is invertible in $M_n(R)$.

Suppose now $\Omega(v)$ is a unit in $M_n(R)$ and let B denote its inverse. Let $v = \alpha_{g_i} g_1 + \alpha_{g_2} g_2 + \dots + \alpha_{g_n} g_n$. Then

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

We do not know a priori that B is a RG - matrix. Let $b = (\beta_1, \beta_2, \dots, \beta_n)$ be the first row of B. Then

$$\begin{array}{ccccccccc} \beta_1\alpha_{g_{1_1}g_1} & + & \beta_2\alpha_{g_{2_1}g_1} & + & \dots & + & \beta_n\alpha_{g_{n_1}g_1} & = & 1, \\ \beta_1\alpha_{g_{1_2}g_2} & + & \beta_2\alpha_{g_{2_2}g_2} & + & \dots & + & \beta_n\alpha_{g_{n_2}g_2} & = & 0, \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta_1\alpha_{g_{1_n}g_n} & + & \beta_2\alpha_{g_{2_n}g_n} & + & \dots & + & \beta_n\alpha_{g_{n_n}g_n} & = & 0. \end{array} \tag{4.2}$$

Now $v = \alpha_{g_i} g_1 + \alpha_{g_2} g_2 + \dots + \alpha_{g_n} g_n = \alpha_{g_{j_i}g_1} g_{j_i} g_1 + \alpha_{g_{j_i}g_2} g_{j_i} g_2 + \dots + \alpha_{g_{j_i}g_n} g_{j_i} g_n$, for each i and j, $1 \leq i \leq n$ and $1 \leq j \leq n$.

Define $w = \beta_1 g_{1_1}^{-1} + \beta_2 g_{1_2}^{-1} + \dots + \beta_n g_{1_n}^{-1}$. Then:

$$\beta_i g_{j_i}^{-1}(\alpha_{g_1}g_1 + \alpha_{g_2}g_2 + \cdots + \alpha_{g_n}g_n) = \beta_i g_{j_i}^{-1}\alpha_{g_{j_i}g_1}g_{j_i}g_1 + \beta_i g_{j_i}^{-1}\alpha_{g_{j_i}g_2}g_{j_i}g_2 +$$
$$+ \cdots + \beta_i g_{j_i}^{-1}\alpha_{g_{j_i}g_n}g_{j_i}g_n = \beta_i\alpha_{g_{j_i}g_1}g_1 + \beta_i\alpha_{g_{j_i}g_2}g_2 + \cdots + \beta_i\alpha_{g_{j_i}g_n}g_n.$$

Hence: $v * w = (\beta_1 g_{1_1}^{-1} + \beta_2 g_{1_2}^{-1} + \cdots + \beta_n g_{1_n}^{-1})(\alpha_{g_i}g_1 + \alpha_{g_2}g_2 + \cdots + \alpha_{g_n}g_n)$ equals to:

$$\begin{array}{ccccccccc} & \beta_1\alpha_{g_{1_1}g_1}g_1 & + & \beta_2\alpha_{g_{2_1}g_1}g_1 & + & \dots & + & \beta_n\alpha_{g_{n_1}g_1}g_1 \\ + & \beta_1\alpha_{g_{1_2}g_2}g_2 & + & \beta_2\alpha_{g_{2_2}g_2}g_2 & + & \dots & + & \beta_n\alpha_{g_{n_2}g_2}g_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ + & \beta_1\alpha_{g_{1_n}g_n}g_n & + & \beta_2\alpha_{g_{2_n}g_n}g_n & + & \dots & + & \beta_n\alpha_{g_{n_n}g_n}g_n \end{array}$$

and this is g_1 from the above. Thus $g_1^{-1} * w$ is the inverse of v and v is a unit in RG.

□

The next results are a direct result of the above and also extensions of the results found in [51].

Corollary 4.0.10. *If the inverse of an $R(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$- matrix exists then this inverse is also an $R(G, H_1, H_2, \ldots, H_{\frac{n^2}{r^2}})$- matrix.*

Corollary 4.0.11. *When R is commutative, then the element v, is a unit in RG if and only if $\Omega(v)$ is a unit in $M_n(R)$ if and only if $det(\Omega(v))$ is a unit in R.*

Corollary 4.0.12. *Let $v \in RG$. Then v is a zero divisor in RG if and only if $\Omega(v)$ is a zero divisor in $M_n(R)$.*

Corollary 4.0.13. *When R is commutative and has no zero-divisors, v is a zero divisor in RG if and only if $\Omega(v)$ is a zero divisor in $M_n(R)$ if and only if $det(\Omega(v)) = 0$.*

Theorem 4.0.14. *When R is a field, $v \neq 0$ in RG is either a unit or a zero divisor, depending on whether $det(\Omega(v)) \neq 0$ or $det(\Omega(v)) = 0$.*

Chapter 5

Composite Matrices from Group Rings, Composite G-Codes and Constructions of Self-Dual Codes

In this chapter, we employ the matrix $\Omega(v)$ from Chapter 4 and define a new family of codes. Namely, we let the matrix $\Omega(v)$ generate the codes over the ring R. We call this new family of codes, composite group codes or for simplicity, composite G-codes. We show that the codes we construct are ideals in the group ring RG and that the dual of a composite G-code is also a composite G-code. We show that our code construction cannot produce the putative $[72, 36, 16]$ code. We also study self-orthogonal composite G-codes over finite commutative Frobenius rings. Our new family of codes extends the idea of group codes studied in [23] where the well-established isomorphism given in Equation (1.18) is used to study linear group codes with. In this chapter, we show that one can construct the same class of group codes as in [23] and even more. That is, our technique allows one to construct more codes that are held invariant under the action of the group G than the technique given in [23].

We consider generator matrices of the form $[I_n \mid \Omega(v)]$ and show when such generator matrices produce self-dual codes over finite commutative Frobenius rings. We employ these generator matrices and together with some well-known code constructions methods, we find many new binary self-dual codes with parameters $[68, 34, 12]$. Our approach is similar to the one from [39], where many new binary self-dual codes with parameters $[68, 34, 12]$ are found by considering generator matrices of the form $[I_n \mid \sigma(v)]$, where $\sigma(v)$ is the matrix given in Equation (1.18). Since our extended isomorphism allows one to construct more complex $n \times n$ matrices over a ring R, it gives one more chances of obtaining more new codes via these matrices. In fact, we show in this chapter that this is the case as we find many new extremal binary self-dual codes of length 68.

5.1 Composite G-codes

We now 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 :

$$\mathcal{C}(v) = \langle \Omega(v) \rangle, \tag{5.1}$$

where $\Omega(v)$ is the composite matrix defined in Chapter 4. The code is formed by taking the row space of $\Omega(v)$ over the ring R. As in [23], the code $\mathcal{C}(v)$ 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 1. *Let* $G = \langle x, y \mid x^4 = 1, y^2 = x^2, x^y = x^{-1} \rangle \cong Q_8$*. Let* $v = \sum_{i=0}^{3} \alpha_{i+1} x^i + \alpha_{i+5} x^i y \in RQ_8$*, 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:

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

in A_1' *and* A_4' *respectively. This results in a composite matrix over* R *of the following form:*

$$\Omega(v) = \left(\begin{array}{cc|cc} X_1 & Y_1 & \multicolumn{2}{c}{\multirow{2}{*}{X_2}} \\ Y_1 & X_1 & & \\ \hline \multicolumn{2}{c|}{\multirow{2}{*}{X_3}} & X_4 & Y_4 \\ & & Y_4 & X_4 \end{array} \right) = \left(\begin{array}{cccc|cccc}
\alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 \\
\alpha_2 & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_8 & \alpha_5 & \alpha_6 & \alpha_7 \\
\alpha_3 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_7 & \alpha_8 & \alpha_5 & \alpha_6 \\
\alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_5 \\
\hline
\alpha_7 & \alpha_6 & \alpha_5 & \alpha_8 & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_2 \\
\alpha_8 & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_3 \\
\alpha_5 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_4 \\
\alpha_6 & \alpha_5 & \alpha_8 & \alpha_7 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_1
\end{array} \right).$$

If we let $v = x^3 + xy + x^2y + x^3y \in \mathbb{F}_2Q_8$*, where* $\langle x, y\rangle \cong Q_8$*, then*

$$\mathcal{C}(v) = \langle\Omega(v)\rangle = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

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

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

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'.

We now extend two results from [23]; 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 5.1.1. *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* $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathcal{C}(v)$*. 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 $v_j^* = \sum_{i=1}^{n} \alpha_{g_{j_i}g_i} g_{j_i} g_i$ in RG, where $\alpha_{g_{j_i}g_i} \in R$, $g_i, g_{j_i} \in G$ and j is the jth row of the matrix $\Omega(v)$. We also know that some of the elements g_{j_i} equal to $\phi_l(h_i)$ for some map ϕ_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. □

Corollary 5.1.2. *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 [23], 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 ϕ_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.

An open problem in the classical coding theory is to establish the existence or non-existence of a binary self-dual code with parameters $[72, 36, 16]$. So far, in the existing literature, no such code was constructed or was proved not to exist. Researchers have however studied the algebraic structure of some of the constructions to show that from certain generator matrices over certain alphabets (finite fields and rings), the binary self-dual code with parameters $[72, 36, 16]$ can not be obtained. Please see [23] for more details. We now also show that one can not produce such code with our technique.

Corollary 5.1.3. *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 [23] 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 [23]. 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 $\mathcal{R}(\mathcal{C}) = \{w \mid vw = 0, \ \forall v \in I\}$. It is immediate that $\mathcal{R}(I)$ is an ideal of RG.

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

$$[(\alpha_{g_{j_i}g_1}, \alpha_{g_{j_i}g_2}, \ldots, \alpha_{g_{j_i}g_n}), (w_1, w_2, \ldots, w_n)] = 0, \ \forall j, \tag{5.2}$$

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

$$\sum_{i=0}^{n} \alpha_{g_{j_i}g_i} w_i = 0, \ \forall j. \tag{5.3}$$

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

$$b_{g_i} = w_{g_i^{-1}}. \tag{5.4}$$

Then

$$\sum_{i=1}^{n} \alpha_{g_{j_i}g_i} w_i = 0 \implies \sum_{i=1}^{n} \alpha_{g_{j_i}g_i} b_{g_i^{-1}} = 0. \tag{5.5}$$

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

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

Theorem 5.1.4. *Let $\mathcal{C} = \mathcal{C}(v)$ be a code in RG formed from the vector $v \in RG$. Then $\Psi^{-1}(\mathcal{C}^{\perp})$ is an ideal of RG.*

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

5.2 Self-Orthogonal Composite G-codes

In this section, we show that the map $\Omega : RG \to M_n(R)$ is an injective ring homomorphism, we show when our construction $\mathcal{C} = \langle \Omega(v) \rangle$ 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

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

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 ϕ_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 5.2.1. *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 $\Omega : RG \to M_n(R)$ is an injective ring homomorphism.*

Proof. We need to show that the map Ω 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 $\Omega : RG \to M_n(R)$ as follows. Suppose $v = \sum_{i=1}^{n} \alpha_{g_i} g_i$. Then

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

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 ϕ_l have been defined to form the composite matrix $\Omega(v)$. This mapping is clearly injective. We now show that Ω is additive and multiplicative. Let $w = \sum_{i=1}^{n} \beta_{g_i} g_i$ then,

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

$$= \begin{pmatrix} \alpha_{g_{1_1}^{-1}g_1} & \alpha_{g_{1_2}^{-1}g_2} & \alpha_{g_{1_3}^{-1}g_3} & \cdots & \alpha_{g_{1_n}^{-1}g_n} \\ \alpha_{g_{2_1}^{-1}g_1} & \alpha_{g_{2_2}^{-1}g_2} & \alpha_{g_{2_3}^{-1}g_3} & \cdots & \alpha_{g_{2_n}^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_{n_1}^{-1}g_1} & \alpha_{g_{n_2}^{-1}g_2} & \alpha_{g_{n_3}^{-1}g_3} & \cdots & \alpha_{g_{n_n}^{-1}g_n} \end{pmatrix} + \begin{pmatrix} \beta_{g_{1_1}^{-1}g_1} & \beta_{g_{1_2}^{-1}g_2} & \beta_{g_{1_3}^{-1}g_3} & \cdots & \beta_{g_{1_n}^{-1}g_n} \\ \beta_{g_{2_1}^{-1}g_1} & \beta_{g_{2_2}^{-1}g_2} & \beta_{g_{2_3}^{-1}g_3} & \cdots & \alpha_{g_{2_n}^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta_{g_{n_1}^{-1}g_1} & \beta_{g_{n_2}^{-1}g_2} & \beta_{g_{n_3}^{-1}g_3} & \cdots & \beta_{g_{n_n}^{-1}g_n} \end{pmatrix} =$$

$$= \Omega(v) + \Omega(w).$$

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

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

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 5.2.2. *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 $\alpha_{(g_i^{-1}g_{j_i})^{-1}} = \alpha_{g_{j_i}^{-1}g_i}$ which is the ji-th element of $\Omega(v)$. □

Lemma 5.2.3. *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 $\mathcal{C}_v$ is a self-orthogonal code.*

Proof. If $v = v^T$ then $\Omega(v)^T = \Omega(v^T)$ by Lemma 5.2.2. 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 5.2.4. *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 $|\mathcal{C}_v| = |R^{\frac{n}{2}}|$ then C_v is a self-dual code.*

Proof. By Lemma 5.2.3 the code C_v is self-orthogonal and since $|C_v| = |R^{\frac{n}{2}}|$, we have that $\mathcal{C}_v$ is self-dual. □

5.3 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. We show when such generator matrices produce self-dual codes. 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 5.3.1. *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 $A = circ(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7, \alpha_8)$, $B = circ(\alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12}, \alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha_{16})$ 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	$\lvert Aut(\mathcal{C}_i)\rvert$
$\mathcal{C}_1$	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 5.3.2. *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 $v = \sum_{i=0}^{7}\sum_{j=0}^{1}\alpha_{1+i+8j}x^iy^j \in \mathbb{F}_2D_{16}$. Also let $H_1 = \langle a, b \mid a^2 = b^2 = 1, ab = ba\rangle \cong C_4 \times C_2$ and $H_2 = \langle c, d \mid c^4 = d^2 = c^d = c^{-1}\rangle \cong D_8$. Now we define the composite matrix as:*

$$\Omega(v) = \begin{pmatrix} A'_1 & A'_2 \\ A'_3 & A'_4 \end{pmatrix},$$

where

$$A'_1 = \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_1((h_1)_2^{-1}(h_1)_5)} & \alpha_{\phi_1((h_1)_2^{-1}(h_1)_6)} & \alpha_{\phi_1((h_1)_2^{-1}(h_1)_7)} & \alpha_{\phi_1((h_1)_2^{-1}(h_1)_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_{\phi_1((h_1)_3^{-1}(h_1)_5)} & \alpha_{\phi_1((h_1)_3^{-1}(h_1)_6)} & \alpha_{\phi_1((h_1)_3^{-1}(h_1)_7)} & \alpha_{\phi_1((h_1)_3^{-1}(h_1)_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_{\phi_1((h_1)_4^{-1}(h_1)_5)} & \alpha_{\phi_1((h_1)_4^{-1}(h_1)_6)} & \alpha_{\phi_1((h_1)_4^{-1}(h_1)_7)} & \alpha_{\phi_1((h_1)_4^{-1}(h_1)_8)} \\
\alpha_{\phi_1((h_1)_5^{-1}(h_1)_1)} & \alpha_{\phi_1((h_1)_5^{-1}(h_1)_2)} & \alpha_{\phi_1((h_1)_5^{-1}(h_1)_3)} & \alpha_{\phi_1((h_1)_5^{-1}(h_1)_4)} & \alpha_{\phi_1((h_1)_5^{-1}(h_1)_5)} & \alpha_{\phi_1((h_1)_5^{-1}(h_1)_6)} & \alpha_{\phi_1((h_1)_5^{-1}(h_1)_7)} & \alpha_{\phi_1((h_1)_5^{-1}(h_1)_8)} \\
\alpha_{\phi_1((h_1)_6^{-1}(h_1)_1)} & \alpha_{\phi_1((h_1)_6^{-1}(h_1)_2)} & \alpha_{\phi_1((h_1)_6^{-1}(h_1)_3)} & \alpha_{\phi_1((h_1)_6^{-1}(h_1)_4)} & \alpha_{\phi_1((h_1)_6^{-1}(h_1)_5)} & \alpha_{\phi_1((h_1)_6^{-1}(h_1)_6)} & \alpha_{\phi_1((h_1)_6^{-1}(h_1)_7)} & \alpha_{\phi_1((h_1)_6^{-1}(h_1)_8)} \\
\alpha_{\phi_1((h_1)_7^{-1}(h_1)_1)} & \alpha_{\phi_1((h_1)_7^{-1}(h_1)_2)} & \alpha_{\phi_1((h_1)_7^{-1}(h_1)_3)} & \alpha_{\phi_1((h_1)_7^{-1}(h_1)_4)} & \alpha_{\phi_1((h_1)_7^{-1}(h_1)_5)} & \alpha_{\phi_1((h_1)_7^{-1}(h_1)_6)} & \alpha_{\phi_1((h_1)_7^{-1}(h_1)_7)} & \alpha_{\phi_1((h_1)_7^{-1}(h_1)_8)} \\
\alpha_{\phi_1((h_1)_8^{-1}(h_1)_1)} & \alpha_{\phi_1((h_1)_8^{-1}(h_1)_2)} & \alpha_{\phi_1((h_1)_8^{-1}(h_1)_3)} & \alpha_{\phi_1((h_1)_8^{-1}(h_1)_4)} & \alpha_{\phi_1((h_1)_8^{-1}(h_1)_5)} & \alpha_{\phi_1((h_1)_8^{-1}(h_1)_6)} & \alpha_{\phi_1((h_1)_8^{-1}(h_1)_7)} & \alpha_{\phi_1((h_1)_8^{-1}(h_1)_8)}
\end{pmatrix},$$

