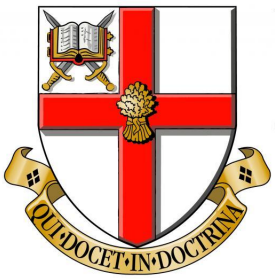

University of Chester

Group Rings: Units and Their Applications in Self-Dual Codes

Rhian Taylor

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

Supervisor: Dr. Joe Gildea

Department of Mathematical and Physical Sciences

March 2021

Contents

Abstract

The initial research presented in this thesis is the structure of the unit group of the group ring $C_n \times D_6$ over a field of characteristic 3 in terms of cyclic groups, specifically $\mathcal{U}(\mathbb{F}_{3^t}(C_n \times D_6))$. There are numerous applications of group rings, such as topology, geometry and algebraic K-theory, but more recently in coding theory. Following the initial work on establishing the unit group of a group ring, we take a closer look at the use of group rings in algebraic coding theory in order to construct self-dual and extremal self-dual codes.

Using a well established isomorphism between a group ring and a ring of matrices, we construct certain self-dual and formally self-dual codes over a finite commutative Frobenius ring. There is an interesting relationships between the Automorphism group of the code produced and the underlying group in the group ring. Building on the theory, we describe all possible group algebras that can be used to construct the well-known binary extended Golay code.

The double circulant construction is a well-known technique for constructing self-dual codes; combining this with the established isomorphism previously mentioned, we demonstrate a new technique for constructing self-dual codes. New theory states that under certain conditions, these self-dual codes correspond to unitary units in group rings. Currently, using methods discussed, we construct 10 new extremal self-dual codes of length 68.

In the search for new extremal self-dual codes, we establish a new technique which considers a double bordered construction. There are certain conditions where this new technique will produce self-dual codes, which are given in the theoretical results. Applying this new construction, we construct numerous new codes to verify the theoretical results; 1 new extremal self-dual code of length 64, 18 new codes of length 68 and 12 new extremal self-dual codes of length 80.

Using the well established isomorphism and the common four block construction, we consider a new technique in order to construct self-dual codes of length 68. There are certain conditions, stated in the theoretical results, which allow this construction to yield self-dual codes, and some interesting links between the group ring elements and the construction. From this technique, we construct 32 new extremal self-dual codes of length 68.

Lastly, we consider a unique construction as a combination of block circulant matrices and quadratic circulant matrices. Here, we provide theory surrounding this construction and conditions for full effectiveness of the method. Finally, we present the 52 new self-dual codes that result from this

method; 1 new self-dual code of length 66 and 51 new self-dual codes of length 68. Note that different weight enumerators are dependant on different values of β. In addition, for codes of length 68, the weight enumerator is also defined in terms of γ, and for codes of length 80, the weight enumerator is also defined in terms of α.

To highlight and summarise the new codes constructed in this thesis, a comprehensive list is shown below:

- **Code of length** 64**:** We were able to construct the following $[64, 32, 12]$ codes with new weight enumerator in $W_{64,2}$:
$$\beta = \{57\}.$$

- **Code of length** 66**:** We were able to construct the following extremal binary self-dual codes with new weight enumerators in $W_{66,3}$:
$$\beta = \{21\}.$$

- **Codes of length** 68**:** We were able to construct the following extremal binary self-dual codes with new weight enumerators in $W_{68,2}$:

$(\gamma = 0, \quad \beta = \{208, 214, 218\}),$
$(\gamma = 1, \quad \beta = \{179, 191, 193, 195, 197, 199, 202, 210, 211, 229\}),$
$(\gamma = 2, \quad \beta = \{61, 161, 163, 169, 171, 173, 191, 193, 195, 199, 204, 218\}),$
$(\gamma = 3, \quad \beta = \{163, 175, 177\}),$
$(\gamma = 4, \quad \beta = \{126, 129, 132, 144, 145, 146, 148, 155, 157, 161, 159, 175, 186, 191, 200\}),$
$(\gamma = 5, \quad \beta = \{182, 187, 189, 191, 193\}),$
$(\gamma = 6, \quad \beta = \{131, 134, 135\}),$
$(\gamma = 7, \quad \beta = \{142, 144, 145, 146, 148, 150, 152, 155, 156, 157, 158, 159, 160, 162, 164, 165, 167\})$
$(\gamma = 8, \quad \beta = \{153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167,$
$168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179\}).$
$(\gamma = 9, \quad \beta = \{169, 171, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185\}).$

- **Codes of length** 80**:** We were able to construct the following $[80, 40, 14]$ codes with new weight enumerators in $W_{80,2}$:

$(\beta = 18, \quad \alpha = \{-211, -229, -249, -256, -274, -287, -306, -310, -325, -355, -363, -401\}).$

Acknowledgements

Writing this thesis, I have received a great amount of support and feedback, I would like to thank the following people for making this thesis possible.

First and foremost, thank you to my supervisor, Dr Joe Gildea, for continued support and invaluable guidance throughout this thesis; it is with his encouragement through my undergraduate degree and Masters, that made this work possible.

I would also like to thank the following academics for their insight and knowledge; Prof Stephen Dougherty, Dr Abidin Kaya, Dr Alexander Tylyshchak and Prof Bahattin Yildiz. I am grateful for their valuable time that they have allocated to work on joint projects.

Finally, I would like to thank my parents for their continued encouragement, and my partner, Rory, for his motivation and support.

List of Symbols

$|G|$, the order of a group G,

$G \cap H$, the intersection of groups G and H,

$G \times H$, the external direct product of groups G and H,

$G.H$ or GH, the internal direct product of groups G and H,

$G \rtimes H$, the semidirect direct product of groups G and H,

G', the commutator subgroup of G,

$C_G(g)$, the centralizer of a group element g of a group G,

$N \lhd G$, N is a normal subgroup of a group G,

G/N, the factor group of N in G,

C_n, the cyclic group of order n,

D_{2n}, the dihedral group of order $2n$,

A_n, the alternating group of order n,

S_n, the symmetric group of order n,

$\mathbb{F}_{p^k}$, the Galois field of p^k elements,

$ker(\theta)$, the kernel of a group/ring homomorphism,

$M_n(R)$, the ring of $n \times n$ matrices over R,

$\mathbb{F}_{p^k}$, the Galois field of p^k elements,

RG, the group ring of G over R,

ϵ, the augmentation mapping of RG,

$\mathcal{U}(RG)$, the unit group of RG,

$ZD(RG)$, the zero divisors of RG,

$V(RG)$, the normalized unit group of RG.

Chapter 1

Introduction

This thesis is comprised of eight chapters in total. Firstly, we discuss the preliminaries required to understanding group rings and codes. The remaining six chapters consist of six pieces of work either submitted or accepted for publication, the details of which are outlined below.

Chapter 1: In the initial chapter, we present the definitions and theorems required as a basis to fully understanding subsequent chapters. Numerous theorems and definitions are given which we will refer back to throughout this thesis.

Chapter 2: In the second chapter, we establish the structure of the unit group of $C_n \times D_6$ over any finite field of characteristic 3 where C_n is the cyclic group of order n and D_6 is the dihedral group of order 6. This first piece of work was published in 2018, as joint work with my PhD supervisor, [46]. I made a considerable contribution to the theorems and proof presented in this paper, with the guidance of Joe Gildea. The focus of this chapter is group rings; in subsequent chapters, we explore a useful application of group rings in coding theory.

Chapter 3: Here, we describe codes that are ideals in a group ring called G-codes, where the ring is a finite commutative Frobenius ring and G is an arbitrary finite group. Notably, we prove that the dual of a G-code is also a G-code. We extend some theory on the construction of self-dual and formally self-dual codes and prove that our constructed codes must have an automorphism group that contains G as a subgroup. This theory is joint work with the help of Stephen Doughterty. We look at some common construction techniques for producing self-dual codes and prove that a certain method cannot produce the putative $[72, 36, 16]$ Type II code. Additionally, we show precisely which groups can be used to construct the extremal Type II codes of length 24. My main contribution to this paper included constructing the extended binary Golay code from certain ideals in group rings. The results presented in this chapter were published in 2018, as joint work with Stephen Dougherty, Alexander Tylyshchak and my PhD supervisor, Joe Gildea, [26].

Chapter 4: In this chapter, I worked with Abidin Kaya and Bahattin Yildiz, along with Joe Gildea. Here, we focus on establishing a stronger connection between group rings and self-dual codes, proving that a group ring element corresponds to a self-dual code if and only if it is a unitary

unit. Looking closer into the well-known double-circulant and four-circulant constructions, we show that the structures correspond to cyclic and dihedral groups, respectively. Using groups of order 8 and 16, we can see new methods for constructing self-dual codes, in addition to more familiar methods. The usefulness of these new construction methods are verified by the discovery of 10 new extremal binary self-dual codes of length 68, which were published in 2018, [44]. My main contribution to this paper includes the construction of self-dual codes coming from groups of order 8 and 16.