$$A'_2 = \begin{pmatrix}
\alpha_{g_1^{-1}g_9} & \alpha_{g_1^{-1}g_{10}} & \alpha_{g_1^{-1}g_{11}} & \alpha_{g_1^{-1}g_{12}} & \alpha_{g_1^{-1}g_{13}} & \alpha_{g_1^{-1}g_{14}} & \alpha_{g_1^{-1}g_{15}} & \alpha_{g_1^{-1}g_{16}} \\
\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_2((h_1)_2^{-1}(h_1)_5)} & \alpha_{\phi_2((h_1)_2^{-1}(h_1)_6)} & \alpha_{\phi_2((h_1)_2^{-1}(h_1)_7)} & \alpha_{\phi_2((h_1)_2^{-1}(h_1)_8)} \\
\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_2((h_1)_3^{-1}(h_1)_5)} & \alpha_{\phi_2((h_1)_3^{-1}(h_1)_6)} & \alpha_{\phi_2((h_1)_3^{-1}(h_1)_7)} & \alpha_{\phi_2((h_1)_3^{-1}(h_1)_8)} \\
\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_{\phi_2((h_1)_4^{-1}(h_1)_5)} & \alpha_{\phi_2((h_1)_4^{-1}(h_1)_6)} & \alpha_{\phi_2((h_1)_4^{-1}(h_1)_7)} & \alpha_{\phi_2((h_1)_4^{-1}(h_1)_8)} \\
\alpha_{\phi_2((h_1)_5^{-1}(h_1)_1)} & \alpha_{\phi_2((h_1)_5^{-1}(h_1)_2)} & \alpha_{\phi_2((h_1)_5^{-1}(h_1)_3)} & \alpha_{\phi_2((h_1)_5^{-1}(h_1)_4)} & \alpha_{\phi_2((h_1)_5^{-1}(h_1)_5)} & \alpha_{\phi_2((h_1)_5^{-1}(h_1)_6)} & \alpha_{\phi_2((h_1)_5^{-1}(h_1)_7)} & \alpha_{\phi_2((h_1)_5^{-1}(h_1)_8)} \\
\alpha_{\phi_2((h_1)_6^{-1}(h_1)_1)} & \alpha_{\phi_2((h_1)_6^{-1}(h_1)_2)} & \alpha_{\phi_2((h_1)_6^{-1}(h_1)_3)} & \alpha_{\phi_2((h_1)_6^{-1}(h_1)_4)} & \alpha_{\phi_2((h_1)_6^{-1}(h_1)_5)} & \alpha_{\phi_2((h_1)_6^{-1}(h_1)_6)} & \alpha_{\phi_2((h_1)_6^{-1}(h_1)_7)} & \alpha_{\phi_2((h_1)_6^{-1}(h_1)_8)} \\
\alpha_{\phi_2((h_1)_7^{-1}(h_1)_1)} & \alpha_{\phi_2((h_1)_7^{-1}(h_1)_2)} & \alpha_{\phi_2((h_1)_7^{-1}(h_1)_3)} & \alpha_{\phi_2((h_1)_7^{-1}(h_1)_4)} & \alpha_{\phi_2((h_1)_7^{-1}(h_1)_5)} & \alpha_{\phi_2((h_1)_7^{-1}(h_1)_6)} & \alpha_{\phi_2((h_1)_7^{-1}(h_1)_7)} & \alpha_{\phi_2((h_1)_7^{-1}(h_1)_8)} \\
\alpha_{\phi_2((h_1)_8^{-1}(h_1)_1)} & \alpha_{\phi_2((h_1)_8^{-1}(h_1)_2)} & \alpha_{\phi_2((h_1)_8^{-1}(h_1)_3)} & \alpha_{\phi_2((h_1)_8^{-1}(h_1)_4)} & \alpha_{\phi_2((h_1)_8^{-1}(h_1)_5)} & \alpha_{\phi_2((h_1)_8^{-1}(h_1)_6)} & \alpha_{\phi_2((h_1)_8^{-1}(h_1)_7)} & \alpha_{\phi_2((h_1)_8^{-1}(h_1)_8)}
\end{pmatrix},$$

$$A'_3 = \begin{pmatrix}
\alpha_{g_9^{-1}g_1} & \alpha_{g_9^{-1}g_2} & \alpha_{g_9^{-1}g_3} & \alpha_{g_9^{-1}g_4} & \alpha_{g_9^{-1}g_5} & \alpha_{g_9^{-1}g_6} & \alpha_{g_9^{-1}g_7} & \alpha_{g_9^{-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_3((h_2)_2^{-1}(h_2)_5)} & \alpha_{\phi_3((h_2)_2^{-1}(h_2)_6)} & \alpha_{\phi_3((h_1)_2^{-1}(h_2)_7)} & \alpha_{\phi_3((h_2)_2^{-1}(h_2)_8)} \\
\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_3((h_2)_3^{-1}(h_2)_5)} & \alpha_{\phi_3((h_2)_3^{-1}(h_2)_6)} & \alpha_{\phi_3((h_2)_3^{-1}(h_2)_7)} & \alpha_{\phi_3((h_2)_3^{-1}(h_2)_8)} \\
\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_3((h_2)_4^{-1}(h_2)_5)} & \alpha_{\phi_3((h_2)_4^{-1}(h_2)_6)} & \alpha_{\phi_3((h_2)_4^{-1}(h_2)_7)} & \alpha_{\phi_3((h_2)_4^{-1}(h_2)_8)} \\
\alpha_{\phi_3((h_2)_5^{-1}(h_2)_1)} & \alpha_{\phi_3((h_2)_5^{-1}(h_2)_2)} & \alpha_{\phi_3((h_2)_5^{-1}(h_2)_3)} & \alpha_{\phi_3((h_2)_5^{-1}(h_2)_4)} & \alpha_{\phi_3((h_2)_5^{-1}(h_2)_5)} & \alpha_{\phi_3((h_2)_5^{-1}(h_2)_6)} & \alpha_{\phi_3((h_2)_5^{-1}(h_2)_7)} & \alpha_{\phi_3((h_2)_5^{-1}(h_2)_8)} \\
\alpha_{\phi_3((h_2)_6^{-1}(h_2)_1)} & \alpha_{\phi_3((h_2)_6^{-1}(h_2)_2)} & \alpha_{\phi_3((h_2)_6^{-1}(h_2)_3)} & \alpha_{\phi_3((h_2)_6^{-1}(h_2)_4)} & \alpha_{\phi_3((h_2)_6^{-1}(h_2)_5)} & \alpha_{\phi_3((h_2)_6^{-1}(h_2)_6)} & \alpha_{\phi_3((h_2)_6^{-1}(h_2)_7)} & \alpha_{\phi_3((h_2)_6^{-1}(h_2)_8)} \\
\alpha_{\phi_3((h_2)_7^{-1}(h_2)_1)} & \alpha_{\phi_3((h_2)_7^{-1}(h_2)_2)} & \alpha_{\phi_3((h_2)_7^{-1}(h_2)_3)} & \alpha_{\phi_3((h_2)_7^{-1}(h_2)_4)} & \alpha_{\phi_3((h_2)_7^{-1}(h_2)_5)} & \alpha_{\phi_3((h_2)_7^{-1}(h_2)_6)} & \alpha_{\phi_3((h_2)_7^{-1}(h_2)_7)} & \alpha_{\phi_3((h_2)_7^{-1}(h_2)_8)} \\
\alpha_{\phi_3((h_2)_8^{-1}(h_2)_1)} & \alpha_{\phi_3((h_2)_8^{-1}(h_2)_2)} & \alpha_{\phi_3((h_2)_8^{-1}(h_2)_3)} & \alpha_{\phi_3((h_2)_8^{-1}(h_2)_4)} & \alpha_{\phi_3((h_2)_8^{-1}(h_2)_5)} & \alpha_{\phi_3((h_2)_8^{-1}(h_2)_6)} & \alpha_{\phi_3((h_2)_8^{-1}(h_2)_7)} & \alpha_{\phi_3((h_2)_8^{-1}(h_2)_8)}
\end{pmatrix},$$

$$A'_4 = \begin{pmatrix}
\alpha_{g_9^{-1}g_9} & \alpha_{g_9^{-1}g_{10}} & \alpha_{g_9^{-1}g_{11}} & \alpha_{g_9^{-1}g_{12}} & \alpha_{g_9^{-1}g_{13}} & \alpha_{g_9^{-1}g_{14}} & \alpha_{g_9^{-1}g_{15}} & \alpha_{g_9^{-1}g_{16}} \\
\alpha_{\phi_4((h_2)_2^{-1}(h_2)_1)} & \alpha_{\phi_4((h_2)_2^{-1}(h_2)_2)} & \alpha_{\phi_4((h_2)_2^{-1}(h_2)_3)} & \alpha_{\phi_4((h_2)_2^{-1}(h_2)_4)} & \alpha_{\phi_4((h_2)_2^{-1}(h_2)_5)} & \alpha_{\phi_4((h_2)_2^{-1}(h_2)_6)} & \alpha_{\phi_4((h_1)_2^{-1}(h_2)_7)} & \alpha_{\phi_4((h_2)_2^{-1}(h_2)_8)} \\
\alpha_{\phi_4((h_2)_3^{-1}(h_2)_1)} & \alpha_{\phi_4((h_2)_3^{-1}(h_2)_2)} & \alpha_{\phi_4((h_2)_3^{-1}(h_2)_3)} & \alpha_{\phi_4((h_2)_3^{-1}(h_2)_4)} & \alpha_{\phi_4((h_2)_3^{-1}(h_2)_5)} & \alpha_{\phi_4((h_2)_3^{-1}(h_2)_6)} & \alpha_{\phi_4((h_2)_3^{-1}(h_2)_7)} & \alpha_{\phi_4((h_2)_3^{-1}(h_2)_8)} \\
\alpha_{\phi_4((h_2)_4^{-1}(h_2)_1)} & \alpha_{\phi_4((h_2)_4^{-1}(h_2)_2)} & \alpha_{\phi_4((h_2)_4^{-1}(h_2)_3)} & \alpha_{\phi_4((h_2)_4^{-1}(h_2)_4)} & \alpha_{\phi_4((h_2)_4^{-1}(h_2)_5)} & \alpha_{\phi_4((h_2)_4^{-1}(h_2)_6)} & \alpha_{\phi_4((h_2)_4^{-1}(h_2)_7)} & \alpha_{\phi_4((h_2)_4^{-1}(h_2)_8)} \\
\alpha_{\phi_4((h_2)_5^{-1}(h_2)_1)} & \alpha_{\phi_4((h_2)_5^{-1}(h_2)_2)} & \alpha_{\phi_4((h_2)_5^{-1}(h_2)_3)} & \alpha_{\phi_4((h_2)_5^{-1}(h_2)_4)} & \alpha_{\phi_4((h_2)_5^{-1}(h_2)_5)} & \alpha_{\phi_4((h_2)_5^{-1}(h_2)_6)} & \alpha_{\phi_4((h_2)_5^{-1}(h_2)_7)} & \alpha_{\phi_4((h_2)_5^{-1}(h_2)_8)} \\
\alpha_{\phi_4((h_2)_6^{-1}(h_2)_1)} & \alpha_{\phi_4((h_2)_6^{-1}(h_2)_2)} & \alpha_{\phi_4((h_2)_6^{-1}(h_2)_3)} & \alpha_{\phi_4((h_2)_6^{-1}(h_2)_4)} & \alpha_{\phi_4((h_2)_6^{-1}(h_2)_5)} & \alpha_{\phi_4((h_2)_6^{-1}(h_2)_6)} & \alpha_{\phi_4((h_2)_6^{-1}(h_2)_7)} & \alpha_{\phi_4((h_2)_6^{-1}(h_2)_8)} \\
\alpha_{\phi_4((h_2)_7^{-1}(h_2)_1)} & \alpha_{\phi_4((h_2)_7^{-1}(h_2)_2)} & \alpha_{\phi_4((h_2)_7^{-1}(h_2)_3)} & \alpha_{\phi_4((h_2)_7^{-1}(h_2)_4)} & \alpha_{\phi_4((h_2)_7^{-1}(h_2)_5)} & \alpha_{\phi_4((h_2)_7^{-1}(h_2)_6)} & \alpha_{\phi_4((h_2)_7^{-1}(h_2)_7)} & \alpha_{\phi_4((h_2)_7^{-1}(h_2)_8)} \\
\alpha_{\phi_4((h_2)_8^{-1}(h_2)_1)} & \alpha_{\phi_4((h_2)_8^{-1}(h_2)_2)} & \alpha_{\phi_4((h_2)_8^{-1}(h_2)_3)} & \alpha_{\phi_4((h_2)_8^{-1}(h_2)_4)} & \alpha_{\phi_4((h_2)_8^{-1}(h_2)_5)} & \alpha_{\phi_4((h_2)_8^{-1}(h_2)_6)} & \alpha_{\phi_4((h_2)_8^{-1}(h_2)_7)} & \alpha_{\phi_4((h_2)_8^{-1}(h_2)_8)}
\end{pmatrix},$$

and where:

$$\phi_1 : \begin{array}{c} (h_1)_i \xrightarrow{\phi_1} g_1^{-1}g_i \\ \text{for } i = \{1, 2, \ldots, 8\} \end{array} \qquad \phi_2 : \begin{array}{c} (h_1)_i \xrightarrow{\phi_2} g_1^{-1}g_i \\ \text{for when } i = \{9, 10, \ldots, 16\} \end{array}$$

$$\phi_3 : \begin{array}{c} (h_2)_i \xrightarrow{\phi_3} g_9^{-1}g_i \\ \text{for } i = \{1, 2, \ldots, 8\} \end{array} \qquad \phi_4 : \begin{array}{c} (h_2)_i \xrightarrow{\phi_4} g_9^{-1}g_i \\ \text{for when } i = \{9, 10, \ldots, 16\}. \end{array}$$

This results in a composite matrix of the following form:

$$\Omega(v) = \left(\begin{array}{cc|cc} A_1 & B_1 & A_2 & B_2 \\ B_1 & A_1 & B_2 & A_2 \\ \hline A_3 & B_3 & A_4 & B_4 \\ B_3^T & A_3^T & B_4^T & A_4^T \end{array} \right),$$

where

$$\begin{aligned} A_1 &= circ(\alpha_1, \alpha_2, \alpha_3, \alpha_4), \\ B_1 &= circ(\alpha_5, \alpha_6, \alpha_7, \alpha_8), \\ A_2 &= circ(\alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12}), \\ B_2 &= circ(\alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha_{16}), \\ A_3 &= circ(\alpha_9, \alpha_{16}, \alpha_{15}, \alpha_{14}), \\ B_3 &= circ(\alpha_{13}, \alpha_{12}, \alpha_{11}, \alpha_{10}), \\ A_4 &= circ(\alpha_1, \alpha_8, \alpha_7, \alpha_6), \\ B_4 &= circ(\alpha_5, \alpha_4, \alpha_3, \alpha_2) \end{aligned}$$

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.*

$\mathcal{C}_i$	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}	$\lvert Aut(\mathcal{C}_i)\rvert$
$\mathcal{C}_1$	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 5.3.2 is different from the order of automorphism of codes obtained in Example 5.3.1. 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 5.3.1. *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 note that the connection defined in Equation (1.19) extends to the map Ω. We also saw earlier in the work that $\Omega(v^T) = \Omega(v)^T$. Now using Theorem 5.3.1, the fact that Ω is a ring homomorphism, and the fact that $\Omega(v) = -I_n$ if and only if $v = -1$, we get the following corollary.

Corollary 5.3.2. *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 $vv^* = -1$. 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 5.3.3. *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 $vv^* = 1$, namely v is a unitary unit in RG.*

5.3.1 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 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 Theorem 9 to obtain codes of length 68. We next apply the i^{th}-range neighbour method described in Definition 33 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 $\gamma = 7, 8, 9$.

The Generator Matrix

We now define the generator matrix of the form $[I_n \mid \Omega(v)]$ which we then employ to search for self-dual codes over the ring $\mathbb{F}_4 + u\mathbb{F}_4$. Of course, I_n 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 $v = \alpha_1 + \alpha_x x + \alpha_{x^2} x^2 + \alpha_{x^3} x^3 + \alpha_y y + \alpha_{xy} xy + \alpha_{x^2y} x^2 y + \alpha_{x^3y} x^3 y \in RD_8$, 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:

$$\Omega(v) = \begin{pmatrix} A_1' & A_2' \\ A_3' & A_4' \end{pmatrix} =$$

$$\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_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)} \\
\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_{\phi_3((h_1)_2^{-1}(h_1)_1)} & \alpha_{\phi_3((h_1)_2^{-1}(h_1)_2)} & \alpha_{\phi_3((h_1)_2^{-1}(h_1)_3)} & \alpha_{\phi_3((h_1)_2^{-1}(h_1)_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_1)_3^{-1}(h_1)_1)} & \alpha_{\phi_3((h_1)_3^{-1}(h_1)_2)} & \alpha_{\phi_3(h_1)_3^{-1}(h_1)_3)} & \alpha_{\phi_3((h_1)_3^{-1}(h_1)_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_1)_4^{-1}(h_1)_1)} & \alpha_{\phi_3((h_1)_4^{-1}(h_1)_2)} & \alpha_{\phi_3(h_1)_4^{-1}(h_1)_3)} & \alpha_{\phi_3((h_1)_4^{-1}(h_1)_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:

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

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

in A_1', A_2', A_3' and A_4'. This results in a composite matrix over R of the following form:

$$\Omega(v) = \left(\begin{array}{cccc|cccc}
\alpha_1 & \alpha_x & \alpha_{x^2} & \alpha_{x^3} & \alpha_y & \alpha_{xy} & \alpha_{x^2y} & \alpha_{x^3y} \\
\alpha_x & \alpha_1 & \alpha_{x^3} & \alpha_{x^2} & \alpha_{xy} & \alpha_y & \alpha_{x^3y} & \alpha_{x^2y} \\
\alpha_{x^3} & \alpha_{x^2} & \alpha_1 & \alpha_x & \alpha_{x^2y} & \alpha_{x^3y} & \alpha_y & \alpha_{xy} \\
\alpha_{x^2} & \alpha_{x^3} & \alpha_x & \alpha_1 & \alpha_{x^3y} & \alpha_{x^2y} & \alpha_{xy} & \alpha_y \\
\hline
\alpha_y & \alpha_{x^3y} & \alpha_{x^2y} & \alpha_{xy} & \alpha_1 & \alpha_{x^3} & \alpha_{x^2} & \alpha_x \\
\alpha_{x^3y} & \alpha_y & \alpha_{xy} & \alpha_{x^2y} & \alpha_{x^3} & \alpha_1 & \alpha_x & \alpha_{x^2} \\
\alpha_{x^2y} & \alpha_{xy} & \alpha_y & \alpha_{x^3y} & \alpha_{x^2} & \alpha_x & \alpha_1 & \alpha_{x^3} \\
\alpha_{xy} & \alpha_{x^2y} & \alpha_{x^3y} & \alpha_y & \alpha_x & \alpha_{x^2} & \alpha_{x^3} & \alpha_1
\end{array}\right). \tag{5.6}$$

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

$$[I_n \mid \Omega(v)], \tag{5.7}$$

where $\Omega(v)$ is the composite matrix defined in (5.6).

Computational Results

We now employ the generator matrix defined in Equation (5.7) 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. Since the matrix $\Omega(v)$ in Equation (5.7) is fully defined by the first row, we only list the elements that appear in this row. This code is listed in Table 5.1. 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* ([4]).

Table 5.1: Type I Codes of length 64 and their β values

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

We now apply Theorem 9 to the $\psi_{\mathbb{F}_4+u\mathbb{F}_4}$- image of the code in Table 5.1. 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 5.2, where $1+u$ in $\mathbb{F}_2 + u\mathbb{F}_2$, is denoted by 3.

Table 5.2: Type I Codes of length 68 from Theorem 9

$\mathcal{C}_{68,i}$	$\mathcal{C}_i$	c	X	γ	β
$\mathcal{C}_{68,1}$	$\mathcal{C}_1$	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

The order of the automorphism group of the code in Table 5.2 is 2. We note that the code from Table 5.2 has parameters that are not new in the literature.

We now apply the i^{th} range neighbour formula to the code obtained in Table 5.2. We set the first 34 entries of x to be 0, the rest of the vectors are listed in Tables 5.3 and 5.4.

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 i^{th} range formula, we obtain:

Table 5.3: i^{th} neighbour of $\mathcal{N}_{(0)}$

i	$\mathcal{N}_{(i+1)}$	x_i	γ	β
0	$\mathcal{N}_{(1)}$	(1111011010011101111111100100111110)	4	101
1	$\mathcal{N}_{(2)}$	(0110100100111101111011111110111011)	6	145
2	$\mathcal{N}_{(3)}$	(0000100000010000011101110110000101)	7	152
3	$\mathcal{N}_{(4)}$	(1111111100000010000111001100101011)	**7**	**143**
4	$\mathcal{N}_{(5)}$	(0110010010100110110111101011111111)	8	162
5	$\mathcal{N}_{(6)}$	(1100001011011111001111110010001011)	9	174
6	$\mathcal{N}_{(7)}$	(1110010010100011111100101110001100)	**9**	**167**
7	$\mathcal{N}_{(8)}$	(0011000000000110110101001101100000)	**9**	**159**
8	$\mathcal{N}_{(9)}$	(1001101110001110110000111101000011)	**9**	**158**
9	$\mathcal{N}_{(10)}$	(1001011111100101110001001011110110)	**9**	**157**
10	$\mathcal{N}_{(11)}$	(1010101101101101110111011111111010)	**9**	**152**
11	$\mathcal{N}_{(12)}$	(1111010110110000110111011010101010)	**7**	**131**
12	$\mathcal{N}_{(13)}$	(1000011111111011110110001010110010)	**6**	**117**

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 Tables 5.3 and 5.4 have an automorphism group of order 1.

Table 5.4: New codes of length 68 as neighbours

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
7		(0001000001011110101000001110100011O)	**7**	**141**	7		(0100101001111001101010101010101110)	**8**	**150**
7		(0111001010000000010001100000101110O)	**8**	**151**	7		(1001100101100110101111100011101101)	**8**	**152**
7		(0011100111101011010101111011100100)	**9**	**164**	7		(1000000010011000001010001011010011)	**9**	**165**
7		(0010010111100000100111110000000000)	**9**	**166**	7		(0010101001010010101010100000000011)	**9**	**168**
7		(1000101001011010000100100100010010)	**9**	**170**	7		(0110110001000000000110000010011110)	**9**	**172**

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
8		(0111100101101011111001111110111101)	**7**	**134**	8		(1000001110101000000101110110100010)	**7**	**135**
8		(1111010110000000011100110100100000O)	**7**	**136**	8		(1111000111011000110111001101111110)	**7**	**137**
8		(00100000011001100110010010001100001)	**7**	**138**	8		(1111001001110111001001100101001100)	**7**	**139**
8		(1011011001100110111011100100011000)	**8**	**144**	8		(1111101110010110001101111111010010)	**8**	**147**
8		(0011000110101010001011010101100101)	**8**	**148**	8		(0110110000000110010110011110100110)	**8**	**149**
8		(0001101100111000101110011001001001)	**9**	**160**	8		(1000001000111101010110000101010001)	**9**	**161**
8		(1110100010110010110000010010000101)	**9**	**162**	8		(0100011010001111001111101001011111)	**9**	**163**

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
10		(1101100111000110001101001101111000)	**7**	**132**	10		(1111000110101101101011011011000011)	**8**	**143**
10		(1110110011011110001010110001101011)	**8**	**145**	10		(0010111101110011010001011100111110)	**8**	**146**
10		(1011010011010100010100010010111010)	**9**	**156**					

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
11		(0101000101100110011001011000111100)	**8**	**139**	11		(1011111100100001110111000101111100)	**8**	**140**
11		(1100011001000111000000110111010110)	**8**	**141**	11		(1101111110110100001101111111011101)	**9**	**151**
11		(0001100111110011010110111001111010)	**9**	**154**	11		(0100100111101001001010101111000001)	**9**	**155**

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
12		(1100011100101100111101111001101100)	**6**	**121**	12		(1111100111100011111001011110101111)	**6**	**123**
12		(0001101000001011101010000001100001)	**6**	**124**	12				

$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β	$\mathcal{N}_{(i)}$	$\mathcal{M}_i$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
13		(0101110011001101000001001000001000)	**5**	**110**	13		(1011011100110111011001011010101001)	**6**	**120**
13		(1000111010010011011000110000101011)	**6**	**122**	13				

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.

Chapter 6

Composite Constructions of Self-Dual Codes from Group Rings and New Extremal Self-Dual Binary Codes of length 68

In this chapter, we employ our extended isomorphism from Chapter 4 to construct binary self-dual $[68, 34, 12]$ codes with parameters in their weight enumerators that were not known in the literature before. In particular, we define two composite constructions with the use of groups of orders 8 and 4 and use these composite matrices to form two generator matrices. We next give the necessary conditions that each generator matrix has to meet in order to produce a self-dual code over a finite commutative Frobenius ring of characteristic 2. We finally, together with the generator matrices, the extension and neighbour methods search for binary self-dual codes with parameters $[68, 34, 12]$. As a result, we obtain 13 such codes with parameters in their weight enumerators that are new. Our approach here is similar to the one given in the previous chapter, but this time, we consider more groups of orders 8 and 4 to define the composite matrices and then the generator matrices with. The technique of employing the composite matrices defined in Chapter 4 to search for binary self-dual codes with is very recent and not much literature exists where this technique is employed. One can see [20] where this idea, with groups of order 16 and 8, is used to construct new extremal binary self-dual codes of length 68 with. We believe that the composite matrices defined earlier in this work will find many applications in coding theory and in particular in constructing new binary self-dual codes of different lengths. This chapter is joint work and the results are published in [19].

6.1 Generator Matrices

In this section, we define two composite matrices using the matrix construction presented in Chapter 4. We then use these composite matrices to form two generator matrices with. We next show under what conditions the generator matrices produce self-dual codes over a finite commutative Frobenius ring.

Let $G = \langle x \mid x^8 = 1 \rangle \cong C_8$. Let $v_1 = \sum_{i=0}^{3} \sum_{j=0}^{1} \alpha_{i+4j+1} x^{2i+j} \in RC_8$, 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 over R as

$$\Omega(v_1) = \begin{pmatrix} A_1' & A_2' \\ A_3' & A_4' \end{pmatrix} =$$

$$= \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_{\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)} \\
\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_{\phi_3((h_1)_2^{-1}(h_1)_1)} & \alpha_{\phi_3((h_1)_2^{-1}(h_1)_2)} & \alpha_{\phi_3((h_1)_2^{-1}(h_1)_3)} & \alpha_{\phi_3((h_1)_2^{-1}(h_1)_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_1)_3^{-1}(h_1)_1}) & \alpha_{\phi_3((h_1)_3^{-1}(h_1)_2)} & \alpha_{\phi_3((h_1)_3^{-1}(h_1)_3)} & \alpha_{\phi_3((h_1)_3^{-1}(h_1)_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_1)_4^{-1}(h_1)_1)} & \alpha_{\phi_3((h_1)_4^{-1}(h_1)_2)} & \alpha_{\phi_3((h_1)_4^{-1}(h_1)_3)} & \alpha_{\phi_3((h_1)_4^{-1}(h_1)_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:

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

$$\phi_3 : \begin{array}{c} (h_1)_i \xrightarrow{\phi_3} g_5^{-1}g_i \\ \text{for } i = \{1,2,3,4\} \end{array} \qquad \phi_4 : \begin{array}{c} (h_1)_i \xrightarrow{\phi_4} g_5^{-1}g_j \\ \text{for when } \{i=1, j=5, i=2, j=6, i=3, j=7, i=4, j=8\}. \end{array}$$

This results in a composite matrix over R of the following form:

$$\Omega(v_1) = \left(\begin{array}{cc|cc} X_1 & Y_1 & X_2 & Y_2 \\ Y_1 & X_1 & Y_2 & X_2 \\ \hline X_3 & Y_3 & X_1 & Y_1 \\ Y_3 & X_3 & Y_1 & X_1 \end{array}\right) = \left(\begin{array}{cccc|cccc}
\alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 \\
\alpha_2 & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_6 & \alpha_5 & \alpha_8 & \alpha_7 \\
\alpha_3 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_7 & \alpha_8 & \alpha_5 & \alpha_6 \\
\alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_5 \\
\hline
\alpha_8 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\
\alpha_5 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_2 & \alpha_1 & \alpha_4 & \alpha_3 \\
\alpha_6 & \alpha_7 & \alpha_8 & \alpha_5 & \alpha_3 & \alpha_4 & \alpha_1 & \alpha_2 \\
\alpha_7 & \alpha_6 & \alpha_5 & \alpha_8 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1
\end{array}\right).$$

Theorem 31. *Let R be a finite commutative Frobenius ring of characteristic 2. Then the matrix*

$$G = \Big[I_8 \;\; | \;\; \Omega(v_1) \Big] = \left[\begin{array}{c|cccc} & A_1 & B_1 & A_2 & B_2 \\ I_8 & B_1 & A_1 & B_2 & A_2 \\ & A_3 & B_3 & A_1 & B_1 \\ & B_3 & A_3 & B_1 & A_1 \end{array} \right], \tag{6.1}$$

where $A_1 = circ(\alpha_1, \alpha_2)$, $B_1 = circ(\alpha_3, \alpha_4)$, $A_2 = circ(\alpha_5, \alpha_6)$, $B_2 = circ(\alpha_7, \alpha_8)$, $A_3 = circ(\alpha_8, \alpha_5)$ and $B_3 = circ(\alpha_6, \alpha_7)$ generates a self-dual code $\mathcal{C}$ over R, if and only if the following equations hold:

$$A_1^2 + A_2^2 + B_1^2 + B_2^2 = I_2, \tag{6.2}$$

$$A_1A_2 + A_1A_3 + B_1B_2 + B_1B_3 = \mathbf{0}, \tag{6.3}$$

$$A_1B_2 + A_2B_1 + A_1B_3 + A_3B_1 = \mathbf{0}, \tag{6.4}$$

$$A_1^2 + A_3^2 + B_1^2 + B_3^2 = I_2. \tag{6.5}$$

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

$$X = \begin{bmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1 & A_1 & B_2 & A_2 \\ A_3 & B_3 & A_1 & B_1 \\ B_3 & A_3 & B_1 & A_1 \end{bmatrix},$$

we have to show that $XX^T = I_8$. Now,

$$XX^T = \begin{bmatrix} A_1 & B_1 & A_2 & B_2 \\ B_1 & A_1 & B_2 & A_2 \\ A_3 & B_3 & A_1 & B_1 \\ B_3 & A_3 & B_1 & A_1 \end{bmatrix} \begin{bmatrix} A_1 & B_1 & A_3 & B_3 \\ B_1 & A_1 & B_3 & A_3 \\ A_2 & B_2 & A_1 & B_1 \\ B_2 & A_2 & B_1 & A_1 \end{bmatrix} = \begin{bmatrix} X_1 & X_2 \\ X_2 & X_3 \end{bmatrix},$$

where

$$X_1 = \begin{bmatrix} A_1^2 + A_2^2 + B_1^2 + B_2^2 & 2A_1B_1 + 2A_2B_2 \\ 2A_1B_1 + 2A_2B_2 & A_1^2 + A_2^2 + B_1^2 + B_2^2 \end{bmatrix},$$

$$X_2 = \begin{bmatrix} A_1A_2 + A_1A_3 + B_1B_2 + B_1B_3 & A_1B_2 + A_2B_1 + A_1B_3 + A_3B_1 \\ A_1B_2 + A_2B_1 + A_1B_3 + A_3B_1 & A_1A_2 + A_1A_3 + B_1B_2 + B_1B_3 \end{bmatrix},$$

$$X_3 = \begin{bmatrix} A_1^2 + A_3^2 + B_1^2 + B_3^2 & 2A_1B_1 + 2A_3B_3 \\ 2A_1B_1 + 2A_3B_3 & A_1^2 + A_3^2 + B_1^2 + B_3^2 \end{bmatrix}.$$