Chapter 5: As joint work with Abidin Kaya, Alexander Tylyshchak and Joe Gildea, we present a double bordered construction of self-dual codes from group rings. This is an extension of the well-established double circulant construction whose extensive use has had frequent results. The effectiveness of the new double bordered construction is proven for groups of order $2p$ where p is odd, over the rings $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$. Numerous new codes of length 64, 68 and 80, and their corresponding weight enumerators, are presented throughout the paper. In this chapter, I contributed significantly to the construction itself, as well as the following calculations and submitting the paper to Cryptography and Communications. The results from this chapter were published in 2020, [47].

Chapter 6: Continuing in the construction of self-dual codes, and working with the same authors as the previous chapter, we consider extending known construction methods. Here, we present a unique combination of 2×2 block circulant matrices, group rings and a reverse circulant matrix. There are certain conditions, proven in this chapter, for when this construction produces self-dual codes. After presenting the theory, we construct self-dual codes of various lengths over $\mathbb{F}_2$, $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$. My contribution to this chapter includes the construction itself, the main theory with the guidance of Alexander Tylyshchak, and the numerical results with the help of Abidin Kaya. In the search for new self-dual codes of length 68, using groups of order 4, 8 and 17, we use known methods for extensions, "neighbours of codes", and we extend this to so-called neighbours of neighbours. This results in the construction of 32 new self-dual codes which have been submitted for publication ([41]).

Chapter 7: Following the success of previous chapters, in constructing self-dual codes extending known construction methods, we consider combining block circulant matrices and block quadratic residue circulant matrices. Along with the authors from the previous chapter, and the addition of Bahattin Yildiz, we provide conditions for when this unique construction can yield self-dual codes. To verify the importance of this theory, we construct self-dual codes of various lengths over $\mathbb{F}_2$ and $\mathbb{F}_2 + u\mathbb{F}_2$. Again, we use extensions, neighbours and sequences of neighbours, in order to construct many new self-dual codes. My contribution to this paper includes the construction, theorems 7.1.1-7.2.2 and corresponding proofs. The numerical results were obtained collaboratively. Notably, we construct one new self-dual code of length 66 and 51 new self-dual codes of length 68. The theory and results presented in this chapter have been submitted for publication, ([42]).

Chapter 8: The final chapter is a conclusion of the work presented, the importance of the results and suggestions for future work. Here, we look back on the achievements of the project and criti-

cally examine what could have been done differently.

1.1 Group Rings

We now provide many definitions and results regarding group rings needed for Chapter 2.

Definition 1.1.1 ([90]) *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:

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

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

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

Definition 1.1.2 ([90]) *Let RG be the group ring of the group G over the ring R. The homomorphism $\varepsilon : RG \to R$ given by*

$$\varepsilon \left(\sum_{g \in G} a_g g \right) = \sum a_g$$

is called the ***augmentation mapping*** *of RG.*

Definition 1.1.3 ([90]) *Let RG be the group ring of the group G over the ring R. Then, we define*

$$V(RG) = \{ u \in \mathcal{U}(RG) \mid \varepsilon(u) = 1 \}$$

as the ***normalized*** *units of RG.*

Theorem 1.1.4 ([89]) *Let RG be the group ring of the group G over the ring R. Then,*

$$\mathcal{U}(RG) \cong \mathcal{U}(R) \times V(RG)$$

where $V(RG)$ are the normalized units of RG.

In order to present the following two important theorems, we need to define a **semisimple** ring.

Definition 1.1.5 ([16]) *A ring R is called left semisimple if it is a direct sum of minimal left ideals. Similarly, a ring R is called right semisimple if it is a direct sum of minimal right ideals.*

Theorem 1.1.6 ***(Wedderburn-Artin Theorem)*** ([90]) *R is a semisimple ring if and only if R can be decomposed as a direct sum of finitely many matrix rings over division rings. i.e.*

$$R \cong M_{n_1}(D_1) \oplus M_{n_2}(D_2) \oplus \cdots \oplus M_{n_s}(D_s)$$

where D_i is a division ring and $M_{n_i}(D_i)$ is the ring of $n_i \times n_i$ matrices over D_i.

Theorem 1.1.7 ***(Maschke's Theorem)***([90]) *Let G be a group and R be a ring. Then RG is semisimple if the following conditions hold:*

1. *R is semisimple*
2. *G is finite*
3. *$|G|$ is invertible in R.*

Corollary 1.1.8 ([90]) *Let G be a group and K be a field. Then KG is semisimple if and only if G is finite and the $char(K) \nmid |G|$.*

Theorem 1.1.9 ([90]) *Let G be a finite group and K be a finite field such that $char(K) \nmid |G|$. Then $KG \cong \oplus_{i=1}^{s} M_{n_i}(D_i)$ where D_i is a division ring containing K in its center and*

$$|G| = \sum_{i=1}^{s} (n_i^2 \cdot dim_k(D_i))$$

Definition 1.1.10 ([90]) *A field K is* ***algebraically closed*** *if it contains all of the roots of the polynomials in $K[x]$.*

Corollary 1.1.11 ([90]) *Let G be a finite group and K be an algebraically closed field, where $char(K) \nmid |G|$. Then,*

$$KG \cong \oplus_{i=1}^{s} M_{n_i}(K) \quad \text{and} \quad |G| = \sum_{i=1}^{2} n_i^2$$

Theorem 1.1.12 ([90]) *Let G be a finite group and K be a field such that $char(K) \nmid |G|$. Then*

$$KG \cong \oplus_{i=1}^{s} M_{n_i}(D_i) \cong K \oplus \oplus_{i=1}^{s-1} M_{n_i}(D_i)$$

i.e. the field itself appears at least once as a direct sum in the Wedderburn-Artin decomposition.

Lemma 1.1.13 ([90]) *Let K be a finite field. Then if $char(K) \nmid |G| < \infty$, then*

$$KG \cong \oplus_{i=1}^{s} M_{n_i}(K_i)$$

where K_i are fields.

Theorem 1.1.14 ([90]) *Let G be an abelian group of order n and K a field such that $char(K) \nmid n$. If K contains a primitive root of unity of order n then*

$$KG \cong \underbrace{K \oplus \cdots \oplus K}_{n}.$$

We now introduce a ring isomorphism from RG to a subring of $M_n(R)$. This isomorphism was constructed by Hurley in [60]. We begin by providing the details required to understand the implementation of this isomorphism. Given a particular element of a group ring, we can use this isomorphism to identify whether or not it is a unit or zero divisor.
We will now provide the necessary details. Given the elements of a group G, consider a fixed listing $G = \{g_1, g_2, \ldots, g_n\}$. Consider the following matrix of G, denoted $M(G)$ relative to its listing.

$$\begin{pmatrix} g_1^{-1}g_1 & g_1^{-1}g_2 & g_1^{-1}g_3 & \cdots & g_1^{-1}g_n \\ g_2^{-1}g_1 & g_2^{-1}g_2 & g_2^{-1}g_3 & \cdots & g_2^{-1}g_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_n^{-1}g_1 & g_n^{-1}g_2 & g_n^{-1}g_3 & \cdots & g_n^{-1}g_n \end{pmatrix}$$

In the matrix $M(G)$, every row and every column contains the elements of G in some order. Now, let $w = \sum_{i=1}^{n} a_{g_i} g_i \in RG$. Then $M(RG, w)$ can be defined as

$$\begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \alpha_{g_1^{-1}g_3} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \alpha_{g_2^{-1}g_3} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \alpha_{g_n^{-1}g_3} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix}$$

Theorem 1.1.15 ([60]) *Given a listing of the elements of a group G of order n, there is a bijective ring homomorphism between RG and the $n \times n$ G-matrices over R. This bijective ring homomorphism is given by $\sigma : w \mapsto M(RG, w)$.*

The next three results provide conditions when a group ring element is a unit or a zero divisor.

Theorem 1.1.16 ([60]) *Suppose R has an identity. Then $w \in RG$ is a unit in RG if and only if $\sigma(w)$ is a unit in $R_{n\times n}$.*

Corollary 1.1.17 ([60]) *When R is commutative, w is a unit in RG if and only if $\sigma(w)$ is a unit in $R_{n\times n}$ if and only if $det(\sigma(w))$ is a unit in R.*

Corollary 1.1.18 ([60]) *w is a zero divisor in RG if and only if $\sigma(w)$ is a zero divisor in $R_{n\times n}$.*

Note that $cir(a_1, a_2, \ldots, a_n)$ denotes a circulant matrix whose first row is $(a_1, a_2, \ldots, a_n)$, each row vector is rotated one element to the right relative to the preceding row vector. The notation $rcir(a_1, a_2, \ldots, a_n)$ denotes a reverse circulant matrix, where each row vector is rotated one element to the left. Furthermore, $CIR(A_1, A_2, \ldots, A_n)$ denotes a block circulant matrix whose first row of block matrices are $A_1, A_2, \ldots, A_n$.

1.2 Codes and Alphabets

Throughout this thesis (Chapter's 3-7), we construct codes over finite commutative Frobenius rings. First, we shall define a Frobenius ring. We will then define a code over such rings and provide many properties/results regarding codes needed for later chapters.