This will equal to I_8 only if $A_1^2 + A_2^2 + B_1^2 + B_2^2 = I_2$, $A_1A_2 + A_1A_3 + B_1B_2 + B_1B_3 = 0$, $A_1B_2 + A_2B_1 + A_1B_3 + A_3B_1 = 0$ and $A_1^2 + A_3^2 + B_1^2 + B_3^2 = I_2$. □

Let $G = \langle x, y \mid x^4 = y^2 = x^y = x^{-1} \rangle \cong D_8$. Let $v_2 = \sum_{i=0}^{3} \alpha_{i+1} x^i + \alpha_{i+5} x^i y \in RD_8$, 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 over R as

$$\Omega(v_2) = \begin{pmatrix} A_1' & A_2' \\ A_3' & A_4' \end{pmatrix} =$$

$$= \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_{\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)} \\
\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_{\phi_3((h_1)_2^{-1}(h_1)_1)} & \alpha_{\phi_3((h_1)_2^{-1}(h_1)_2)} & \alpha_{\phi_3((h_1)_2^{-1}(h_1)_3)} & \alpha_{\phi_3((h_1)_2^{-1}(h_1)_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_1)_3^{-1}(h_1)_1}) & \alpha_{\phi_3((h_1)_3^{-1}(h_1)_2)} & \alpha_{\phi_3((h_1)_3^{-1}(h_1)_3)} & \alpha_{\phi_3((h_1)_3^{-1}(h_1)_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_1)_4^{-1}(h_1)_1)} & \alpha_{\phi_3((h_1)_4^{-1}(h_1)_2)} & \alpha_{\phi_3((h_1)_4^{-1}(h_1)_3)} & \alpha_{\phi_3((h_1)_4^{-1}(h_1)_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:

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

$$\phi_3 : \begin{array}{c} (h_1)_i \xrightarrow{\phi_3} g_5^{-1} g_i \\ \text{for } i = \{1,2,3,4\} \end{array} \qquad \phi_4 : \begin{array}{c} (h_1)_i \xrightarrow{\phi_4} g_5^{-1} g_j \\ \text{for when } \{i = 1, j = 5, i = 2, j = 6, i = 3, j = 7, i = 4, j = 8\}. \end{array}$$

This results in a composite matrix over R of the following form:

$$\Omega(v_2) = \left(\begin{array}{cc|cc} X_1 & Y_1 & X_2 & Y_2 \\ Y_1 & X_1 & Y_2 & X_2 \\ \hline X_3 & Y_3 & X_4 & Y_4 \\ Y_3 & X_3 & Y_4 & X_4 \end{array}\right) = \left(\begin{array}{cccc|cccc}
\alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 \\
\alpha_2 & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_6 & \alpha_5 & \alpha_8 & \alpha_7 \\
\alpha_3 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_7 & \alpha_8 & \alpha_5 & \alpha_6 \\
\alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_5 \\
\hline
\alpha_5 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_2 \\
\alpha_8 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_3 \\
\alpha_7 & \alpha_6 & \alpha_5 & \alpha_8 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_4 \\
\alpha_6 & \alpha_7 & \alpha_8 & \alpha_5 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_1
\end{array}\right).$$

Theorem 32. *Let R be a finite commutative Frobenius ring of characteristic 2. Then the matrix*

$$G = \Big[I_8 \quad | \quad \Omega(v_2) \Big] = \left[\begin{array}{c|cc} & A_1\ B_1 & A_2\ B_2 \\ I_8 & B_1\ A_1 & B_2\ A_2 \\ & A_3\ B_3 & A_4\ B_4 \\ & B_3\ A_3 & B_4\ A_4 \end{array}\right], \tag{6.6}$$

where $A_1 = circ(\alpha_1, \alpha_2)$, $B_1 = circ(\alpha_3, \alpha_4)$, $A_2 = circ(\alpha_5, \alpha_6)$, $B_2 = circ(\alpha_7, \alpha_8)$, $A_3 = circ(\alpha_5, \alpha_8)$, $B_3 = circ(\alpha_7, \alpha_6)$, $A_4 = circ(\alpha_1, \alpha_4)$ and $B_4 = circ(\alpha_3, \alpha_2)$ generates a self-dual code $\mathcal{C}$ over R, if and only if the following equations hold:

$$A_1^2 + A_2^2 + B_1^2 + B_2^2 = I_2, \tag{6.7}$$

$$A_1A_3 + A_2A_4 + B_1B_3 + B_2B_4 = \mathbf{0}, \tag{6.8}$$

$$A_1B_3 + A_3B_1 + A_2B_4 + A_4B_2 = \mathbf{0}, \tag{6.9}$$

$$A_3^2 + A_4^2 + B_3^2 + B_4^2 = I_2. \tag{6.10}$$

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

$$X = \begin{bmatrix} A_1 \; B_1 & A_2 \; B_2 \\ B_1 \; A_1 & B_2 \; A_2 \\ A_3 \; B_3 & A_4 \; B_4 \\ B_3 \; A_3 & B_4 \; A_4 \end{bmatrix},$$

we have to show that $XX^T = I_8$. Now,

$$XX^T = \begin{bmatrix} A_1 \; B_1 & A_2 \; B_2 \\ B_1 \; A_1 & B_2 \; A_2 \\ A_3 \; B_3 & A_4 \; B_4 \\ B_3 \; A_3 & B_4 \; A_4 \end{bmatrix} \begin{bmatrix} A_1 \; B_1 & A_3 \; B_3 \\ B_1 \; A_1 & B_3 \; A_3 \\ A_2 \; B_2 & A_4 \; B_4 \\ B_2 \; A_2 & B_4 \; A_4 \end{bmatrix} = \begin{bmatrix} X_1 & X_2 \\ X_2 & X_3 \end{bmatrix},$$

where

$$X_1 = \begin{bmatrix} A_1^2 + A_2^2 + B_1^2 + B_2^2 & 2A_1B_1 + 2A_2B_2 \\ 2A_1B_1 + 2A_2B_2 & A_1^2 + A_2^2 + B_1^2 + B_2^2 \end{bmatrix},$$

$$X_2 = \begin{bmatrix} A_1A_3 + A_2A_4 + B_1B_3 + B_2B_4 & A_1B_3 + A_3B_1 + A_2B_4 + A_4B_2 \\ A_1B_3 + A_3B_1 + A_2B_4 + A_4B_2 & A_1A_3 + A_2A_4 + B_1B_3 + B_2B_4 \end{bmatrix},$$

$$X_3 = \begin{bmatrix} A_3^2 + A_4^2 + B_3^2 + B_4^2 & 2A_3B_3 + 2A_4B_4 \\ 2A_3B_3 + 2A_4B_4 & A_3^2 + A_4^2 + B_3^2 + B_4^2 \end{bmatrix}.$$

This will equal to I_8 only if $A_1^2 + A_2^2 + B_1^2 + B_2^2 = -I_2$, $A_1A_3 + A_2A_4 + B_1B_3 + B_2B_4 = 0$, $A_1B_3 + A_3B_1 + A_2B_4 + A_4B_2 = 0$ and $A_3^2 + A_4^2 + B_3^2 + B_4^2 = -I_2$. □

We note that in the above constructions we have only used the dihedral group with 8 elements and the cyclic group of order 8. There are other possible groups of order 8 that one could consider, for example, the quaternion group of order 8, Q_8, the group $C_2 \times C_4$ or the group $C_2 \times C_2 \times C_2$.

6.2 Numerical Results

In this section, we employ Theorems 31 and 32 to search for binary self-dual codes over $\mathbb{F}_4$ of length 32. We then lift these codes over to the ring $\mathbb{F}_4 + u\mathbb{F}_4$ to obtain codes whose binary images are the self-dual codes with parameters $[64, 32, 12]$. We finally use the well-known extension and neighbour methods to search for binary self-dual codes with parameters $[68, 34, 12]$. We implement the searches using the software *MAGMA* ([4]).

6.2.1 Singly-Even Binary $[64, 32, 12]$ Self-Dual Codes as Images of $\mathbb{F}_4 + u\mathbb{F}_4$ lifts of Codes over $\mathbb{F}_4$

We first employ Theorem 31 to search for self-dual codes of length 32 over $\mathbb{F}_4$. Since the matrices A_1, B_1, A_2, B_2, A_3 and B_3 in Theorem 31 are fully defined by their first rows, we only list the elements that appear in these rows. We label these as $r_{A_1}, r_{B_1}, r_{A_2}, r_{B_2}, r_{A_3}$ and r_{B_3} respectively. We summarise the results in Table 6.1.

Table 6.1: Theorem 31 over $\mathbb{F}_4$

$\mathcal{C}_i$	r_{A_1}	r_{B_1}	r_{A_2}	r_{B_2}	r_{A_3}	r_{B_3}	$\psi_{\mathbb{F}_4}(\mathcal{C})$	$\lvert Aut(\mathcal{C}_i)\rvert$
$\mathcal{C}_1$	$(0,0)$	$(1,1)$	$(\omega,1)$	$(\omega+1,1)$	$(1,\omega)$	$(1,\omega+1)$	$[32,16,8]_{II}$	2^93^25
$\mathcal{C}_2$	$(0,\omega)$	$(1,\omega+1)$	$(0,0)$	$(\omega+1,\omega)$	$(\omega,0)$	$(0,\omega+1)$	$[32,16,8]_{II}$	$2^{15}3^25\cdot 7$
$\mathcal{C}_3$	$(0,0)$	$(1,1)$	$(0,\omega)$	$(1,\omega)$	$(\omega,0)$	$(\omega,1)$	$[32,16,6]_I$	2^83
$\mathcal{C}_4$	$(0,0)$	$(1,1)$	$(\omega,0)$	$(\omega+1,0)$	$(0,\omega)$	$(0,\omega+1)$	$[32,16,6]_I$	2^93^25
$\mathcal{C}_5$	$(0,1)$	$(\omega,\omega+1)$	$(0,1)$	(ω,ω)	$(\omega,0)$	$(1,\omega)$	$[32,16,6]_I$	2^73
$\mathcal{C}_6$	$(0,\omega)$	$(1,\omega+1)$	$(0,1)$	$(\omega+1,\omega+1)$	$(\omega+1,0)$	$(1,\omega+1)$	$[32,16,6]_I$	$2^{11}3$

We now lift the codes in Table 6.1 to $\mathbb{F}_4 + u\mathbb{F}_4$, as a result we obtain extremal binary self-dual codes of length 64 given in Table 6.2.

Table 6.2: The $\mathbb{F}_4 + u\mathbb{F}_4$-lifts of $\mathcal{C}_i$ and the β values of the binary images

code		r_{A_1}	r_{B_1}	r_{A_2}	r_{B_2}	r_{A_3}	r_{B_3}	β in $W_{64,2}$	$\lvert Aut(\mathcal{C}_i)\rvert$
I_1	$\mathcal{C}_5$	$(A,9)$	$(4,7)$	$(8,1)$	$(6,4)$	$(4,8)$	$(1,6)$	8	2^4
I_2	$\mathcal{C}_5$	$(8,1)$	$(C,5)$	$(2,9)$	(E,C)	$(C,2)$	$(9,E)$	8	2^5

We now employ Theorem 32 to search for self-dual codes of length 32 over $\mathbb{F}_4$. Since the matrices $A_1, B_1, A_2, B_2, A_3, B_3, A_4$ and B_4 in Theorem 32 are fully defined by their first rows, we only list the elements that appear in these rows. We label these as $r_{A_1}, r_{B_1}, r_{A_2}, r_{B_2}, r_{A_3}, r_{B_3}$, r_{A_4} and r_{B_4} respectively. We summarise the results in Table 6.3.

We now lift the codes in Table 6.3 to $\mathbb{F}_4 + u\mathbb{F}_4$, as a result we obtain extremal binary self-dual codes of length 64 given in Table 6.4.

Table 6.3: Theorem 32 over $\mathbb{F}_4$

$\mathcal{C}_i$	r_{A_1}	r_{B_1}	r_{A_2}	r_{B_2}	r_{A_3}	r_{B_3}	r_{A_4}	r_{B_4}	$\psi_{\mathbb{F}_4}(\mathcal{C})$	$\|Aut(\mathcal{C}_i)\|$
$\mathcal{C}_1$	$(0,0)$	$(0,\omega)$	$(\omega+1,1)$	$(\omega+1,\omega)$	$(\omega+1,\omega)$	$(\omega+1,1)$	$(0,\omega)$	$(0,0)$	$[32,16,8]_{II}$	$2^9 3^2 5$
$\mathcal{C}_2$	$(0,0)$	$(1,\omega)$	$(0,\omega)$	$(\omega+1,\omega+1)$	$(0,\omega+1)$	$(\omega+1,\omega)$	$(0,\omega)$	$(1,0)$	$[32,16,8]_{II}$	$2^5 3 \cdot 5 \cdot 31$
$\mathcal{C}_3$	$(0,1)$	$(1,\omega)$	$(1,0)$	$(\omega+1,1)$	$(1,1)$	$(\omega+1,0)$	$(0,\omega)$	$(1,1)$	$[32,16,8]_{II}$	$2^{15} 3^2 5 \cdot 7$
$\mathcal{C}_4$	$(0,\omega)$	$(\omega,\omega+1)$	$(\omega,1)$	$(\omega+1,\omega)$	(ω,ω)	$(\omega+1,1)$	$(0,\omega+1)$	(ω,ω)	$[32,16,8]_I$	$2^{12} 3 \cdot 7$
$\mathcal{C}_5$	$(0,0)$	$(0,\omega)$	$(1,0)$	$(1,\omega+1)$	$(1,\omega+1)$	$(1,0)$	$(0,\omega)$	$(0,0)$	$[32,16,6]_I$	$2^9 3^2 5$
$\mathcal{C}_6$	$(0,0)$	$(0,\omega)$	$(1,1)$	$(1,\omega)$	$(1,\omega)$	$(1,1)$	$(0,\omega)$	$(0,0)$	$[32,16,6]_I$	$2^8 3$
$\mathcal{C}_7$	$(0,0)$	$(1,\omega)$	$(1,0)$	$(\omega,1)$	$(1,1)$	$(\omega,0)$	$(0,\omega)$	$(1,0)$	$[32,16,6]_I$	2^6
$\mathcal{C}_8$	$(0,0)$	$(1,\omega)$	$(1,\omega)$	$(\omega,\omega+1)$	$(1,\omega+1)$	(ω,ω)	$(0,\omega)$	$(1,0)$	$[32,16,6]_I$	$2^3 3$
$\mathcal{C}_9$	$(0,1)$	$(1,\omega)$	$(1,\omega)$	$(\omega+1,\omega+1)$	$(1,\omega+1)$	$(\omega+1,\omega)$	$(0,\omega)$	$(1,1)$	$[32,16,6]_I$	2^5

Table 6.4: The $\mathbb{F}_4 + u\mathbb{F}_4$-lifts of $\mathcal{C}_i$ and the β values of the binary images

code		r_{A_1}	r_{B_1}	r_{A_2}	r_{B_2}	r_{A_3}	r_{B_3}	r_{A_4}	r_{B_4}	β in $W_{64,2}$	$\|Aut(\mathcal{C}_i)\|$
K_1	$\mathcal{C}_2$	$(0,2)$	$(9,4)$	$(2,4)$	$(5,F)$	$(2,F)$	$(5,4)$	$(0,4)$	$(9,2)$	0	2^5
K_2	$\mathcal{C}_3$	$(0,1)$	$(9,4)$	$(9,2)$	$(7,3)$	$(9,3)$	$(7,2)$	$(0,4)$	$(9,1)$	0	2^4
K_3	$\mathcal{C}_9$	$(0,1)$	$(9,6)$	$(1,4)$	$(7,F)$	$(1,F)$	$(7,4)$	$(0,6)$	$(9,1)$	0	2^5
K_4	$\mathcal{C}_7$	$(0,0)$	$(1,6)$	$(1,8)$	$(6,B)$	$(1,B)$	$(6,8)$	$(0,6)$	$(1,0)$	0	2^4
K_{23}	$\mathcal{C}_7$	$(0,0)$	$(9,6)$	$(1,A)$	$(4,9)$	$(1,9)$	$(4,A)$	$(0,6)$	$(9,0)$	36	2^4

6.2.2 New Extremal Binary Self-Dual Codes of Length 68 from $\mathbb{F}_2 + u\mathbb{F}_2$ Extensions and Neighbours

We now apply Theorem 9 to the $\psi_{\mathbb{F}+4+u\mathbb{F}_4}$- images of the codes in Tables 6.2 and 6.4. Without loss of generality we assume that the first 16 entries of the extension vector X (in Theorem 9) are 0, which narrows down the search field remarkably. The results are tabulated in Table 6.5, where $1+u$ in $\mathbb{F}_2 + u\mathbb{F}_2$ is denoted as 3.

Table 6.5: New codes of length 68

$\mathcal{D}$	$\mathcal{C}$	$(x_{17}, x_{18}, \ldots, x_{32})$	c	γ	β in $W_{68,2}$
$\mathcal{C}_{68,1}$	I_2	$(u,0,0,3,u,1,3,u,3,3,1,1,3,0,1,0)$	3	0	38
$\mathcal{C}_{68,2}$	K_3	$(3,1,1,3,u,u,0,u,0,0,0,3,1,1,1,3)$	1	1	38
$\mathcal{C}_{68,3}$	K_3	$(3,3,1,1,0,u,0,u,0,u,0,3,1,1,3,3)$	1	1	46
$\mathcal{C}_{68,4}$	K_2	$(u,1,u,u,1,3,3,3,u,1,1,u,u,0,3,3)$	3	2	67
$\mathcal{C}_{68,5}$	K_1	$(0,0,1,0,1,3,u,3,u,0,u,0,3,0,3,1)$	3	3	77
$\mathcal{C}_{68,6}$	K_1	$(1,1,0,3,0,u,u,u,1,1,1,0,1,3,0,3)$	3	3	78
$\mathcal{C}_{68,7}$	I_1	$(1,3,1,3,1,0,1,0,1,3,1,3,u,1,0,0)$	1	3	81
$\mathcal{C}_{68,8}$	K_{23}	$(0,u,1,1,u,3,0,1,0,1,1,3,u,1,3,u)$	3	3	179
$\mathcal{C}_{68,9}$	K_3	$(1,0,0,3,u,3,u,3,1,3,3,3,1,1,1,u)$	1	4	92
$\mathcal{C}_{68,10}$	K_3	$(u,u,3,3,1,1,1,1,3,0,3,3,1,1,0,u)$	1	4	94
$\mathcal{C}_{68,11}$	K_4	$(1,u,1,0,u,u,1,u,1,1,0,u,u,u,1,1)$	1	4	119

We now employ Definition 32 to investigate the possible neighbours of the codes in Table 6.5. Without loss of generality we assume that the first 34 entries of x are 0, the last half of x is given in the table below. As a result, we find two new codes which are listed in Table 6.6.

Table 6.6: New codes of length 68 as neighbours

$\mathcal{D}$	$\mathcal{C}$	x	γ	β
$\mathcal{C}_{68,12}$	$C_{68,11}$	(1010110101000110000001111110000011)	4	107
$\mathcal{C}_{68,13}$	$C_{68,10}$	(1011111011101111011000100111110111)	4	115

Chapter 7

Composite G-Codes over Formal Power Series Rings and Finite Chain Rings

In this chapter, we take the code construction given in Section 5.1 and study composite G-codes over formal power series rings and finite chain rings. In particular, we show that the composite G-codes over the infinite ring R_∞ are ideals in the group ring $R_\infty G$ and we show that the dual of a composite G-code is again a composite G-code in this setting. Moreover, we extend some known results on projections and lifts of G-codes over the finite chain rings and over the formal power series rings to composite G-codes. Additionally, we extend some known results on γ-adic G-codes over R_∞ to composite G-codes and study these codes over principal ideal rings. Please see [5, 17, 29, 30, 31] for some examples of work on codes over formal power series rings and finite chain rings. The work in this chapter is a generalisation of the work from [17]. Here, we show that one can construct an infinite family of composite group codes via lifts of composite group codes formal power series rings and finite chain rings. That is, we give codes in this chapter the structure of composite group codes by employing the extended isomorphism introduced earlier in this thesis, and we study projections and lifts of such codes. The work presented in this chapter is published in [56].

7.1 Composite G-codes and Ideals in the Group Ring $R_\infty G$

In this section, we show that the composite G- codes are ideals in the group ring $R_\infty G$ and that the dual of the composite G- code is also a composite G- code in this setting. These two results are a simple generalization of Theorem 3.1 and Theorem 3.2 from [17]. We use the same arguments as in [17] to prove our results.

For simplicity, we write each non-zero element in R_∞ in the form $\gamma^i a$ where $a = a_0 + a_1\gamma + \cdots + \cdots$ with $a_0 \neq 0$ and $i \geq 0$, which means that a is a unit in R_∞.

We note that if $v = \gamma^{l_{g_1}} a_{g_1} g_1 + \gamma^{l_{g_2}} a_{g_2} g_2 + \cdots + \gamma^{l_{g_n}} a_{g_n} g_n \in R_\infty G$, then each row of $\Omega(v)$ corresponds to an element in $R_\infty G$ of the following form:

$$v_j^* = \sum_{i=1}^{n} \gamma^{l_{g_{j_i} g_i}} a_{g_{j_i} g_i} g_{j_i} g_i, \tag{7.1}$$

where $\gamma^{l_{g_{j_i} g_i}} a_{g_{j_i} g_i} \in R_\infty$, $g_i, g_{j_i} \in G$ and j is the jth row of the matrix $\Omega(v)$. In other words, we can define the composite matrix $\Omega(v)$ as:

$$\Omega(v) = \begin{pmatrix} \gamma^{l_{g_{1_1} g_1}} a_{g_{1_1} g_1} & \gamma^{l_{g_{1_2} g_2}} a_{g_{1_2} g_2} & \gamma^{l_{g_{1_3} g_3}} a_{g_{1_3} g_3} & \dots & \gamma^{l_{g_{1_n} g_n}} a_{g_{1_n} g_n} \\ \gamma^{l_{g_{2_1} g_1}} a_{g_{2_1} g_1} & \gamma^{l_{g_{2_2} g_2}} a_{g_{2_2} g_2} & \gamma^{l_{g_{2_3} g_3}} a_{g_{2_3} g_3} & \dots & \gamma^{l_{g_{2_n} g_n}} a_{g_{2_n} g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \gamma^{l_{g_{n_1} g_1}} a_{g_{n_1} g_1} & \gamma^{l_{g_{n_2} g_2}} a_{g_{n_2} g_2} & \gamma^{l_{g_{n_3} g_3}} a_{g_{n_3} g_3} & \dots & \gamma^{l_{g_{n_n} g_n}} a_{g_{n_n} g_n} \end{pmatrix}, \tag{7.2}$$

where the elements g_{j_i} 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 ϕ_l map in individual blocks. Then we take the row space of the matrix $\Omega(v)$ over R_∞ to get the corresponding composite G-code, namely $\mathcal{C}(v)$.

Theorem 33. *Let R_∞ be the formal power series 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 $v \in R_\infty G$ and let $\mathcal{C}(v) = \langle \Omega(v) \rangle$ be the corresponding code in R_∞^n. Let $I(v)$ be the set of elements of $R_\infty G$ such that $\sum \gamma^{l_i} a_i g_i \in I(v)$ if and only if $(\gamma^{l_1} a_1, \gamma^{l_2} a_2, \dots, \gamma^{l_n} a_n) \in \mathcal{C}(v)$. Then $I(v)$ is a left ideal in $R_\infty G$.*

Proof. We saw above that the rows of $\Omega(v)$ consist precisely of the vectors that correspond to the elements of the form $v_j^* = \sum_{i=1}^{n} \gamma^{l_{g_{j_i} g_i}} a_{g_{j_i} g_i} g_{j_i} g_i$ in $R_\infty G$, where $\gamma^{l_{g_{j_i} g_i}} a_{g_{j_i} g_i} \in R_\infty$, $g_i, g_{j_i} \in G$ and j is the jth row of the matrix $\Omega(v)$. Let $a = \sum \gamma^{l_i} a_i g_i$ and $b = \sum \gamma^{l_j} b_j g_i$ be two elements in $I(v)$, then $a + b = \sum (\gamma^{l_i} a_i + \gamma^{l_j} b_j) g_i$, which corresponds to the sum of the corresponding elements in $\mathcal{C}(v)$. This implies that $I(v)$ is closed under addition.

Let $w_1 = \sum \gamma^{l_i} b_i g_i \in R_\infty G$. Then if w_2 corresponds to a vector in $\mathcal{C}(v)$, it is of the form $\sum (\gamma^{l_j} \alpha_j) v_j^*$. Then $w_1 w_2 = \sum \gamma^{l_i} b_i g_i \sum (\gamma^{l_j} \alpha_j) v_j^* = \sum \gamma^{l_i} b_i \gamma^{l_j} \alpha_j g_i v_j^*$ 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 $R_\infty G$. □

Next we show that the dual of a composite G-code is also a composite G-code.

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

Let $v = \gamma^{l_{g_1}} a_{g_1} g_1 + \gamma^{l_{g_2}} a_{g_2} g_2 + \cdots + \gamma^{l_{g_n}} a_{g_n} g_n \in R_\infty G$ and $\mathcal{C}(v)$ be the corresponding code. Let $\Omega : R_\infty G \to R_\infty^n$ be the canonical map that sends $\gamma^{l_{g_1}} a_{g_1} g_1 + \gamma^{l_{g_2}} a_{g_2} g_2 + \cdots + \gamma^{l_{g_n}} a_{g_n} g_n$

to $(\gamma^{l_{g_1}} a_{g_1}, \gamma^{l_{g_2}} a_{g_2}, \cdots, \gamma^{l_{g_n}} a_{g_n})$. Let I be the ideal $\Omega^{-1}(\mathcal{C})$. Let $\mathbf{w} = (w_1, w_2, \ldots, w_n) \in \mathcal{C}^{\perp}$. Then the operator of product between any row of $\Omega(v)$ and $\mathbf{w}$ is zero:

$$[(\gamma^{l_{g_{j_1}g_1}} a_{g_{j_1}g_1}, \gamma^{l_{g_{j_2}g_1}} a_{g_{j_2}g_1}, \ldots, \gamma^{l_{g_{j_n}g_1}} a_{g_{j_n}g_1}), (w_1, w_2, \ldots, w_n)] = 0, \ \forall j. \tag{7.3}$$

Which gives

$$\sum_{i=1}^{n} \gamma^{l_{g_{j_i}g_i}} a_{g_{j_i}g_i} w_i = 0, \ \forall j. \tag{7.4}$$

Let $w = \Omega^{-1}(\mathbf{w}) = \sum \gamma^{k_{g_i}} w_{g_i} g_i$ and define $\overline{\mathbf{w}} \in R_\infty G$ to be $\overline{\mathbf{w}} = \gamma^{k_{g_1}} b_{g_1} g_1 + \gamma^{k_{g_2}} b_{g_2} g_2 + \cdots + \gamma^{k_{g_n}} b_{g_n} g_n$, where

$$\gamma^{k_{g_i}} b_{g_i} = \gamma^{k_{g_i^{-1}}} w_{g_i^{-1}}. \tag{7.5}$$

Then

$$\sum_{i=1}^{n} \gamma^{l_{g_{j_i}g_i}} a_{g_{j_i}g_i} w_i = 0 \implies \sum_{i=1}^{n} \gamma^{l_{g_{j_i}g_i}} a_{g_{j_i}g_i} \gamma^{k_{g_i^{-1}}} b_{g_i^{-1}} = 0. \tag{7.6}$$

Here, $g_{j_i} g_i g_i^{-1} = g_{j_i}$, thus this is the coefficient of g_{j_i} in the product of $\mathbf{w}$ and v_j^*, where v_j^* is any row of the matrix $\Omega(v)$. This gives that $\overline{\mathbf{w}} \in \mathcal{R}(I)$ if and only if $\mathbf{w} \in \mathcal{C}^{\perp}$.

Let $\phi : R_\infty^n \to R_\infty G$ by $\phi(\mathbf{w}) = \overline{\mathbf{w}}$, then this map is a bijection between $\mathcal{C}^{\perp}$ and $\mathcal{R}(\Omega^{-1}(\mathcal{C})) = \mathcal{R}(I)$.

Theorem 34. *Let $\mathcal{C} = \mathcal{C}(v)$ be a code in $R_\infty G$ formed from the vector $v \in R_\infty G$. Then $\Omega^{-1}(\mathcal{C}^{\perp})$ is an ideal of $R_\infty G$.*

Proof. The composite mapping $\Omega(\phi(\mathcal{C}^{\perp}))$ is permutation equivalent to $\mathcal{C}^{\perp}$ and $\phi(\mathcal{C}^{\perp})$ is an ideal of $R_\infty G$. We know that ϕ is a bijection between $\mathcal{C}^{\perp}$ and $\mathcal{R}(\Omega^{-1}(\mathcal{C}))$, and we also know that $\Omega^{-1}(\mathcal{C})$ is an ideal of $R_\infty G$ as well. This proves that the dual of a composite G-code is also a composite G-code over the formal power series ring. □

7.2 Projections and Lifts of Composite G-codes

In this section, we extend more results from [17]. In fact, many of the results presented in this section are a consequence of the results proven in [31] and a simple generalization of the results proven in [17].

We first show that if $v \in R_\infty G$ then $\Omega(v)$ is permutation equivalent to the matrix defined in Equation (1.12). For simplicity, we write each non-zero element in R_∞ in the form $\gamma^i a$ where $a = a_0 + a_1\gamma + \cdots + \cdots$ with $a_0 \neq 0$ and $i \geq 0$, which means that a is a unit in R_∞.

Theorem 35. *Let $v = \gamma^{l_{g_i}} a_{g_1} g_1 + \gamma^{l_{g_2}} a_{g_2} g_2 + \cdots + \gamma^{l_{g_n}} a_{g_n} g_n \in R_\infty G$, where a_{g_i} are units in R_∞. Let $\mathcal{C}$ be a finitely generated code over R_∞. Then*

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

is permutation equivalent to the standard generator matrix given in Equation (1.12).

Proof. Take one non-zero element of the form $\gamma^{m_0} a_{g_i}$, where m_0 is the minimal non-negative integer. By applying column and row permutations and by dividing a row by a unit, the element that corresponds to the first row and column of $\Omega(v)$ can be replaced by γ^{m_0}. The elements in the first column of matrix $\Omega(v)$ have the form $\gamma^{l_{g_j}} a_{g_j}$ with $l_{g_j} \geq m_0$ and a_{g_j} a unit, thus, these can be replaced by zero when they are added to the first row multiplied by $-\gamma^{l_{g_j} - m_0}(a_{g_j})^{-1}$. Continuing the process using elementary operations, we obtain the standard generator matrix of the code $\mathcal{C}$ given in Equation (1.12). □

Example 7.2.1. *Let $G = \langle x, y \mid x^4 = 1, y^2 = x^2, yxy^{-1} = x^{-1} \rangle \cong Q_8$. Let*

$$v = \sum_{i=0}^{3} \left(\alpha_{i+1} x^i + \alpha_{i+5} x^i y \right) \in R_\infty Q_8,$$

where $\alpha_i = \alpha_{g_i} \in R_\infty$. 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:

$$\phi_1 : \begin{array}{c} (h_1)_i \xrightarrow{\phi_1} g_1^{-1} g_i \\ \text{for } i = \{1, 2, 3, 4\} \end{array} \qquad \phi_4 : \begin{array}{c} (h_1)_i \xrightarrow{\phi_4} g_5^{-1} g_j \\ \text{for when } \{i = 1, \ldots, 4 \text{ and } j = i + 4\}, \end{array}$$

in A_1' and A_4' respectively. This results in a composite matrix over R_∞ of the following form:

$$\Omega(v) = \left(\begin{array}{cc|c} X_1 & Y_1 & \multirow{2}{*}{X_2} \\ Y_1 & X_1 & \\ \hline \multicolumn{2}{c|}{\multirow{2}{*}{X_3}} & \begin{array}{cc} X_4 & Y_4 \\ Y_4 & X_4 \end{array} \end{array}\right) = \left(\begin{array}{cccc|cccc} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 \\ \alpha_2 & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_8 & \alpha_5 & \alpha_6 & \alpha_7 \\ \alpha_3 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_7 & \alpha_8 & \alpha_5 & \alpha_6 \\ \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_5 \\ \hline \alpha_7 & \alpha_6 & \alpha_5 & \alpha_8 & \alpha_1 & \alpha_4 & \alpha_3 & \alpha_2 \\ \alpha_8 & \alpha_7 & \alpha_6 & \alpha_5 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_5 & \alpha_8 & \alpha_7 & \alpha_6 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_4 \\ \alpha_6 & \alpha_5 & \alpha_8 & \alpha_7 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_1 \end{array}\right).$$

If we let $v = \gamma^2 x^3 + \gamma^2(1+\gamma)xy + \gamma^2(1+\gamma+\gamma^2)x^2y + \gamma^2x^3y \in R_\infty Q_8$, where $\langle x, y\rangle \cong Q_8$, then

$$\mathcal{C}(v) = \langle \Omega(v)\rangle =$$

$$\begin{pmatrix} 0 & 0 & 0 & \gamma^2 & 0 & \gamma^2(1+\gamma) & \gamma^2(1+\gamma+\gamma^2) & \gamma^2 \\ 0 & 0 & \gamma^2 & 0 & \gamma^2 & 0 & \gamma^2(1+\gamma) & \gamma^2(1+\gamma+\gamma^2) \\ 0 & \gamma^2 & 0 & 0 & \gamma^2(1+\gamma+\gamma^2) & \gamma^2 & 0 & \gamma^2(1+\gamma) \\ \gamma^2 & 0 & 0 & 0 & \gamma^2(1+\gamma) & \gamma^2(1+\gamma+\gamma^2) & \gamma^2 & 0 \\ \gamma^2(1+\gamma+\gamma^2) & \gamma^2(1+\gamma) & 0 & \gamma^2 & 0 & \gamma^2 & 0 & 0 \\ \gamma^2 & \gamma^2(1+\gamma+\gamma^2) & \gamma^2(1+\gamma) & 0 & \gamma^2 & 0 & 0 & 0 \\ 0 & \gamma^2 & \gamma^2(1+\gamma+\gamma^2) & \gamma^2(1+\gamma) & 0 & 0 & 0 & \gamma^2 \\ \gamma^2(1+\gamma) & 0 & \gamma^2 & \gamma^2(1+\gamma+\gamma^2) & 0 & 0 & \gamma^2 & 0 \end{pmatrix},$$

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

$$\begin{pmatrix} \gamma^2 & 0 & 0 & 0 & 0 & \gamma^2(1+\gamma) & \gamma^2(1+\gamma+\gamma^2) & \gamma^2 \\ 0 & \gamma^2 & 0 & 0 & \gamma^2 & 0 & \gamma^2(1+\gamma) & \gamma^2(1+\gamma+\gamma^2) \\ 0 & 0 & \gamma^2 & 0 & \gamma^2(1+\gamma+\gamma^2) & \gamma^2 & 0 & \gamma^2(1+\gamma) \\ 0 & 0 & 0 & \gamma^2 & \gamma^2(1+\gamma) & \gamma^2(1+\gamma+\gamma^2) & \gamma^2 & 0 \end{pmatrix}.$$

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

We now generalize the results from [17] on the projection of codes with a given type.