Definition 1.2.1 ([8]) *Suppose that R is a ring with identity. A left* **R-*module*** *M consists of an abelian group $(M, +)$ and an operation $\cdot : R \times M \to M$ such that:*

- $r \cdot (x + y) = r \cdot x + r \cdot y$,
- $(r + s) \cdot x = r \cdot x + s \cdot x$,
- $(rs) \cdot x = r \cdot (s \cdot x)$ *and*
- $1 \cdot x = x$

for all $x, y \in M$ and $r, s \in R$.

Definition 1.2.2 ([8]) *Let M and N be left modules over a ring R. Then, the function $f : M \to N$ is called an R-module homomorphism if:*

- $f(x + y) = f(x) + f(y)$ *for all $x, y \in M$ and*
- $f(rx) = rf(x)$ *for all $r \in R$ and $x \in M$*

The set of all module homomorphisms from M to N is denoted by $Hom_R(M, N)$. A left R-module is denoted ${}_RR$, and a right R-module is denoted R_R.

Definition 1.2.3 ([96]) *Let R be a finite ring. Then $\widehat{R} = Hom_{\mathbb{Z}}(R, \mathbb{C}^{\times})$ is called the* ***character module*** *of R.*

Definition 1.2.4 ([24]) *A finite ring is called* ***Frobenius*** *if:*

- *As a left module, $\widehat{R} \cong {}_RR$.*
- *As a right module, $\widehat{R} \cong R_R$.*

Definition 1.2.5 ([24]) *A* ***code*** *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 a* ***linear code****. If a code is a k-dimensional submodule of R^n, then the code is denoted as an $[n, k]$ linear code over R.*

Definition 1.2.6 ([24]) *Let C be a linear code over R. Then, the* ***orthogonal*** *of C is defined as:*

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

where $[\mathbf{v}, \mathbf{w}] = \sum v_i w_i$.

Definition 1.2.7 ([24]) *A code is said to be* ***self-orthogonal*** *if* $C \subseteq C^{\perp}$ *and* ***self-dual*** *if* $C = C^{\perp}$.

Definition 1.2.8 ([24]) *Two codes* C *and* C' *are* ***equivalent*** *if* C' *can be formed from* C *by permuting the coordinates of* C.

Definition 1.2.9 ([24]) *A code* C *is said to be* ***isodual*** *if* C *and* $C^{\perp}$ *are equivalent codes.*

([24])

Definition 1.2.10 *The* ***automorphism group*** *of a code* C*, denoted* $Aut(G)$*, consists of all permutations of the coordinates of the code that fix the code.*

Definition 1.2.11 ([24]) *Let* C *be a code over a ring* $R = \{a_0, a_1, \ldots, a_{r-1}\}$. *The* ***complete weight enumerator*** *for the code* C *is defined as:*

$$cwe_C(x_{a_0}, x_{a_1}, \ldots, x_{a_{r-1}}) = \sum_{\mathbf{c} \in C} \prod_{i=0}^{r-1} x_{a_i}^{n_i(\mathbf{c})} \tag{1.1}$$

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

Definition 1.2.12 ([24]) *The* ***Hamming weight*** *of a vector* $\mathbf{v} \in R^n$ *is* $wt_H(\mathbf{v}) = |\{i \mid v_i \neq 0\}|$.

Definition 1.2.13 ([24]) *The* ***minimum distance*** *of a code* C *over* R *is the minimum of all the hamming weights.*

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

Definition 1.2.14 ([90]) *The general weight enumerator of a code is defined to be the polynomial*

$$W_c(z) = \sum_{i=0}^{n} A_i z^i$$

where A_i *denotes the number of codewords in* C *of weight* i.

Definition 1.2.15 ([24]) *We say that a code is* ***formally self-dual*** *with respect to some weight enumerator if the code and its orthogonal have the same weight enumerator.*

Definition 1.2.16 ([24]) *A code is* ***isodual*** *if any weight enumerator for the code* C *is identical to the weight enumerator of its orthogonal.*

Lemma 1.2.17 ([24]) *If* C *is an isodual code then it is formally self-dual with respect to any weight enumerator.*

Lemma 1.2.18 ([24]) *A code* C *over a Frobenius ring* R *satisfies* $|C||C^{\perp}| = |R|^n$.

Definition 1.2.19 ([59]) *If the weights of all codewords in the self-dual code* C *are divisible by* 4*, then* C *is called a* ***Type II*** *(doubly even) code. Otherwise* C *is called a* ***Type I*** *(singly even) code.*

Binary self-dual codes have bounds on their minimum distances:

Theorem 1.2.20 ([91]) *Let $d_I(n)$ and $d_{II}(n)$ be the minimum distance of a Type I and Type II binary code of length n, respectively. Then*

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

and

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

Definition 1.2.21 ([59]) *Self-dual codes meeting these bounds are called* ***extremal****.*

We now introduce a new family of rings called R_k.

Definition 1.2.22 ([30–32]) *Define the ring R_k as*

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

These rings are local rings of characteristic 2 with maximal ideal $\mathfrak{m} = \langle u_1, u_2, \ldots, u_k \rangle$. This maximal ideal is also necessarily the Jacobson radical of the ring, which can be characterized as the intersection of all maximal ideals. The socle, which is the sum of all minimal ideals, for the ring R_k is $Soc(R_k) = \langle u_1 u_2 \cdots u_k \rangle = \mathfrak{m}^{\perp}$. We have that $|R_k| = 2^{2^k}$.

In general, a Gray map is a distance preserving map, but we will define a Gray map formally over R_k.

Definition 1.2.23 ([32]) *We define $\phi_1(a + bu_1) = (b, a + b)$, where ϕ maps R_1 to $\mathbb{F}_2^2$. Then view $R[u_1, u_2, \ldots, u_s]$ as $R[u_1, u_2, \ldots, u_{s-1}][u_s]$ and define $\phi_s(a + bu_s) = (b, a + b)$. Then the map ϕ_k is map from R_k to $\mathbb{F}_2^{2^k}$.*

Theorem 1.2.24 ([32]) *Let C be a self-dual code over R_k, then $\phi_k(C)$ is a self-dual code in $\mathbb{F}_2^{2^k}$.*

We now describe the ring $\mathbb{F}_4 + u\mathbb{F}_4$ and its connection to $\mathbb{F}_2 + u\mathbb{F}_2$ (R_1). Note that $\mathbb{F}_2 = \{0, 1\}$ and $\mathbb{F}_2 + u\mathbb{F}_2 = \{0, 1, u, 1 + u\}$. We also provide other Gray maps that allow us to go from $\mathbb{F}_4 + u\mathbb{F}_4$ to $\mathbb{F}_2 + u\mathbb{F}_2$. Note that $\omega, \overline{\omega} \in \mathbb{F}_4 + u\mathbb{F}_4$. We also give important results regarding these other Gray maps.

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 $\mathbb{F}_4 + u\mathbb{F}_4$ is defined via $u^2 = 0$. Note that $\mathbb{F}_4 + u\mathbb{F}_4$ can be viewed as an extension of $\mathbb{F}_2 + u\mathbb{F}_2$ and so we can describe any element of $\mathbb{F}_4 + u\mathbb{F}_4$ in the form $\omega a + \bar{\omega} b$ uniquely, where $a, b \in \mathbb{F}_2 + u\mathbb{F}_2$.

In [34] and [25] the following Gray maps were introduced;

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

Those were generalized to the following maps in [82];

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

These maps are distance preserving. The binary images $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ and $\psi_{\mathbb{F}_4} \circ \varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ are equivalent. The Lee weight of an element is defined to be the Hamming weight of its binary image.

Proposition 1.2.25 ([82]) *Let C be a code over $\mathbb{F}_4+u\mathbb{F}_4$. If C is self-orthogonal, so are $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ and $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$. C is a Type I (resp. Type II) code over $\mathbb{F}_4+u\mathbb{F}_4$ if and only if $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ is a Type I (resp. Type II) $\mathbb{F}_4$-code, if and only if $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ is a Type I (resp. Type II) $\mathbb{F}_2+u\mathbb{F}_2$-code. Furthermore, the minimum Lee weight of C is the same as the minimum Lee weight of $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ and $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$.*

Corollary 1.2.26 ([82]) *Suppose that C is a self-dual code over $\mathbb{F}_4+u\mathbb{F}_4$ of length n and minimum Lee distance d. Then $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ is a binary $[4n, 2n, d]$ self-dual code. Moreover, C and $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ have the same weight enumerator. If C is Type I (Type II), then so is $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$.*

Theorem 1.2.27 ([29]) *Let R be a finite Frobenius ring with the property that there exists $c \in R$ such that $c^2 = -1$. Let $G = (\mathbf{r}_i)$ be a generator matrix of a self-dual code C over R of even length n, where $\mathbf{r}_i$ are the row vectors of the matrix G respectively for $1 \le i \le k$. Let $\mathbf{x} = (x_1, ..., x_n)$ be a vector in R^n such that $[\mathbf{x}, \mathbf{x}] = -1$ in R. Suppose $\mathbf{y}_i = [\mathbf{x}, \mathbf{r}_i]$ for $1 \le i \le k$. Then 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 C over R of length $n+2$.

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

$$\begin{aligned} 0 &\leftrightarrow 0000,\ 1 \leftrightarrow 0001,\ 2 \leftrightarrow 0010,\ 3 \leftrightarrow 0011, \\ 4 &\leftrightarrow 0100,\ 5 \leftrightarrow 0101,\ 6 \leftrightarrow 0110,\ 7 \leftrightarrow 0111, \\ 8 &\leftrightarrow 1000,\ 9 \leftrightarrow 1001,\ A \leftrightarrow 1010,\ B \leftrightarrow 1011, \\ C &\leftrightarrow 1100,\ D \leftrightarrow 1101,\ E \leftrightarrow 1110,\ F \leftrightarrow 1111. \end{aligned}$$

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.

Finally, we define k-range neighbours as we will use this definition to construct new extremal binary self-dual codes. Two self-dual binary codes of dimension k are said to be neighbours if their intersection has dimension $k-1$.

Definition 1.2.28 ([90]) *Let $\mathcal{N}_{(0)}$ be a binary self-dual code of length $2n$. Let $x_0 \in \mathbb{F}_2^{2n} \setminus \mathcal{N}_{(0)}$, define*

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

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

Chapter 2

The Structure of $\mathcal{U}(\mathbb{F}_{3^t}(C_n \times D_6))$

Group rings have been a topic of increasing interest since their introduction by Higman in the 1940s, [58]. In particular, units of group rings have been studied extensively by many authors such as [11, 12, 19, 58, 66, 88], to name a few. By 1992, numerous units of group rings had been presented, which allowed conjectures to be formulated and hypotheses to be tested, [93].

Despite the extensive research in the area growing, it is still relatively difficult to establish the structure of the unit group of a group ring, especially in terms of the group or the ring. To date, the best known result relating the structure of the unit group of a group ring regarding the underlying ring is $\mathcal{U}(RG) \cong \mathcal{U}(R) \times V(RG)$ where $V(RG)$ is the normalized unit group of RG, [89].

When the characteristic of the ring doesn't divide the order of the group, there exist many useful results that can be used to find the decomposition of the group ring and hence the structure of the unit group (see section 1.1). However, when the characteristic of the ring divides the order of the group, very little is known in terms of techniques for establishing the structure of the unit group.

It is well known that if F is a field of characteristic p and G is a finite p group, then, $V(FG)$ is a finite p-group of order $|F|^{|G|-1}$. In [92], a basis for $V(\mathbb{F}_p G)$ was established where $\mathbb{F}_p$ is the Galois field of p elements and G is a finite abelian p-group.

In terms of group algebras, numerous unit groups have been established for small cases of dihedral groups, alternating groups and symmetric groups; the structures of the unit groups of order 6, 12, 18 and 24 over fields of characteristic 3, have been shown in numerous papers, [21, 36, 45, 81, 94, 95]. In [78], the unit group of $\mathbb{F}_2 D_{2p}$ is constructed where p is an odd prime. In [79], the order of $\mathcal{U}(\mathbb{F}_{2^k}(G \ltimes C_{2^n}))$ is determined in terms of the order of $\mathcal{U}(RG)$ for any finite group, G.

In this chapter, we continue this line of research in establishing the structure of the unit group of a group algebra where the characteristic of the ring divides the order of the group. In [21, 36, 45] respectively, the structures of $\mathcal{U}(\mathbb{F}_{3^k} D_6)$, $\mathcal{U}(\mathbb{F}_{3^k} D_{12})$ and $\mathcal{U}(\mathbb{F}_{3^k}(C_3 \times D_6))$ were established. In this chapter, we extend the techniques used in these papers to determine the structure of $\mathcal{U}(\mathbb{F}_{3^k}(C_n \times D_6))$. This chapter is joint work with my supervisor, Joe Gildea, and the results are published in [46].

From here, we provide numerous individual results and calculations in order to prove our main results. However, first we will begin by stating our main result, Theorem 2.0.4:

$$\mathcal{U}(\mathbb{F}_{3^t}(C_n \times D_6)) \cong (C_3^{3nt} \rtimes C_3^{nt}) \rtimes \mathcal{U}(\mathbb{F}_{3^t}(C_2 \times C_n))$$

and Corollary 2.0.5:

$$\mathcal{U}(\mathbb{F}_{3^t}(C_n \times D_6)) \cong \begin{cases} (C_3^{3nt} \rtimes C_3^{nt}) \rtimes C_{3^t-1}^{2n} & \text{if } n|(3^t-1) \\ (C_3^{3nt} \rtimes C_3^{nt}) \rtimes \left(C_3^{2f_1(V)} \times C_{3^2}^{2f_2(V)} \times \cdots \times C_{3^m}^{2f_m(V)} \times C_{3^m-1}^2\right) & \text{if } n = 3^m \end{cases}$$

where $f_i(V) = t(|{C_{3^m}}^{3^{i-1}}| - 2|{C_{3^m}}^{3^i}| + |{C_{3^m}}^{3^{i+1}}|)$.

Firstly, let $C'_{2p} = \langle x \mid x^{2p} = 1 \rangle$ and

$$v = \sum_{i=0}^{p-1} \sum_{j=0}^{1} \alpha_{i+pj+1} x^{2i+j} \in RC'_{2p}$$

then,

$$\sigma(v) = \begin{pmatrix} A_1 & A_2 \\ A'_2 & A_1 \end{pmatrix}$$

where $A_j = cir(\alpha_{(j-1)p+1}, \alpha_{(j-1)p+2}, \ldots, \alpha_{jp})$ and $A'_j = cir(\alpha_{jp}, \alpha_{(j-1)p+1}, \ldots, \alpha_{jp-1})$.

Alternatively, let $D_{2p} = \langle x, y \mid x^p = y^2 = 1, x^y = y^{-1} \rangle$ and

$$v = \sum_{i=0}^{p-1} \sum_{j=0}^{1} \alpha_{i+pj+1} x^i y^j \in RD_{2p}$$

then,

$$\sigma(v) = \begin{pmatrix} A_1 & A_2 \\ A_2^T & A_1^T \end{pmatrix}$$

where $A_j = cir(\alpha_{(j-1)p+1}, \alpha_{(j-1)p+2}, \ldots, \alpha_{jp})$.

Let $G = C_n \times D_6 = \langle x, y, z \,|\, x^3 = y^2 = z^n = 1, x^y = x^{-1}, xz = zx, yz = zy \rangle$ where $n \geq 1$. The natural group homomorphism $G \longrightarrow G/\langle x \rangle$ extends linearly to the algebra homomorphism $\theta : \mathbb{F}_{3^t}(C_n \times D_6) \longrightarrow \mathbb{F}_{3^t}(C_2 \times C_n)$ where

$$\sum_{i=1}^{3} x^{i-1}(\alpha_i + \alpha_{i+3}z + \cdots + \alpha_{i+3n}z^{n-1} + \alpha_{i+3n+3}y + \alpha_{i+3n+6}yz + \cdots + \alpha_{i+6n}yz^{n-1}) \mapsto$$

$$\sum_{i=1}^{4} (\alpha_i + \alpha_{i+3}b + \cdots + \alpha_{i+3n}b^{n-1} + \alpha_{i+3n+3}a + \alpha_{i+3n+6}ab + \cdots + \alpha_{i+6n}ab^{n-1})$$

and $C_2 \times C_n = \langle a, b \,|\, a^2 = b^{n-1} = 1,\, ab = ba \rangle$. If we restrict θ to $\mathcal{U}(\mathbb{F}_{3^t}(C_n \times D_6))$, we can construct the group epimorphism $\theta' : \mathcal{U}(\mathbb{F}_{3^t}(C_n \times D_6)) \longrightarrow \mathcal{U}(\mathbb{F}_{3^t}(C_2 \times C_n))$. Consider the group homomorphism $\psi : \mathcal{U}(\mathbb{F}_{3^t}(C_2 \times C_n)) \longrightarrow \mathcal{U}(\mathbb{F}_{3^t}(C_n \times D_6))$ by

$$\begin{aligned}\gamma_1+\gamma_2 b + \cdots + \gamma_n b^{n-1} + \delta_1 a + \delta_2 ab + \cdots + \delta_n ab^{n-1} \mapsto \\ \gamma_1 + \gamma_2 z + \cdots + \gamma_n z^{n-1} + \delta_1 y + \delta_2 yz + \cdots + \delta_n yz^{n-1}\end{aligned}$$

where $\gamma_i, \delta_j \in \mathbb{F}_{3^t}$. Clearly, $\theta' \circ \psi$ is the identity map of $\mathcal{U}(\mathbb{F}_{2^k}(C_2 \times C_n))$. Therefore $\mathcal{U}(\mathbb{F}_{3^t}(C_n \times D_6))$ is a split extension of $\mathcal{U}(\mathbb{F}_{3^t}(C_2 \times C_n))$ by $ker(\theta')$ and $\mathcal{U}(\mathbb{F}_{3^t}(C_n \times D_6)) \cong H \rtimes \mathcal{U}(\mathbb{F}_{3^t}(C_2 \times C_n))$ where $H \cong ker(\theta')$.