Proposition 7.2.1. *Let $\mathcal{C}$ be a composite G-code over R_∞ of type*

$$\{(\gamma^{m_0})^{k_0}, (\gamma^{m_1})^{k_1}, \ldots, (\gamma^{m_{r-1}})^{k_{r-1}}\}$$

with generator matrix $\Omega(v)$. The code generated by $\Psi_i(\Omega(v))$ is a code over R_i of type $\{(\gamma^{m_0})^{k_0}, (\gamma^{m_1})^{k_1}, \ldots, (\gamma^{m_{s-1}})^{k_{s-1}}\}$ where m_s is the largest m_i that is less than e. Also, the code generated by $\Psi_i(\Omega(v))$ is equal to

$$\{(\Psi_i(c_1), \Psi_i(c_2), \ldots, \Psi_i(c_n)) \mid (c_1, c_2, \ldots, c_n) \in \mathcal{C}\}. \tag{7.7}$$

Proof. If $m_i > e-1$ then Ψ_i sends $\gamma^{m_i}M'$, where M' is a matrix, to a zero matrix which gives the first part.

The code $\mathcal{C}$ is formed by taking the row space of $\Omega(v)$ over the ring R_∞, i.e. $\gamma^{l_1}a_1v_1 + \gamma^{l_2}a_2v_2 + \cdots + \gamma^{l_n}a_nv_n$ where $\gamma^{l_i}a_i \in R_\infty$ and v_i are the rows of $\Omega(v)$. If $w = \gamma^{l_j}a_jv_j$, then $\Psi_i(w) = \Psi_i(\gamma^{l_i}a_i)\Psi_i(v_i)$ by the equation given in (1.16) where $\Psi_i(v_i)$ applies the map coordinate-wise. This gives the second part. □

Since a composite G- code over R_∞ is a linear code, the following results are a direct consequence of some results proven in [31]. We omit the proofs.

Lemma 7.2.2. *Let $\mathcal{C}$ be a composite G-code of length n over R_∞, then,*

(1) $\mathcal{C}^\perp$ has type 1^m for some m,

(2) $\mathcal{C} = (\mathcal{C}^\perp)^\perp$ if and only if $\mathcal{C}$ has type 1^k for some k,

(3) If $\mathcal{C}$ has a standard generator matrix G as in equation (1.12), then we have

(i) the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$ has a generator matrix

$$H = \begin{pmatrix} B_{0,r} & B_{0,r-1} & \dots & B_{0,2} & B_{0,1} & I_{k_r} \end{pmatrix}, \tag{7.8}$$

where $B_{0,j} = -\sum_{l=1}^{j-1} B_{0,l}A^T_{r-j,r-l} - A^T_{r-j,r}$ for all $1 \leq j \leq r$;

(ii) rank($\mathcal{C}$)+rank($\mathcal{C}^\perp$)=n.

Example 7.2.2. *If we take the generator matrix G of a code $\mathcal{C}$ from Example 7.2.1, we can see that*

$$G = \left(\gamma^2 \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \gamma^2 \begin{pmatrix} 0 & 1+\gamma & 1+\gamma+\gamma^2 & 1 \\ 1 & 0 & 1+\gamma & 1+\gamma+\gamma^2 \\ 1+\gamma+\gamma^2 & 1 & 0 & 1+\gamma \\ 1+\gamma & 1+\gamma+\gamma^2 & 1 & 0 \end{pmatrix} \right),$$

which is the standard generator matrix- here,

$$A_{0,1} = \begin{pmatrix} 0 & 1+\gamma & 1+\gamma+\gamma^2 & 1 \\ 1 & 0 & 1+\gamma & 1+\gamma+\gamma^2 \\ 1+\gamma+\gamma^2 & 1 & 0 & 1+\gamma \\ 1+\gamma & 1+\gamma+\gamma^2 & 1 & 0 \end{pmatrix}.$$

In this case the generator matrix of the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$ has the form:

$$H = \begin{pmatrix} B_{0,1} & I_{k_1} \end{pmatrix}.$$

Now,

$$B_{0,1} = -A^T_{0,1},$$

thus

$$H = \begin{pmatrix} 0 & -(1+\gamma) & -(1+\gamma+\gamma^2) & -1 & 1 & 0 & 0 & 0 \\ -1 & 0 & -(1+\gamma) & -(1+\gamma+\gamma^2) & 0 & 1 & 0 & 0 \\ -(1+\gamma+\gamma^2) & -1 & 0 & -(1+\gamma) & 0 & 0 & 1 & 0 \\ -(1+\gamma) & -(1+\gamma+\gamma^2) & -1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

We also have

$$rank(\mathcal{C}) + rank(\mathcal{C}^{\perp}) = 4 + 4 = 8 = n.$$

Proposition 7.2.3. *Let $\mathcal{C}$ be a self-orthogonal composite G-code over R_∞. Then the code $\Psi_i(\mathcal{C})$ is a self-orthogonal composite G-code over R_i for all $i < \infty$.*

Proof. We first show that $\Psi_i(\mathcal{C})$ is self-orthogonal. Let $v \in R_\infty G$ and $\langle \Omega(v) \rangle = \mathcal{C}(v)$ be the corresponding self-orthogonal composite G-code. This implies that $[\mathbf{v}, \mathbf{w}] = 0$ for all $\mathbf{v}, \mathbf{w} \in \langle \Omega(v) \rangle = \mathcal{C}(v)$. This gives that

$$\sum_{l=1}^{n} v_l w_l \equiv \sum_{l=1}^{n} \Psi_i(v_l)\Psi_i(w_l) (\text{mod } \gamma^i) \equiv \Psi_i([\mathbf{v}, \mathbf{w}]) (\text{mod } \gamma^i) \equiv 0 \ (\text{mod } \gamma^i).$$

Hence $\Psi_i(\mathcal{C})$ is a self-orthogonal code over R_i. To show that $\Psi_i(\mathcal{C})$ is also a G-code, we notice that when taking $\Psi_i(\mathcal{C}) = \Psi_i(\langle \Omega(v) \rangle)$, it corresponds to $\Psi_i(v) = \Psi_i(\gamma^{l_{g_1}} a_{g_1}) g_1 + \Psi_i(\gamma^{l_{g_2}} a_{g_2}) g_2 + \cdots + \Psi_i(\gamma^{l_{g_n}} a_{g_n}) g_n$, then $\Psi_i(\mathcal{C}) \in R_i G$. Thus $\Psi_i(\mathcal{C})$ is also a composite G-code. □

Definition 54. *Let i, j be two integers such that $1 \leq i \leq j < \infty$. We say that an $[n, k]$ code C_1 over R_i lifts to an $[n, k]$ code C_2 over R_j, denoted by $C_1 \succeq C_2$, if C_2 has a generator matrix G_2 such that $\Psi_i^j(G_2)$ is a generator matrix of C_1. We also denote C_1 by $\Psi_i^j(C_2)$. If $\mathcal{C}$ is a $[n, k]$ γ-adic code, then for any $i < \infty$, we call $\Psi_i(\mathcal{C})$ a projection of $\mathcal{C}$. We denote $\Psi_i(\mathcal{C})$ by $\mathcal{C}^i$.*

Lemma 7.2.4. *Let $\mathcal{C}$ be a composite G-code over R_∞ with type 1^k. If $\Omega(v)$ is a standard form of $\mathcal{C}$, then for any positive integer, i, $\Psi_i(\Omega(v))$ is a standard form of $\Psi_i(\mathcal{C})$.*

Proof. We know from Theorem 35 that $\Omega(v)$ is permutation equivalent to a standard form matrix defined in Equation (1.12). We also have that $\mathcal{C}$ has type 1^k, hence $\Psi_i(\mathcal{C})$ has type 1^k. The rest of the proof is the same as in [31]. □

In the following, to avoid confusion, we let v_∞ and v be elements of the group rings $R_\infty G$ and $R_i G$ respectively. Let $v_\infty = \gamma^{l_1} a_{g_1} g_1 + \gamma^{l_2} a_{g_2} g_2 + \cdots + \gamma^{l_n} a_{g_n} g_n \in R_\infty G$, and $\mathcal{C}(v_\infty) = \langle \Omega(v_\infty) \rangle$ be the corresponding composite G-code. Define the following map:

$$\Omega_1 : R_\infty G \to \mathcal{C}(v_\infty),$$

$$(\gamma^{l_{g_1}} a_{g_1} g_1 + \gamma^{l_{g_2}} a_{g_2} g_2 + \cdots + \gamma^{l_{g_n}} a_{g_n} g_n) \mapsto M(R_\infty G, v_\infty).$$

We define a projection of composite G-codes over $R_\infty G$ to $R_i G$.

Let

$$\Psi_i : R_\infty G \to R_i G \tag{7.9}$$

$$\gamma^i a \mapsto \Psi_i(\gamma^i a). \tag{7.10}$$

The projection is a homomorphism which means that if I is an ideal of $R_\infty G$, then $\Psi_i(I)$ is an ideal of $R_i G$. We have the following commutative diagram:

$$\begin{tikzcd}
R^n_\infty G \arrow[r, "\Omega_1"] \arrow[d, "\Psi_i"'] & \mathcal{C}(v_\infty) \arrow[d, "\Psi_i"] \\
R^n_i G \arrow[r, "\Omega_1"'] & \mathcal{C}(v)
\end{tikzcd} .$$

This gives that $\Psi_i \Omega_1 = \Omega_1 \Psi_i$, which gives the following theorem.

Theorem 36. *If $\mathcal{C}$ is a composite G-code over R_∞, then $\Psi_i(\mathcal{C})$ is a composite G-code over R_i for all $i < \infty$.*

Proof. Let $v_\infty \in R_\infty G$ and $\mathcal{C}(v_\infty)$ be the corresponding composite G-code over R_∞. Then $\Omega_1(v_\infty) = \mathcal{C}(v_\infty)$ is an ideal of $R_\infty G$. By the homomorphism in Equation 7.9 and the commutative diagram above, we know that $\Psi_i(\Omega_1(v_\infty)) = \Omega_1(\Psi_i(v_\infty))$ is an ideal of the group ring $R_i G$. This implies that $\Psi_i(\mathcal{C})$ is a composite G-code over R_i for all $i < \infty$. □

Theorem 37. *Let C be a composite G-code over R_i, then the lift of $\mathcal{C}$, $\tilde{\mathcal{C}}$ over R_j, where $j > i$, is also a composite G-code.*

Proof. Let $v_1 = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \cdots + \alpha_{g_n} g_n \in R_i G$ and $\mathcal{C} = \langle \Omega(v_1) \rangle$ be the corresponding composite G-code. Let $v_2 = \beta_{g_1} g_1 + \beta_{g_2} g_2 + \cdots + \beta_{g_n} g_n \in R_j G$ and $\tilde{\mathcal{C}} = \langle \Omega(v_2) \rangle$ be the corresponding composite G-code. We can say that v_1 and v_2 act as generators of $\mathcal{C}$ and $\tilde{\mathcal{C}}$ respectively. We can clearly see that we can have $\Psi^j_i(v_2) = \Psi^j_i(\beta_{g_1}) g_1 + \Psi^j_i(\beta_{g_2}) g_2 + \cdots + \Psi^j_i(\beta_{g_n}) g_n = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \cdots + \alpha_{g_n} g_n \in R_i G$, thus $\Psi^j_i(v_2)$ is a generator matrix of $\mathcal{C}$. This implies that the composite G-code $\mathcal{C}(v_1)$ over R_i lifts to a composite G-code over R_j, for all $j > i$. □

The following results consider composite G-codes over chain rings that are projections of γ-adic codes. The results are just a simple consequence of the results proven in [31]. For details on notation and proofs, please refer to [31] and [17].

Lemma 7.2.5. *Let $\mathcal{C}$ be a $[n, k]$ composite G-code of type 1^k, and G, H be a generator and parity-check matrices of $\mathcal{C}$. Let $G_i = \Psi_i(G)$ and $H_i = \Psi_i(H)$. Then G_i and H_i are generator and parity check matrices of $\mathcal{C}^i$ respectively. Let $i < j < \infty$ be two positive integers, then*

(i) $\gamma^{j-i} G_i \equiv \gamma^{j-i} G_j \pmod{\gamma^j}$;

(ii) $\gamma^{j-i}H_i \equiv \gamma^{j-i}H_j \pmod{\gamma^j}$.

(iii) $\gamma^{j-1}\mathcal{C}^i \subseteq \mathcal{C}^j$*;*

(iv) $\mathbf{v} = \gamma^i\mathbf{v}_0 \in \mathcal{C}^j$ *if and only if* $\mathbf{v}_0 \in \mathcal{C}^{j-i}$*;*

(v) *Ker(*Ψ_i^j*)=*$\gamma^i\mathcal{C}^{j-i}$.

Theorem 38. *Let $\mathcal{C}$ be a composite G-code over R_∞. Then the following two results hold.*

(i) the minimum Hamming distance $d_H(\mathcal{C}^i)$ of $\mathcal{C}^i$ is equal to $d = d_H(\mathcal{C}^1)$ for all $i < \infty$;

(ii) the minimum Hamming distance $d_\infty = d_H(\mathcal{C})$ of $\mathcal{C}$ is at least $d = d_H(\mathcal{C}^1)$.

The final two results we present in this section are a simple extension of the two results from [31] on MDS and MDR codes over R_∞. We omit the proofs since a composite G- code over R_∞ is a linear code and for that fact, the proofs are the same as in [31].

Theorem 39. *Let $\mathcal{C}$ be a composite G-code over R_∞. If $\mathcal{C}$ is an MDR or MDS code then $\mathcal{C}^\perp$ is an MDS code.*

Theorem 40. *Let $\mathcal{C}$ be a composite G-code over R_i, and $\tilde{\mathcal{C}}$ be a lift of C over R_j, where $j > i$. If $\mathcal{C}$ is an MDS code over R_i then the code $\tilde{\mathcal{C}}$ is an MDS code over R_j.*

7.3 Self-Dual γ-adic composite G-codes

In this section, we extend some results for self-dual γ-adic codes to composite G-codes over R_∞. As in previous sections, the results presented here are just a simple generalization of the results proven in [31] and [17].

Fix the ring R_∞ with

$$R_\infty \to \cdots \to R_i \to \cdots \to R_2 \to R_1$$

and $R_1 = \mathbb{F}_q$ where $q = p^r$ for some prime p and nonnegative integer r. The field $\mathbb{F}_q$ is said to be the underlying field of the rings.

We now generalize four theorems from [31]. The first two consider self-dual codes over R_i with a specific type and projections of self-dual codes over R_∞ respectively. The third one considers a method for constructing self-dual codes over $\mathbb{F}$ from a self-dual code over R_i. We extend these to self-dual composite G-codes over R_i and R_∞ respectively.