Clearly, we have expressed $\mathcal{U}(\mathbb{F}_{3^t}(C_n \times D_6))$ in terms of H and $\mathcal{U}(\mathbb{F}_{3^t}(C_2 \times C_n))$. Now, we will concentrate on establishing the structure of H; we can show it has exponent 3, and we will express H as a semidirect product of two abelian subgroups of H.

Lemma 2.0.1 *H has exponent 3.*

Proof. Let $h = 1 + \sum_{j=1}^{n} \mathfrak{A}_j + \sum_{k=1}^{n} \mathfrak{B}_k y \in H$ where

$$\mathfrak{A}_j = \sum_{i=1}^{2} \alpha_{i+2(j-1)} z^{j-1}(x^i - 1) \text{ and } \mathfrak{B}_k = \sum_{i=1}^{2} \alpha_{i+2(k+n-1)} z^{k-1}(x^i - 1)$$

$\alpha_j \in \mathbb{F}_{3^t}$. Then

$$\begin{aligned} h^2 &= \left(1 + \sum_{j=1}^{n} \mathfrak{A}_j + \sum_{k=1}^{n} \mathfrak{B}_k y\right)^2 \\ &= 1 + 2\sum_{j=1}^{n} \mathfrak{A}_j + 2\sum_{k=1}^{n} \mathfrak{B}_k y + \sum_{j=1}^{n}\sum_{k=1}^{n} \mathfrak{A}_j \mathfrak{A}_k \\ &+ \sum_{j=1}^{n}\sum_{k=1}^{n} \mathfrak{A}_j \mathfrak{B}_k y + \sum_{j=1}^{n}\sum_{k=1}^{n} \mathfrak{B}_j y \mathfrak{A}_k + \sum_{j=1}^{n}\sum_{k=1}^{n} \mathfrak{B}_j y \mathfrak{B}_k y \\ &= 1 + 2\sum_{j=1}^{n} \mathfrak{A}_j + 2\sum_{k=1}^{n} \mathfrak{B}_k y \\ &+ \sum_{j=1}^{n}\sum_{k=1}^{n} (\mathfrak{A}_j \mathfrak{A}_k + \mathfrak{B}_j \mathfrak{B}'_k) + \sum_{j=1}^{n}\sum_{k=1}^{n} (\mathfrak{A}_j \mathfrak{B}_k + \mathfrak{B}_j \mathfrak{A}'_k) y \end{aligned}$$

where $y\mathfrak{A}_k = \mathfrak{A}'_k y$ and $y\mathfrak{B}_k = \mathfrak{B}'_k y$.

Firstly, note that,

$$\begin{aligned}(x-1)^2 &= (x-1)(x-1)\\ &= x^2-2x+1\\ &= x^2+x+1=\hat{x}\\ (x^2-1)^2 &= (x^2-1)(x^2-1)\\ &= x^4-2x^2+1\\ &= x+x^2+1=\hat{x}\\ \text{and } (x-1)(x^2-1) &= (x^2-1)(x-1)\\ &= x^3-x^2-x+1\\ &= 1-x^2-x+1\\ &= 2x^2+2x+2=2\hat{x}\end{aligned}$$

Now

$$\begin{aligned}\mathfrak{A}_j\mathfrak{A}_k &= (z^{j-1}(\alpha_{2j-1}(x-1)+\alpha_{2j}(x^2-1))(z^{k-1}(\alpha_{2k-1}(x-1)+\alpha_{2k}(x^2-1))\\ &= z^{j+k-2}(\alpha_{2j-1}\alpha_{2k-1}(x-1)^2+\alpha_{2j-1}\alpha_{2k}(x-1)(x^2-1)\\ &+\alpha_{2j}\alpha_{2k-1}(x^2-1)(x-1)+\alpha_{2j}\alpha_{2k}(x^2-1)^2)\\ &= z^{j+k-2}(\alpha_{2j-1}\alpha_{2k-1}\hat{x}+2\alpha_{2j-1}\alpha_{2k}\hat{x}+2\alpha_{2j}\alpha_{2k-1}\hat{x}+\alpha_{2j}\alpha_{2k}\hat{x})\\ &= z^{j+k-2}((\alpha_{2j-1}\alpha_{2k-1}+\alpha_{2j}\alpha_{2k})+2(\alpha_{2j-1}\alpha_{2k}+\alpha_{2j}\alpha_{2k-1}))\hat{x},\end{aligned}$$

$$\begin{aligned}\mathfrak{B}_j\mathfrak{B}'_k &= \mathfrak{B}_j y\mathfrak{B}_k y\\ &= (z^{j-1}(\alpha_{2j+2n-1}(x-1)+\alpha_{2j+2n}(x^2-1))(z^{k-1}(\alpha_{2k-1}(x-1)+\alpha_{2k}(x^2-1))\\ &= z^{j+k-2}(\alpha_{2j+2n-1}(x-1)+\alpha_{2j+2n}(x^2-1))(\alpha_{2k-1}(x-1)+\alpha_{2k}(x^2-1))\\ &= z^{j+k-2}(\alpha_{2j+2n-1}\alpha_{2k-1}(x-1)^2+\alpha_{2j+2n-1}\alpha_{2k}(x-1)(x^2-1)\\ &+\alpha_{2j+2n}\alpha_{2k-1}(x^2-1)(x-1)+\alpha_{2j+2n}\alpha_{2k}(x^2-1)^2)\\ &= z^{j+k-2}(\alpha_{2j+2n-1}\alpha_{2k-1}\hat{x}+\alpha_{2j+2n-1}\alpha_{2k}2\hat{x}+\alpha_{2j+2n}\alpha_{2k-1}2\hat{x}+\alpha_{2j+2n}\alpha_{2k}\hat{x}\\ &= z^{j+k-2}((\alpha_{2j+2n-1}\alpha_{2k+2n}+\alpha_{2j+2n}\alpha_{2k+2n-1})+2(\alpha_{2j+2n-1}\alpha_{2k+2n-1}+\alpha_{2j+2n}\alpha_{2k+2n}))\hat{x},\end{aligned}$$

$$\begin{aligned}\mathfrak{A}_j\mathfrak{B}_k &= (z^{j-1}(\alpha_{2j-1}(x-1)+\alpha_{2j}(x^2-1))(z^{k-1}(\alpha_{2k+2n-1}(x-1)+\alpha_{2k+2n}(x^2-1))\\ &= z^{j+k-2}(\alpha_{2j-1}(x-1)+\alpha_{2j}(x^2-1))(\alpha_{2k+2n-1}(x-1)+\alpha_{2k+2n}(x^2-1))\\ &= z^{j+k-2}(\alpha_{2j-1}\alpha_{2k+2n-1}(x-1)^2+\alpha_{2j-1}\alpha_{2k+2n}(x-1)(x^2-1)\\ &+\alpha_{2j}\alpha_{2k+2n-1}(x^2-1)(x-1)+\alpha_{2j}\alpha_{2k+2n}(x^2-1)^2)\\ &= z^{j+k-2}(\alpha_{2j-1}\alpha_{2k+2n-1}\hat{x}+\alpha_{2j-1}\alpha_{2k+2n}2\hat{x}+\alpha_{2j}\alpha_{2k+2n-1}2\hat{x}+\alpha_{2j}\alpha_{2k+2n}\hat{x}\\ &= z^{j+k-2}((\alpha_{2j-1}\alpha_{2k+2n-1}+\alpha_{2j}\alpha_{2k+2n})+2(\alpha_{2j-1}\alpha_{2k+2n}+\alpha_{2j}\alpha_{2k+2n-1}))\hat{x},\end{aligned}$$

and

$$\begin{aligned}
\mathfrak{B}_j\mathfrak{A}'_k &= \mathfrak{B}_j y\mathfrak{A}_k \\
&= (z^{j-1}(\alpha_{2j+2n-1}(x-1)+\alpha_{2j+2n}(x^2-1))(z^{k-1}(\alpha_{2k-1}(x-1)+\alpha_{2k}(x^2-1)) \\
&= z^{j+k-2}(\alpha_{2j+2n-1}(x-1)+\alpha_{2j+2n}(x^2-1)(\alpha_{2k-1}(x-1)+\alpha_{2k}(x^2-1) \\
&= z^{j+k-2}(\alpha_{2j+2n-1}\alpha_{2k-1}(x-1)^2+\alpha_{2j+2n-1}\alpha_{2k}(x-1)(x^2-1) \\
&+ \alpha_{2j+2n}\alpha_{2k-1}(x^2-1)(x-1)+\alpha_{2j+2n}\alpha_{2k}(x^2-1)^2 \\
&= z^{j+k-2}(\alpha_{2j+2n-1}\alpha_{2k-1}\hat{x}+\alpha_{2j+2n-1}\alpha_{2k}2\hat{x}+\alpha_{2j+2n}\alpha_{2k-1}2\hat{x}+\alpha_{2j+2n}\alpha_{2k}\hat{x} \\
&= z^{j+k-2}((\alpha_{2j+2n-1}\alpha_{2k}+\alpha_{2j+2n-1}\alpha_{2k-1})+2(\alpha_{2j+2n-1}\alpha_{2k-1}+\alpha_{2j+2n}\alpha_{2k}))\hat{x}.
\end{aligned}$$

Therefore, $\sum_{j=1}^{n}\sum_{k=1}^{n}(\mathfrak{A}_j\mathfrak{A}_k+\mathfrak{B}_j\mathfrak{B}'_k)+\sum_{j=1}^{n}\sum_{k=1}^{n}(\mathfrak{A}_j\mathfrak{B}_k+\mathfrak{B}_j\mathfrak{A}'_k)y$ takes the form $\hat{x}(\gamma_1+\gamma_2 y)$ where $\gamma_1,\gamma_2 \in \mathbb{F}_{3^t}$. Now,

$$\begin{aligned}
h^3 &= \left(1+2\sum_{j=1}^{n}\mathfrak{A}_j+2\sum_{k=1}^{n}\mathfrak{B}_k y+\hat{x}(\gamma_1+\gamma_2 y)\right)\left(1+2\sum_{j=1}^{n}\mathfrak{A}_j+2\sum_{k=1}^{n}\mathfrak{B}_k y\right) \\
&= 1+3\sum_{j=1}^{n}\mathfrak{A}_j+3\sum_{k=1}^{n}\mathfrak{B}_k y+2\left(\sum_{j=1}^{n}\sum_{k=1}^{n}(\mathfrak{A}_j\mathfrak{A}_k+\mathfrak{B}_j\mathfrak{B}'_k)+\sum_{j=1}^{n}\sum_{k=1}^{n}(\mathfrak{A}_j\mathfrak{B}_k+\mathfrak{B}_j\mathfrak{A}'_k)y\right) \\
&+ \hat{x}(\gamma_1+\gamma_2 y)+\hat{x}(\gamma_1+\gamma_2 y)\sum_{j=1}^{n}\mathfrak{A}_j+\hat{x}(\gamma_1+\gamma_2 y)\sum_{k=1}^{n}\mathfrak{B}_k y \\
&= 1+2(\hat{x}(\gamma_1+\gamma_2 y))+\hat{x}(\gamma_1+\gamma_2 y)+\hat{x}(\gamma_1+\gamma_2 y)\sum_{j=1}^{n}\mathfrak{A}_j+\hat{x}(\gamma_1+\gamma_2 y)\sum_{k=1}^{n}\mathfrak{B}_k y \\
&= 1+\hat{x}(\gamma_1+\gamma_2 y)\sum_{j=1}^{n}\mathfrak{A}_j+\hat{x}(\gamma_1+\gamma_2 y)\sum_{k=1}^{n}\mathfrak{B}_k y.
\end{aligned}$$

Clearly $\hat{x}\mathfrak{A}_j=\hat{x}\sum_{i=1}^{2}\alpha_{i+2(j-1)}z^{j-1}(x^i-1)=\sum_{i=1}^{2}\alpha_{i+2(j-1)}z^{j-1}(\hat{x}-\hat{x})=0$, $\hat{x}(\gamma_1+\gamma_2 y)\sum_{j=1}^{n}\mathfrak{A}_j=0$ and $\hat{x}(\gamma_1+\gamma_2 y)\sum_{k=1}^{n}\mathfrak{B}_k y=0$. Therefore H has exponent 3. ■

The first abelian subgroup of H that we construct is $C_H(x)$, where $C_H(x)$ is the centralizer of x in H. As the exponent of H is 3 and $C_H(x)$ is abelian, $C_H(x)$ is an abelian 3-group.

Lemma 2.0.2 *$C_H(x)\cong C_3^{3nt}$.*

Proof. Clearly $C_H(x) = \{h \in H \mid xh = hx\}$. Let $h = 1 + \sum_{j=1}^{n} \mathfrak{A}_j + \sum_{k=1}^{n} \mathfrak{B}_k y \in H$ where

$$\mathfrak{A}_j = \sum_{i=1}^{2} \alpha_{i+2(j-1)} z^{j-1}(x^i - 1) \text{ and } \mathfrak{B}_k = \sum_{i=1}^{2} \alpha_{i+2(k+n-1)} z^{k-1}(x^i - 1)$$

and $\alpha_j \in \mathbb{F}_{2^t}$. Now

$$\begin{aligned} xh - hx &= x\left(1 + \sum_{j=1}^{n} \mathfrak{A}_j + \sum_{k=1}^{n} \mathfrak{B}_k y\right) - \left(1 + \sum_{j=1}^{n} \mathfrak{A}_j + \sum_{k=1}^{n} \mathfrak{B}_k y\right) x \\ &= x\left(\sum_{k=1}^{n} \mathfrak{B}_k y\right) - \left(\sum_{k=1}^{n} \mathfrak{B}_k y\right) x. \end{aligned}$$

Now,

$$\begin{aligned} x\mathfrak{B}_k y - \mathfrak{B}_k yx &= z^{k-1}[(\alpha_{2j+2n-1}(x^2 - x) + \alpha_{2j+2n}(1 - x)) - (\alpha_{2j+2n-1}(1 - x^2) + \alpha_{2j+2n}(x - x^2))]y \\ &= \hat{x}yz^{k-1}(\alpha_{2j+2n} - \alpha_{2j+2n-1}). \end{aligned}$$

Therefore, every element of $C_H(x)$ takes the form

$$1 + \sum_{j=1}^{n} \mathfrak{A}_j + \sum_{l=1}^{n} \alpha_{l+2n} \hat{x} y z^{l-1}$$

where $\mathfrak{A}_j = \sum_{i=1}^{2} \alpha_{i+2(j-1)} z^{j-1}(x^i - 1)$ and $\alpha_i \in \mathbb{F}_{2^t}$. Clearly, $(\hat{x})^2 = 3\hat{x} = 0$ and $\hat{x}\mathfrak{A}_j = \mathfrak{A}_j \hat{x}$. Therefore $C_H(x)$ is an abelian group of order $3^{2nt} \cdot 3^{nt} = 3^{3nt}$. ■

The next subgroup that we construct is also an abelian 3-group. We define it element-wise as follows:

Lemma 2.0.3 *Let S be the subgroup of H where the elements of H take the form:*

$$1 + \sum_{j=1}^{n} \mathfrak{R}_j$$

consisting of $\mathfrak{R}_j = \sum_{i=1}^{2} i r_j x^i (1 + y) z^{j-1}$ and $r_i \in \mathbb{F}_{3^t}$. Then $S \cong C_3^{nt}$.

Proof. Let $s_1 = 1 + \sum_{j=1}^{n} \mathfrak{R}_j \in S$ and $s_2 = 1 + \sum_{j=1}^{n} \mathfrak{T}_j \in S$ where $\mathfrak{R}_j = \sum_{i=1}^{2} i r_j x^i (1+y) z^{j-1}$, $\mathfrak{T}_j = \sum_{i=1}^{2} i t_j x^i (1+y) z^{j-1}$ and $r_i, t_j \in \mathbb{F}_{3^t}$. Now

$$\begin{aligned} s_1 s_2 &= \left(1 + \sum_{j=1}^{n} \mathfrak{R}_j\right)\left(1 + \sum_{j=1}^{n} \mathfrak{T}_j\right) \\ &= 1 + \sum_{j=1}^{n} (\mathfrak{R}_j + \mathfrak{T}_j) + \left(\sum_{j=1}^{n} \mathfrak{R}_j\right)\left(\sum_{j=1}^{n} \mathfrak{T}_j\right) \end{aligned}$$

and

$$\begin{aligned} \mathfrak{R}_j \mathfrak{T}_k &= \left(\sum_{i=1}^{2} i r_j x^i (1+y) z^{j-1}\right)\left(\sum_{i=1}^{2} i t_k x^i (1+y) z^{k-1}\right) \\ &= (r_j x + r_j xy + 2r_j x^2 + 2r_j x^2 y)(t_k x + t_k xy + 2t_k x^2 + 2t_k x^2 y) z^{j+k-2} \\ &= r_j t_k (9 + 9y + 6x + 6xy + 3x^2 + 3x^2 y) z^{j+k-2} \\ &= \sum_{i=1}^{3} (12 - 3i) r_j t_k x^{i-1} (1+y) z^{j+k-2} \\ &= 0. \end{aligned}$$

Clearly $s_1 s_2 \in S$ and S is abelian, therefore $S \cong C_3^{nt}$. ■

We are now in a position to describe the structure of H in terms of the semidirect product of abelain 3-groups.