Theorem 41. *Let i be odd and $\mathcal{C}$ be a composite G-code over R_i with type $1^{k_0}(\gamma)^{k_1}(\gamma^2)^{k_2}\ldots(\gamma^{i-1})^{k_{i-1}}$. Then $\mathcal{C}$ is a self-dual code if and only if $\mathcal{C}$ is self-orthogonal and $k_j = k_{i-j}$ for all j.*

Proof. It is enough to show that $\Omega(v)$ where $v \in R_iG$ and G is a finite group, is permutation equivalent to the matrix (1.10). The rest of the proof is the same as in [31]. $\square$

Theorem 42. *If $\mathcal{C}$ is a self-dual composite G-code of length n over R_∞ then $\Psi_i(\mathcal{C})$ is a self-dual composite G-code of length n over R_i for all $i < \infty$.*

Proof. This is a direct consequence of Theorem 3.4 in [31] and Proposition 7.2.3 of this work. $\square$

Theorem 43. *Let i be odd. A self-dual composite G-code of length n over R_i induces a self-dual composite G-code of length n over $\mathbb{F}_q$.*

Proof. The first part of the proof is identical to the one of Theorem 5.5 from [17]. Secondly, when the map $\Psi_1^i(\tilde{G})$ is used in [31], we notice that in our case the map will correspond to $\Psi_1^i(\tilde{G}) = \Psi_1^i(v) = \Psi_1^i(\gamma^{l_{g_1}}a_{g_1})g_1 + \Psi_1^i(\gamma^{l_{g_2}}a_{g_2})g_2 + \cdots + \Psi_1^i(\gamma^{l_{g_n}}a_{g_n})g_n$, assuming that $\tilde{G}$ is the generator matrix of a composite G-code and $v \in R_iG$. Then $\Psi_1^i(\tilde{G})$ is the generator matrix of a composite G-code over $\mathbb{F}_q$. $\square$

Theorem 44. *Let $R = R_e$ be a finite chain ring, $\mathbb{F} = R/\langle\gamma\rangle$, where $|\mathbb{F}| = q = p^r, 2 \neq p$ is a prime. Then any self-dual composite G-code $\mathcal{C}$ over $\mathbb{F}$ can be lifted to a self-dual composite G-code over R_∞.*

Proof. From Theorem 37 we know that a composite G-code over R_i can be lifted to a composite G-code over R_j, where $j > i$. To show that a self-dual composite G-code over $\mathbb{F}$ lifts to a self-dual composite G-code over R_∞, it is enough to follow the proof in [31]. $\square$

7.4 Composite G-codes over Principal Ideal Rings

In this section, we study composite G-codes over principal ideal rings. We study codes over this class of rings by the generalized Chinese Remainder Theorem. Please see [12] for more details on the notation and definitions of the principal ideal rings.

Let $R_{e_1}^1, R_{e_2}^2, \ldots, R_{e_s}^s$ be chain rings, where $R_{e_j}^j$ has unique maximal ideal $\langle\gamma_j\rangle$ and the nilpotency index of γ_j is e_j. Let $\mathbb{F}^j = R_{e_j}^j/\langle\gamma_j\rangle$. Let

$$A = \text{CRT}(R_{e_1}^1, \ldots, R_{e_j}^j, \ldots, R_{e_s}^s).$$

We know that A is a principal ideal ring. For any $1 \leq i < \infty$, let

$$A_i^j = \text{CRT}(R_{e_1}^1, \ldots, R_i^j, \ldots, R_{e_s}^s).$$

This gives that all the rings A_i^j are principal ideal rings. In particular, $A_{e_j}^j = A$. We denote $\text{CRT}(R_{e_1}^1 \ldots, R_\infty^j, \ldots, R_{e_s}^s)$ by A_∞^j.

For $1 \leq i < \infty$, let $\mathcal{C}_i^j$ be a code over R_i^j. Let

$$\mathcal{C}_i^j = \text{CRT}(\mathcal{C}_{e_1}^1, \ldots, \mathcal{C}_i^j, \ldots, \mathcal{C}_{e_s}^s)$$

be the associated code over A_i^j. Let

$$\mathcal{C}_\infty^j = \text{CRT}(\mathcal{C}_{e_1}^1, \ldots, \mathcal{C}_\infty^j, \ldots, \mathcal{C}_{e_s}^s)$$

be associated code over A_∞^j. We can now prove the following.

Theorem 45. *Let $\mathcal{C}_{e_j}^j$ be a composite G-code over the chain ring $R_{e_j}^j$ that is $\mathcal{C}_{e_j}^j$ is an ideal in $R_{e_j}G$. Then $\mathcal{C}_\infty^j$ =$CRT(\mathcal{C}_{e_1}^1, \ldots, \mathcal{C}_\infty^j, \ldots, \mathcal{C}_{e_s}^s)$ is a composite G-code over A_∞^j.*

Proof. Let $\mathbf{v}_j \in \mathcal{C}_{e_j}^j$. We know that $\mathbf{v}_j^*$ also belongs to $\mathcal{C}_{e_j}^j$ where $\mathbf{v}_j^*$ has the form defined in (7.1). Let $\mathbf{v} \in \mathcal{C}_\infty^j$. Now if $\mathbf{v} = CRT(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s)$, then $\mathbf{v}^* = CRT(\mathbf{v}_1^*, \mathbf{v}_2^*, \ldots, \mathbf{v}_s^*)$ and so $\mathbf{v}^* \in \mathcal{C}_\infty^j$ giving that $\mathcal{C}_\infty^j$ is an ideal in $A_\infty^j G$, and thus giving that $\mathcal{C}_\infty^j$ is a composite G-code over A_∞^j. □

Chapter 8

Conclusion

In this thesis, we presented a number of generator matrices for self-dual codes over a finite commutative Frobenius ring. We showed that together with our generator matrices and some well-known code construction methods, one can obtain extremal binary self-dual codes with new weight enumerators. We introduced a new family of commutative Frobenius rings and studied group codes over this new alphabet. We extended an established isomorphism between group rings and a subring of the $n \times n$ matrices to enable one to construct complex matrices, fully defined by the elements appearing in the first row. Moreover, we showed that our extension has applications to algebraic coding theory and in particular for constructing generator matrices which can be used to search for new binary extremal self-dual codes - we presented many examples. We now reflect on the work published and review the importance of the theory and numerical results.

In Chapter 2, we presented a generator matrix that can be used to search for self-dual codes over a finite commutative Frobenius ring. We gave the necessary conditions that our generator matrix has to meet in order to produce a self-dual code over this specific alphabet. We were able to construct many extremal binary self-dual codes of length 68 only for the simple case when the group is the cyclic group of order 2. A suggestion for future research is to consider our generator matrix for groups different than the cyclic group of order 2. One may for example consider groups of higher orders and search for self-dual codes of higher lengths over different alphabets.

In Chapter 3, we introduced a new family of the commutative Frobenius rings. We studied group codes over this new alphabet and presented a Gray map associated with this new family of rings. We showed that one can obtain codes with rich automorphism group via the Gray map. A suggestion for future research is to consider our new family of rings together with the Gray map and to construct codes with weight enumerators not known in the literature. One may for example consider our generator matrix from Chapter 2 and construct self-dual codes over the ring $\mathcal{B}_{j,k}$ to then obtain the binary images, that is, binary self-dual codes. Since we have shown that codes obtained in this way have rich automorphism groups, we believe that in this way, there is a high chance of finding new binary self-dual codes of different lengths with new weight enumerators that could not be obtained from other known techniques or generator matrices.

Chapters 4, 5, 6 and 7 are all connected. We firstly extended an established isomorphism between group rings and a subring of the $n \times n$ matrices to then present many of its applications to algebraic coding theory. In particular, we showed that one can use our extended isomorphism to construct generator matrices which can be employed to search for extremal binary self-dual codes with new parameters in their weight enumerators. We only restricted our attention to binary self-dual codes with parameters $[68, 34, 12]$, but our extended isomorphism can be used to construct generator matrices that can be used to search for extremal binary self-dual codes of different lengths. We also used our extended isomorphism to introduce a new family of codes that we call composite G-codes. We studied many properties of this class of codes. A suggestion for future work is to employ our extended isomorphism and construct generator matrices that can be then used to search for extremal or optimal codes of different lengths. Another possible direction is to consider generator matrices over non-commutative rings and explore the possible numerical outcomes.

Throughout this thesis, we constructed many new binary self-dual codes with parameters $[68, 34, 12]$. To highlight the contribution of our work we now summarise all the new codes constructed in this thesis. In particular, we were able to construct the following extremal binary self-dual codes with new weight enumerators in $W_{68,2}$:

$$\begin{aligned}
&(\gamma = 0, \quad \beta = \{38\}),\\
&(\gamma = 1, \quad \beta = \{38, 46, 173, 177, 181\}),\\
&(\gamma = 2, \quad \beta = \{67, 167, 175, 177, 179, 181, 183, 187, 191, 197\}),\\
&(\gamma = 3, \quad \beta = \{74, 77, 78, 81, 157, 179, 181, 183, 185, 187, 195, 197, 199, 201, 203, 217\}),\\
&(\gamma = 4, \quad \beta = \{92, 94, 107, 115, 119\}),\\
&(\gamma = 5, \quad \beta = \{110, 183, 184, 185, 186, 188, 190, 192, 194, 196, 197, 199, 203, 204, 205, 213\}),\\
&(\gamma = 6, \quad \beta = \{117, 120, 121, 122, 123, 124, 192, 210\}),\\
&(\gamma = 7, \quad \beta = \{131, 132, 134, 135, 136, 137, 138, 139, 141, 143\}),\\
&(\gamma = 8, \quad \beta = \{139, 140, 141, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152\}),\\
&(\gamma = 9, \quad \beta = \{151, 152, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165,\\
&\qquad\qquad\quad 166, 167, 168, 170, 172\}).
\end{aligned}$$

Appendices

Appendix A

Magma Programs

We now give a number of *MAGMA* programs that can be used and adapted to search for binary self-dual codes of different lengths. The examples we present are specifically designed for the generator matrices from Chapters 2, 5 and 6 of this thesis.

A.1 Chapter 2

Here, we present a *MAGMA* program that one can use to construct a binary $[24, 12, 6]$ self-dual code with the generator matrix defined in Chapter 2. This code is designed for the cyclic group of order 3 and can be easily adapted to explore other cases.

```
t:=Cputime();
SetLogFile("Bisymmetric(1).txt");

Rk:=GF(2);
codeF2:=[];
M:=[];

Mtemp1:=RMatrixSpace(Rk,12,12)!0;
            for i:=1 to 12 do
              Mtemp1[i,i]:=1;
            end for;

Mtemp2:=RMatrixSpace(Rk,6,6)!0;
            for i:=1 to 6 do
              Mtemp1[i,i]:=1;
            end for;
```

```
function cycgen(gg)
  n:=3;
  M:=RMatrixSpace(Rk,n,n)!0;
     for k:=1 to n do
       M[k]:=gg;
       temp:=gg;
       for t:=1 to (n-1) do
         temp[t+1]:=gg[t];
       end for;
       temp[1]:=gg[n];
       gg:=temp;
     end for;
     return M;
  end function;

counter:=0;

for i1:=0 to 1 do for i2:=0 to 1 do
for i3:=0 to 1 do for i4:=0 to 1 do
for i5:=0 to 1 do for i6:=0 to 1 do
for i7:=0 to 1 do for i8:=0 to 1 do
for i9:=0 to 1 do for i10:=0 to 1 do
for i11:=0 to 1 do for i12:=0 to 1 do
for i13:=0 to 1 do for i14:=0 to 1 do
for i15:=0 to 1 do for i16:=0 to 1 do
for i17:=0 to 1 do for i18:=0 to 1 do
for i19:=0 to 1 do for i20:=0 to 1 do
for i21:=0 to 1 do

v1:=RSpace(Rk,3)![i1,i2,i2];
B1:=cycgen(v1);

v2:=RSpace(Rk,3)![i3,i3,i3];
B2:=cycgen(v2);

B:=BlockMatrix(2,2,
[
B1,B2,
B2,B1
]);

A1:=HorizontalJoin(B,Mtemp2);

A2:=HorizontalJoin(Mtemp2,B);

A:=VerticalJoin(A1,A2);

w1:=RSpace(Rk,3)![i4,i5,i6];
w2:=RSpace(Rk,3)![i7,i8,i9];
w3:=RSpace(Rk,3)![i10,i11,i12];
w4:=RSpace(Rk,3)![i13,i14,i15];
w5:=RSpace(Rk,3)![i16,i17,i18];
w6:=RSpace(Rk,3)![i19,i20,i21];

S1:=cycgen(w1);
S2:=cycgen(w2);
S3:=cycgen(w3);
S4:=cycgen(w4);
S5:=cycgen(w5);
S6:=cycgen(w6);

S:=BlockMatrix(4,4,
[
S1,S2,S3,S4,
S2,S5,S6,S3,
S3,S6,S5,S2,
S4,S3,S2,S1
]);

CM:=HorizontalJoin(A,S);

if CM*Transpose(CM) eq Mtemp1 then
M:=Append(M,CM);
end if;

end for;end for;end for;end for;
end for;end for;end for;end for;
end for;end for;end for;end for;
end for;end for;end for;end for;
end for;end for;end for;end for;
end for;

#M;

for i:=1 to #M do

M1:=M[i];

   C:=LinearCode(M1); dm:=MinimumWeight(C);
   if (dm ge 6) and IsSelfDual(C) then

     eql:=false;
             for i2:=1 to #codeF2 do
               eql:=eql or IsEquivalent(C,codeF2[i2]) ;
             end for;
             if not eql then

              counter:=counter+1;
              counter;
              codeF2[counter]:=C;
             M1;
             AutomorphismGroup(C);
             WeightDistribution(C);
             "*********************";
             end if;

  end if;

end for;

print Cputime(t);
```

A.2 Chapter 5

Here, we present a *MAGMA* program that one can use to construct a binary $[16, 8, 4]$ self-dual code with the generator matrix defined in Chapter 5, Section 5.3.1. This code can be easily adapted to other alphabets and codes of other lengths.

```
t:=Cputime();
SetLogFile("(Omega(v))");

Rk:=GF(2);
codeF2:=[];
M:=[];

Mtemp1:=RMatrixSpace(Rk,8,8)!0;
            for i:=1 to 8 do
              Mtemp1[i,i]:=1;
            end for;

function cycgen(gg)
  n:=2;
  M:=RMatrixSpace(Rk,n,n)!0;
     for k:=1 to n do
       M[k]:=gg;
       temp:=gg;
       for t:=1 to (n-1) do
         temp[t+1]:=gg[t];
       end for;
       temp[1]:=gg[n];
       gg:=temp;
     end for;
     return M;
  end function;

counter:=0;

for i1:=0 to 1 do for i2:=0 to 1 do
for i3:=0 to 1 do for i4:=0 to 1 do
for i5:=0 to 1 do for i6:=0 to 1 do
for i7:=0 to 1 do for i8:=0 to 1 do
```

```
v1:=RSpace(Rk,2)![i1,i2];
v2:=RSpace(Rk,2)![i3,i4];
v3:=RSpace(Rk,2)![i4,i3];
A1:=cycgen(v1);
A2:=cycgen(v2);
A3:=cycgen(v3);

A:=BlockMatrix(2,2,
[
A1,A2,
A3,A1
]);

AA:BlockMatrix(2,2,
[
A1,A2,
A2,A1
]);

w1:=RSpace(Rk,2)![i5,i6];
w2:=RSpace(Rk,2)![i7,i8];

B1:=cycgen(w1);
B2:=cycgen(w2);

B:=BlockMatrix(2,2,
[
B1,B2,
B2,B1
]);

CM:=BlockMatrix(2,2,
[
A,B,
B,AA
]);

if CM*Transpose(CM) eq Mtemp1 then
M:=Append(M,CM);
```

```
end if;

end for;end for;end for;end for;
end for;end for;end for;end for;

#M;

for i:=1 to #M do

M1:=HorizontalJoin(Mtemp1,M[i]);

   C:=LinearCode(M1); dm:=MinimumWeight(C);
   if (dm ge 4) and IsSelfDual(C) then

     eql:=false;
             for i2:=1 to #codeF2 do
               eql:=eql or IsEquivalent(C,codeF2[i2]) ;
             end for;
             if not eql then

              counter:=counter+1;
              counter;
              codeF2[counter]:=C;
             M1;
             AutomorphismGroup(C);
             WeightDistribution(C);
             "*********************";
             end if;

  end if;

end for;

print Cputime(t);
```

A.3 Chapter 6

Here, we present a *MAGMA* program that one can use to construct a binary $[16, 8, 4]$ self-dual code with the generator matrix defined in Chapter 6, and specifically in Theorem 31. This code can be easily adapted to other alphabets and codes of other lengths.

```
t:=Cputime();
SetLogFile("(Omega(v_1))");

Rk:=GF(2);
codeF2:=[];
M:=[];

Mtemp1:=RMatrixSpace(Rk,8,8)!0;
            for i:=1 to 8 do
              Mtemp1[i,i]:=1;
            end for;

function cycgen(gg)
  n:=2;
  M:=RMatrixSpace(Rk,n,n)!0;
     for k:=1 to n do
       M[k]:=gg;
       temp:=gg;
       for t:=1 to (n-1) do
         temp[t+1]:=gg[t];
       end for;
       temp[1]:=gg[n];
       gg:=temp;
     end for;
     return M;
  end function;

counter:=0;

for i1:=0 to 1 do for i2:=0 to 1 do
for i3:=0 to 1 do for i4:=0 to 1 do
for i5:=0 to 1 do for i6:=0 to 1 do
for i7:=0 to 1 do for i8:=0 to 1 do
```

```
v1:=RSpace(Rk,2)![i1,i2];
v2:=RSpace(Rk,2)![i3,i4];
A1:=cycgen(v1);
A2:=cycgen(v2);

A:=BlockMatrix(2,2,
[
A1,A2,
A2,A1
]);


w1:=RSpace(Rk,2)![i5,i6];
w2:=RSpace(Rk,2)![i7,i8];
B1:=cycgen(w1);
B2:=cycgen(w2);

B:=BlockMatrix(2,2,
[
B1,B2,
B2,B1
]);

z1:=RSpace(Rk,2)![i8,i5];
z2:=RSpace(Rk,2)![i6,i7];
C1:=cycgen(z1);
C2:=cycgen(z2);

C:=BlockMatrix(2,2,
[
C1,C2,
C2,C1
]);

CM:=BlockMatrix(2,2,
[
A,B,
C,A
]);
```

```
if CM*Transpose(CM) eq Mtemp1 then
M:=Append(M,CM);
end if;

end for;end for;end for;end for;
end for;end for;end for;end for;

#M;

for i:=1 to #M do

M1:=HorizontalJoin(Mtemp1,M[i]);

   C:=LinearCode(M1); dm:=MinimumWeight(C);
   if (dm ge 4) and IsSelfDual(C) then

     eql:=false;
             for i2:=1 to #codeF2 do
               eql:=eql or IsEquivalent(C,codeF2[i2]) ;
             end for;
             if not eql then

              counter:=counter+1;
              counter;
              codeF2[counter]:=C;
             M1;
             AutomorphismGroup(C);
             WeightDistribution(C);
             "********************";
             end if;

  end if;

end for;

print Cputime(t);
```

Bibliography

[1] M. Anthony, M. Harvey, “Linear Algebra Concepts and Methods”, Cambridge University Press, 2012.

[2] E. F. Assmus Jr., H. F. Mattson Jr., “New 5-Designs ”, J. Comb. Theory, vol. 6, pp. 122–151, 1969.

[3] A. Bannai, S. T. Dougherty, M. Harada, M. Oura, “Type II Codes, Even Unimodular Lattices and Invariant Rings ”, IEEE-IT, vol. 45, pp. 1194–1205, 1999.

[4] W. Bosma, J. Cannon, C. Playoust, “The Magma Algebra system I, the user language ”, J. Symbolic Comput., vol. 24, pp. 235–265, 1997.

[5] R. L. Bouzara, K. Guenda, E. Martinez-Moro, “Lifted Codes and Lattices from Codes over Finite Chain Rings ”, arXiv:2007.05871.

[6] S. Buyuklieva, I. Bouyukliev, “Extremal Self-Dual Codes with an Automorphism of Order 2 ”, IEEE Trans. Inform. Theory, vol. 44, pp. 323–328, 1998.

[7] A. R. Calderbank, A.R. Hammons Jr., P.V. Kumar, N.J.A. Sloane, P. Sole, “A Linear Construction for Certain Kerdock and Preparata Codes ”Bull. Amer. Math. Soc. vol. 29, pp. 218–222, 193.

[8] Y. Cengellenmis, A. Dertli, S.T. Dougherty, “Codes over an Infinite Family of Rings with a Gray Map”, Des., Codes and Crypt., vol. 72, pp. 559–580, 2014.

[9] Y. Cengellenmis, A. Dertli, S.T. Dougherty, A. Korban, S. Sahinkaya, “Reversible G-Codes over the Ring $\mathcal{F}_{j,k}$ with Applications to DNA Codes”, **in submission**.

[10] J.H. Conway, N.J.A. Sloane, “A New Upper Bound on the Minimal Distance of Self-Dual Codes ”, IEEE Trans. Inform. Theory, vol. 36, no. 6, pp. 1319–1333, 1990.

[11] J. Denes, A. Donald Keedwell, “Latin Squares and their Applications”, Second edition, North Holland, 2015.

[12] S.T. Dougherty, “Algebraic Coding Theory over Finite Commutative Rings”, Springer-Verlag, Springer Briefs in Mathematics (ISBN 978-3-319-59805-5), 2017.

[13] S.T. Dougherty, P. Gaborit, M. Harada, P. Sole, “Type II Codes over $\mathbb{F}_2 + u\mathbb{F}_2$ ”, IEEE Trans. Inform. Theory, vol. 45, pp. 32–45, 1999.

[14] S.T. Dougherty, J. Gildea, A. Kaya, “Quadruple Bordered Constructions of Self-Dual Codes from Group Rings over Frobenius Rings ”, Cryptogr. Commun., vol. 12, pp. 127–146, 2019.

[15] S.T. Dougherty, J. Gildea, A. Kaya, “2^n Bordered Constructions of Self-Dual Codes from Group Rings ”, Finite Fields Appl., vol. 67, 2020.

[16] S.T. Dougherty, J. Gildea, A. Kaya, B. Yildiz, “New Self-Dual and Formally Self-Dual Codes from Group Ring Constructions ”, Advances in Mathematics of Communications, vol. 14, no. 1, pp. 11–22, 2020.

[17] S. T. Dougherty, J. Gildea, A. Korban, “G- Codes over Formal Power Series Rings and Finite Chain Rings”, J. Algebra Comb. Discrete Appl., vol. 7, pp. 55–71, 2020.

[18] S. T. Dougherty, J. Gildea, A. Korban, “Extending an Established Isomorphism between Group Rings and a Subring of the $n \times n$ Matrices ”, International Journal of Algebra and Computation, DOI: https://doi.org/10.1142/S0218196721500223.

[19] S.T. Dougherty, J. Gildea, A. Korban, A. Kaya, “Composite Constructions of Self-Dual Codes from Group Rings and New Extremal Self-Dual Binary Codes of Length 68 ”, Advances in Mathematics of Communications, vol. 14, no. 4, pp. 677–702, 2020.

[20] S.T. Dougherty, J. Gildea, A. Korban, A. Kaya, “New Extremal Self-Dual Binary Codes of Length 68 via Composite Construction, $\mathbb{F}_2 + u\mathbb{F}_2$ Lifts, Extensions and Neighbors”, International Journal of Information and Coding Theory, vol. 5, no. 3/4, pp. 211–226, 2020.

[21] S.T. Dougherty, J. Gildea, A. Kaya, A. Korban, “Composite Matrices from Group Rings, Composite G-Codes and Constructions of Self-Dual Codes ”, arXiv:2002.11614.

[22] S.T. Dougherty, J. Gildea, A. Korban, A. Kaya, A. Tylshchak, B. Yildiz, “Bordered Constructions of Self-Dual Codes from Group Rings ”, Finite Fields Appl., vol. 57, pp. 108–127, 2019.

[23] S.T. Dougherty, J. Gildea, R. Taylor, A. Tylshchak, “Group Rings, G-Codes and Constructions of Self-Dual and Formally Self-Dual Codes”, Des., Codes and Cryptog., vol. 86, no. 9, pp. 2115–2138, 2018.

[24] S.T. Dougherty, S. Karadeniz, B. Yildiz "Codes over R_k, Gray Maps and their Binary Images", Finite Fields Appl., vol. 17, pp. 205–219, 2011.

[25] S.T. Dougherty, S. Karadeniz, B. Yildiz, "Cyclic Codes over R_k ", Des., Codes and Cryptog., vol. 63, pp. 113–126, 2012.

[26] S.T. Dougherty, S. Karadeniz, B. Yildiz, "Self-Dual Codes over R_k and Binary Self-Dual Codes ", European Journal of Pure and Applied Mathematics, vol. 6, no. 1, pp. 89–106, 2013.

[27] S.T. Dougherty, S. Karadeniz, B. Yildiz, "Constructing Formally Self-Dual Codes over R_k", Discrete Applied Mathematics, vol. 167, pp. 188–196, 2014.

[28] S.T. Dougherty, J.L. Kim, H. Kulosman, H. Liu, "Self-Dual Codes over Commutative Frobenius Rings ", Finite Fields Appl., vol. 16, pp. 14–26, 2010.

[29] S.T. Dougherty, H. Liu, "Independence of Vectors in Codes over Rings", Des., Codes and Cryptog. vol. 51, pp. 55–68, 2009.

[30] S.T. Dougherty, H. Liu, "Cyclic Codes over Formal Power Series Rings", Acta Mathematica Scientia, vol. 31, no. 1, pp. 331–343, 2011.

[31] S.T. Dougherty, H. Liu, Y.H. Park, "Lifted Codes over Finite Chain Rings", Mathematical Journal of Okayama University, vol. 53, pp. 39–53, 2010.

[32] S.T. Dougherty, E. Salturk, S. Szabo, "On Codes over Frobenius Rings: Generating characters, MacWilliams Identities and Generator Matrices ", Applicable Algebra in Engineering, Communication and Computing, vol. 30, pp. 193–206, 2019.

[33] D.S. Dummit, R.M. Foote, "Abstract Algebra", Third Edition, (ISBN 0471433349, 9780471433347), 2003.

[34] P. Gaborit, V. Pless, P. Sole, O. Atkin, "Type II Codes over $\mathbb{F}_4$ ", Finite Fields Appl., vol. 8, pp. 171–183, 2002.

[35] J. Gildea, A. Kaya, A. Korban, A. Tylyshchak, "Self-Dual Codes using Bisymmetric Matrices and Group Rings ", Discrete Math., vol. 343, no. 11, 2020.

[36] J. Gildea, A. Kaya, A. Korban, B. Yildiz, "Constructing Self-Dual Codes from Group Rings and Reverse Circulant Matrices ", Advances in Mathematics of Communications, doi: 10.3934/amc.2020077.

[37] J. Gildea, A. Kaya, A. Korban, B. Yildiz, "New Extremal Binary Self-Dual Codes of Length 68 from Generalized Neighbours ", Finite Fields Appl., vol. 67, 2020.

[38] J. Gildea, A. Kaya, R. Taylor, A. Tylyshchak, “Double Bordered Constructions of Self-Dual Codes from Group Rings over Frobenius Rings ”, Cryptogr. Commun., vol. 12, pp. 769–784, 2020.

[39] J. Gildea, A. Kaya, R. Taylor, B. Yildiz, “Constructions for Self-Dual Codes induced from Group Rings ”, Finite Fields Appl., vol. 51, pp. 71–92, 2018.

[40] J. Gildea, A. Kaya, A. Tylyshchak, B. Yildiz, “A Modified Bordered Construction for Self-Dual Codes from Group Rings ”, J. Algebra Comb. Discrete Appl., vol. 7, no. 2, pp. 103–119, 2019.

[41] T.A. Gulliver, M. Harada “Weight Enumerators of Double Circulant Codes and New Extremal Self-Dual Codes ”, Des. Codes and Cryptogr., vol. 11, pp. 141–150, 1997.

[42] T.A. Gulliver, M. Harada, “Classification of Extremal Double Circulant Self-Dual Codes of Lengths 64 to 72 ”, Des. Codes and Cryptogr., vol. 13, pp. 257–269, 1998.

[43] T.A. Gulliver, M. Harada, “Classification of Extremal Double Circulant Self-Dual Codes of Lengths 74 to 88 ”, Discrete Math., vol. 306, pp. 2064–2072, 2006.

[44] T.A. Gulliver, M. Harada, H. Kaneta, “Classification of Extremal Double-Circulant Self-Dual Codes of Length up to 62 ”, Discrete Math., vol. 188, pp. 127–136, 1998.

[45] A. R. Hammonds Jr., P.V. Kumar, A. R. Calderbank, N.J.A. Sloane, P. Sole, “The $\mathbb{Z}_4$- linearity of Kerdock, Preparata, Goethals and related Codes ”IEEE Trans. Inform. Theory, vol. 40, pp. 301–319, 1994.

[46] A. R. Hammonds Jr., P.V. Kumar, A. R. Calderbank, N.J.A. Sloane, P. Sole, “On the Apparent Duality of the Kerdock and Preparata Codes ”, Applied algebra, algebraic algorithms and error-correcting codes, Lecture Notes in Comput. Sci., Springer, vol. 673, 1993.

[47] M. Harada, A. Munemasa, “Some Restrictions on Weight Enumerators of Singly Even Self-Dual Codes ”, IEEE Trans. Inform. Theory, vol. 52, pp. 1266–1269, 2006.

[48] J. Hefferon, “Linear Algebra ”, Third edition, http://joshua.smcvt.edu/linearalgebra.

[49] R. Hill, “A First Course in Coding Theory ”, Oxford Applied Mathematics and Computing Science Series, Clarendon Press, Oxford, 1986.

[50] W. Huffman, V. Pless, “Fundamentals of error-correcting codes ”, Cambridge University Press, Cambridge, 2003.

[51] T. Hurley, “Group Rings and Rings of Matrices ”, Int. Jour. Pure and Appl. Math, vol. 31, no. 3, pp. 319–335, 2006.

[52] Irwansyah, D. Suprijanto, “Structure of linear codes over the ring B_k”, Journal of Applied Mathematics and Computing, vol. 58, pp. 755–775, 2018.

[53] A. Kaveh, H. Rahami, “Block Circulant Matrices and Applications in Free Vibration Analysis of Cyclically Repetitive Structures ”, Acta Mechanica, vol. 217, pp. 51–62, 2011.

[54] A. Kaya, “New Extremal Binary Self-Dual Codes of Lengths 64 and 66 from R_2-Lifts ”, Finite Fields Appl., vol. 46, pp. 271–279, 2017.

[55] A. Kaya, B. Yildiz, “Various Constructions for Self-Dual Codes over Rings and New Binary Self-Dual Codes ”, Discrete Math., vol. 339, pp. 460–469, 2016.

[56] A. Korban, “Composite G- Codes over Formal Power Series Rings and Finite Chain Rings ”, J. Algebra Comb. Discrete Appl., DOI: 10.13069/jacodesmath.00000.

[57] C. W. H. Lam, “The Search for a Finite Projective Plane of order 10 ”, Amer. Math. Monthly, vol. 98, pp. 305–318, 1991.

[58] S. Ling, P. Sole, “Type II Codes over $\mathbb{F}_4 + u\mathbb{F}_4$ ”, European J. Combin., vol. 22, pp. 983–997, 2001.

[59] B. R. McDonald, “Finite Rings with Identity”, New York: Marcel Dekker, Inc, 1974.

[60] F. J. MacWilliams, “Combinatorial Problems of Elementary Group Theory ”, PhD. thesis, Harvard University, 1961.

[61] C.P. Milies, S. K. Sehgal, “An Introduction to Group Rings ”, Kluver, Dordrecht-Boston, London, 2002.

[62] E.M. Rains, “Shadow Bounds for Self-Dual Codes”, IEEE Trans. Inf. Theory, vol. 44, pp. 134–139, 1998.

[63] Y. Wang, F. Lu, W. Lu, “The Inverse of Bisymmetric Matrices ”, Linear and Multilinear Algebra, vol. 67, pp. 479–489, 2019.

[64] J. Wood, “Duality for modules over finite rings and applications to coding theory ”, Amer. J. Math., vol. 121, pp. 555–575, 1999.

[65] N. Yankov, D. Anev, “On the Self-Dual Codes with an Automorphism of Order 5 ”, Applicable Algebra in Engineering, Communication and Computing, vol. 32, pp. 97–111, 2021.

[66] N. Yankov, M. Ivanova, M. Gurel, M.H. Lee, “Self-Dual Codes with an Automorphism of order 11 ”, IEEE Trans. Inform. Theory, vol. 61, no. 3, pp. 1188–1193, 2015.

[67] N. Yankov, M. Ivanova, M. H. Lee, “Self-Dual Codes with an Automorphism of order 7 and s-Extremal Codes of Length 68 ”, Finite Fields Appl., vol. 51, pp. 17–30, 2018.