Theorem 2.0.4

$$\mathcal{U}(\mathbb{F}_{3^t}(C_n \times D_6)) \cong (C_3^{3nt} \rtimes C_3^{nt}) \rtimes \mathcal{U}(\mathbb{F}_{3^t}(C_2 \times C_n))$$

Proof. Let $c = 1 + \sum_{j=1}^{n} \mathfrak{A}_j + \sum_{l=1}^{n} \alpha_{l+2n} \hat{x} y z^{l-1} \in C_H(x)$ and $s = 1 + \sum_{j=1}^{n} \mathfrak{R}_j \in S$ where $\mathfrak{A}_j = \sum_{i=1}^{2} \alpha_{i+2(j-1)} z^{j-1}(x^i - 1)$, $\mathfrak{R}_j = \sum_{i=1}^{2} i r_j x^i (1+y) z^{j-1}$ and $\alpha_i, r_j \in \mathbb{F}_{3^t}$. Now

$$\begin{aligned} c^s &= s^2 c s \\ &= \left(1 + \sum_{j=1}^{n} \mathfrak{R}_j\right)^2 \left(1 + \sum_{j=1}^{n} \mathfrak{A}_j + \sum_{l=1}^{n} \alpha_{l+2n} \hat{x} y z^{l-1}\right)\left(1 + \sum_{j=1}^{n} \mathfrak{R}_j\right) \\ &= \left(1 + 2\sum_{j=1}^{n} \mathfrak{R}_j\right)\left(1 + \sum_{j=1}^{n} \mathfrak{A}_j + \sum_{l=1}^{n} \alpha_{l+2n} \hat{x} y z^{l-1}\right)\left(1 + \sum_{j=1}^{n} \mathfrak{R}_j\right). \end{aligned}$$

Now ${\mathfrak{R}_j}^2 = 0$ and $\hat{x}\mathfrak{R}_j = 3\hat{x}r_j(1+y)z^{j-1} = 0 = \mathfrak{R}_j\hat{x}$, therefore

$$c^s = 1 + \sum_{j=1}^{n}\mathfrak{A}_j + \sum_{l=1}^{n}\alpha_{l+2n}\hat{x}yz^{l-1} + 2\left(\sum_{j=1}^{n}\mathfrak{R}_j\right)\left(\sum_{j=1}^{n}\mathfrak{A}_j\right) + \left(\sum_{j=1}^{n}\mathfrak{A}_j\right)\left(\sum_{j=1}^{n}\mathfrak{R}_j\right)$$
$$+ 2\left(\sum_{j=1}^{n}\mathfrak{R}_j\right)\left(\sum_{j=1}^{n}\mathfrak{A}_j\right)\left(\sum_{j=1}^{n}\mathfrak{R}_j\right).$$

Now, $\mathfrak{R}_j\mathfrak{A}_k = r_j(\alpha_{2k} - \alpha_{2k-1})\hat{x}(1-y)z^{j+k-2}$, $\mathfrak{A}_k\mathfrak{R}_j = r_j(\alpha_{2k} - \alpha_{2k-1})\hat{x}(1+y)z^{j+k-2}$ and

$$\begin{aligned} 2\mathfrak{R}_j\mathfrak{A}_k + \mathfrak{A}_k\mathfrak{R}_j &= r_j(\alpha_{2k} - \alpha_{2k-1})\hat{x}[2(1-y) + (1+y)]z^{j+k-2} \\ &= r_j(\alpha_{2k-1} - \alpha_{2k})\hat{x}yz^{j+k-2}. \end{aligned}$$

Additionally, $\mathfrak{R}_j\mathfrak{A}_k\mathfrak{R}_j = 0$ since $\hat{x}\mathfrak{R}_j = 0$. Therefore $c^s \in C_H(x)$ and consequently $C_H(x)$ is a normal subgroup of H. Finally, $C_H(x) \cap S = \{1\}$, $H = C_H(x).S$ and $H \cong C_H(x) \rtimes S \cong C_3^{3nt} \rtimes C_3^{nt}$. ■

It remains to establish the structure of $\mathcal{U}(\mathbb{F}_{3^t}(C_2 \times C_n))$.

Corollary 2.0.5

$$\mathcal{U}(\mathbb{F}_{3^t}(C_n \times D_6)) \cong \begin{cases} (C_3^{3nt} \rtimes C_3^{nt}) \rtimes C_{3^t-1}^{2n} & \text{if } n|(3^t-1) \\ (C_3^{3nt} \rtimes C_3^{nt}) \rtimes \left(C_3^{2f_1(V)} \times C_{3^2}^{2f_2(V)} \times \cdots \times C_{3^m}^{2f_m(V)} \times C_{3^m-1}^2\right) & \text{if } n = 3^m \end{cases}$$

where $f_i(V) = t(|{C_{3^m}}^{3^{i-1}}| - 2|{C_{3^m}}^{3^i}| + |{C_{3^m}}^{3^{i+1}}|)$.

Proof. It is well known ([92]) that

$$\mathbb{F}_{3^t}(C_2 \times C_n) \cong (\mathbb{F}_{3^t}C_2)C_n \cong (\mathbb{F}_{3^t} \oplus \mathbb{F}_{3^t})C_n \cong \mathbb{F}_{3^t}C_n \oplus \mathbb{F}_{3^t}C_n.$$

If $n|(3^t-1)$, then $\mathbb{F}_{3^t}C_n \cong \oplus_{i=1}^{n}\mathbb{F}_{3^t}$ by Corollary 3.5.6 in [90]. Therefore, $\mathcal{U}(\mathbb{F}_{3^t}(C_2 \times C_n)) \cong C_{3^t-1}^{2n}$ when $n|(3^t-1)$. When $n = 3^m$, the number of cyclic groups $f_i(V)$ of order 3^i in the direct product of $V(\mathbb{F}_{3^t}G)$ is

$$f_i(V) = t(|{C_{3^m}}^{3^{i-1}}| - 2|{C_{3^m}}^{3^i}| + |{C_{3^m}}^{3^{i+1}}|).$$

■

Chapter 3

Constructions of Self-Dual and Formally Self-Dual Codes from Group Rings

It is a well known fact that certain ideals in Group Rings correspond to certain linear block codes. In [13], it was shown that the Reed-Muller codes can be constructed from certain ideals of the group algebra of 2-groups over a finite field of characteristic 2. Furthermore, in [14], it was shown that certain ideals of the group algebra of p-groups over a field that contained a p^{th}-root of unity, correspond to MDS-codes. A useful collation of known results on error-correcting codes which are ideals in group algebras have been constructed by Kelarev and Solé, [80].

In 1990, the famous extended binary Golay code was constructed from an ideal of the group algebra $\mathbb{F}_2S_4$ where S_4 is the symmetric group on 4 elements, [15]. In 2006, a certain isomorphism from a group ring to a certain subring of the $n \times n$ matrices was established [60]; a representation of RG expressed in the basis G. Later, this isomorphism was used to construct the extended binary Golay code and the famous $[48, 24, 12]$ code from the group algebras $\mathbb{F}_2D_{24}$ and $\mathbb{F}_2D_{48}$ where D_{24} and D_{48} are the dihedral groups of orders 24 and 48, [84, 85]. Today, this established isomorphism is used, under certain conditions, to construct self-dual and quantum codes. In particular, three essential conditions are provided for when group rings can be used to construct self-dual codes.

In this chapter, we describe G-codes, which are ideals in a group ring of a finite group G, over a finite commutative Frobenius ring. We prove that the dual of a G-code is also a code. Building on the work of Hurley [61], we show that one of the three conditions that is required for construction self-dual codes from group rings in unnecessary. We show that several of the standard constructions of self-dual codes are found within our general framework, and we prove that our constructed codes must have an automorphism group that contains G as a subgroup. Here, we also prove that a common construction technique for producing self-dual codes cannot produce the putative [72, 36, 16] Type II code. Furthermore, we produce formally self-dual codes over a finite commutative Frobenius ring. Finally, we conclude this chapter with establishing which group algebras ($\mathbb{F}_2G$ where $|G| = 24$) can be used to construct the extended binary Golay code. This chapter is joint work and the results are published in [26].

3.1 Codes and Ideals

We shall consider codes that are ideals inside of a group ring, where the ring is the alphabet of the code and assume that the ring is a finite commutative Frobenius ring. For a given element $v \in RG$ (where R is a Frobenius commutative ring and G is a group), we define the following code over the ring R:

$$C(v) = \langle \sigma(v) \rangle, \tag{3.1}$$

where σ is defined in Theorem 1.1.15. Namely, the code is formed by taking the row space of $\sigma(v)$ over the ring R where $\sigma(v)$ is the previously described map in [60].

We shall now show that the codes we construct are actually ideals in the group ring. We use this to get information about the automorphism group of the constructed code.

Theorem 3.1.1 *Let R be a finite commutative Frobenius ring and G a finite group of order n. Let $v \in RG$ and let $C(v)$ 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 $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in C(v)$. Then $I(v)$ is a left ideal in RG.*

Proof. The rows of $\sigma(v)$ consist precisely of the vectors that correspond to the elements hv in RG where h is any element of G. The sum of any two elements in $I(v)$ corresponds exactly to the sum of the corresponding elements in $C(v)$ and so $I(v)$ is closed under addition.

Let $w_1 = \sum \beta_i g_i \in RG$. Then if w_2 corresponds to a vector in $C(v)$, it is of the form $\sum \gamma_j h_j v$. Then $w_1 w_2 = \sum \beta_i g_i \sum \gamma_i h_i v = \sum \beta_i \gamma_j g_i h_j v$ which corresponds to an element in $C(v)$ and gives that the element is in $I(v)$. Therefore $I(v)$ is a left ideal of RG. ■

Example 3.1.2 *Let $v = 1 + ba + ba^2 + ba^3 \in \mathbb{F}_2 D_8$ where $\langle a, b \rangle \cong D_8$. Then $\sigma(v) = \begin{pmatrix} 1&0&0&0&0&1&1&1 \\ 0&1&0&0&1&1&1&0 \\ 0&0&1&0&1&1&0&1 \\ 0&0&0&1&1&0&1&1 \\ 0&1&1&1&1&0&0&0 \\ 1&1&1&0&0&1&0&0 \\ 1&1&0&1&0&0&1&0 \\ 1&0&1&1&0&0&0&1 \end{pmatrix}$ and $\sigma(v)$ is equivalent to $A = \begin{pmatrix} 1&0&0&0&0&1&1&1 \\ 0&1&0&0&1&1&1&0 \\ 0&0&1&0&1&1&0&1 \\ 0&0&0&1&1&0&1&1 \end{pmatrix}$. Clearly $C(v) = \langle \sigma(v) \rangle$ is the $[8, 4, 4]$ extended Hamming code. Let $v_1 = 1 + ba + ba^2 + ba^3 \in \mathbb{F}_2 D_8$, $v_2 = 1 + b + ba + ba^2 \in \mathbb{F}_2 D_8$, $v_3 = 1 + b + ba + ba^3 \in \mathbb{F}_2 D_8$ and $v_4 = 1 + b + ba^2 + ba^3 \in \mathbb{F}_2 D_8$ where v_i are the group ring elements corresponding to the rows of A. Let $I(v) = \left\{ \sum_{i=1}^{4} \alpha_i v_i | \alpha_i \in \mathbb{F}_2 \right\}$. Then $I(v)$ is a left ideal of $\mathbb{F}_2 D_8$ and in particular $I(v)$ is the left principle ideal of $\mathbb{F}_2 D_8$ generated by v.*

Corollary 3.1.3 *Let R be a finite commutative Frobenius ring and G a finite group of order n. Let $v \in RG$ and let $C(v)$ be the corresponding code in R^n. Then the automorphism group of $C(v)$ has a subgroup isomorphic to 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 G. It follows immediately that the automorphism group of $C(v)$ contains G as a subgroup. ■

We note that our construction gives a natural generalization of cyclic codes since cyclic codes are ideals in RC_n where C_n is the cyclic group of order n. Cyclic codes are held invariant by the cyclic shift, whereas our codes are held invariant by the action of the group G on the coordinates. Moreover, this is the strength of our construction technique. Specifically, we can construct a code whose automorphism group must contain a given group. In this sense, when the group used is G, we can refer to a code that is an ideal in RG as G-codes, where G is replaced by the name of the code when known. Therefore, classically we can say cyclic codes, but we can now say dihedral codes or dicyclic codes. When something applies to any group we can still say G-codes. It is immediate that a code of length n can only be a G-code for some G if it has a subgroup of its automorphism group of order n.

Example 3.1.4 *Let C be the extremal $[48, 24, 12]$ Pless symmetry code. The automorphism group of this code is $PSL(2, 47)$. A computation in GAP [97] shows that the only subgroup of $PSL(2, 47)$ of order 48 is D_{48}. Hence the only possible construction of this code by our technique must have $G = D_{48}$. This construction is given by McLoughlin in [85]. This gives that the Pless symmetry code is, in fact, a dihedral code.*

Combining the results in [4], [6], [10], [86], [87] and [99], we have that the automorphism group of a putative $[72, 36, 16]$ code must have order 1,2, 3, 4, or 5. Since it is impossible for a group of order 72 to satisfy these we have the following corollary.

Corollary 3.1.5 *The putative $[72, 36, 16]$ code cannot be of the form $C(v)$ for any $v \in \mathbb{F}_2 G$ for any group G.*

Proof. The result follows immediately from Corollary 3.1.3 and the previous discussion. ■

Note that a code whose automorphism group is trivial cannot be constructed by this technique.

One of the fundamental results about cyclic codes is that the orthogonal of a cyclic code is again a cyclic code. In this subsection, we generalize this results to codes that are ideals in a group ring. That is, we show that if C is a G-code for some G then its orthogonal $C^{\perp}$ is also a G-code.

Let I be an ideal in a group ring RG. Define $\mathcal{R}(C) = \{w \mid vw = 0, \forall v \in I\}$. It is immediate that $\mathcal{R}(I)$ is an ideal of RG. Let $v = a_{g_1}g_1 + a_{g_2}g_2 + \ldots a_{g_n}g_n \in RG$ and $C(v)$ be the corresponding code. Let $\Psi : RG \to R^n$ be the canonical map that sends $a_{g_1}g_1 + a_{g_2}g_2 + \ldots a_{g_n}g_n$ to $(a_{g_1}, a_{g_2}, \ldots, a_{g_n})$. Let I be the ideal $\Psi^{-1}(C)$, and let $\mathbf{w} = (w_1, w_2, \ldots, w_n) \in C^{\perp}$. Then

$$[(a_{g_j^{-1}g_1}, a_{g_j^{-1}g_2}, \ldots, a_{g_j^{-1}g_n}), (w_1, w_2, \ldots, w_n)] = 0, \forall j. \tag{3.2}$$

This gives

$$\sum_{i=1}^{n} a_{g_j^{-1}g_i} w_i = 0, \ \forall j. \tag{3.3}$$

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

$$b_{g_i} = w_{g_i^{-1}}. \tag{3.4}$$

Then

$$\sum_{i=1}^{n} a_{g_j^{-1}g_i} w_i = 0 \implies \sum_{i=1}^{n} a_{g_j^{-1}g_i} b_{g_i^{-1}} = 0. \tag{3.5}$$

Then $g_j^{-1}g_i g_i^{-1} = g_j^{-1}$, hence this is the coefficient of g_j^{-1} in the product of $\overline{\mathbf{w}}$ and $g_j^{-1}v$. This gives that $\overline{\mathbf{w}} \in \mathcal{R}(I)$ if and only if $\mathbf{w} \in C^{\perp}$.

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

Theorem 3.1.6 *Let $C = C(v)$ be a code in RG formed from the vector $v \in RG$. Then $\Psi^{-1}(C^{\perp})$ is an ideal of RG.*

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

The following is a rephrasing, in more general terms, of Theorem 1 in [60] where R is assumed to be a finite commutative Frobenius ring. The proof is identical and simply consists of showing that addition and multiplication is preserved.

Theorem 3.1.7 *Let R be a finite commutative Frobenius ring and let G be a group of order n. Then the map $\sigma : RG \to M_n(R)$ is an injective ring homomorphism.*

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. Note that involution is defined as a function or operator that is equal to its inverse, and therefore gives the identity when applied to itself. The reason this notation is used in this setting will be apparent by the next lemma.

Lemma 3.1.8 *Let R be a finite commutative Frobenius ring and let G be a group of order n. For an element $v \in RG$, we have that $\sigma(v)^T = \sigma(v^T)$.*

Proof. The ij-th element of $\sigma(v^T)$ is $\alpha_{(g_i^{-1}g_j)^{-1}} = \alpha_{g_j^{-1}g_i}$ which is the ji-th element of $\sigma(v)$. ■

Next, we give our first result about the structure of our constructed codes.

Lemma 3.1.9 *Let R be a finite commutative Frobenius ring and let G be a group of order n. If $v = v^T$ and $v^2 = 0$ then $C(v)$ is a self-orthogonal code.*

Proof. If $v = v^T$ then $\sigma(v)^T = \sigma(v^T)$ by Lemma 3.1.8. Then we have that $(\sigma(v)\sigma(v))_{ij}$ is the inner-product of the i-th and j-th rows of $\sigma(v)$. Since $v^2 = 0$, by Theorem 3.1.7 we have that $\sigma(v)\sigma(v) = \mathbf{0}$. This gives that any two rows of $\sigma(v)$ are orthogonal and hence they generate a self-orthogonal code. ■

We can now use this lemma to construct self-dual codes. For codes over fields we could simply use the dimension of $\sigma(v)$, however over an arbitrary Frobenius ring, we cannot determine the size of the generated code simply from the rank of the matrix. Therefore, we have the following theorem.

Theorem 3.1.10 *Let R be a finite commutative Frobenius ring and G be a group of order n, with v an element in RG. If $v = v^T$, $v^2 = 0$ and $|C_v| = |R|^{\frac{n}{2}}$ then C_v is a self-dual code.*

Proof. By Lemma 3.1.9 the code C_v is self-orthogonal and since $|C_v| = |R|^{\frac{n}{2}}$ we have that C_v is self-dual. ■

Notice that unlike the field case we are not assuming that n is even. For example, let $R = R_k$ and G be the trivial group of size 1 with $v = u_i e_G$ where e_G is the identity of the group. Then $\sigma(v) = (u_i)$ and C_v is a self-dual code of length 1.

In the following example, we show the strength of this construction by constructing a code over R_1 using the alternating group on 4 elements, which has an image under the associated Gray map of the length 24 extended Golay code.

Example 3.1.11 *We shall use the previous results to construct the binary Golay code from the ring R_1. Let $v = u(b + ab + ac + bc^2) + (bc + bc^2) + (1 + u)(c^2 + abc^2) \in R_1A_4$. Then, C_v is a self-dual code of length 12 over R_1. Hence $\phi_k(C)$ is a binary self-dual code of length 12 by Theorem 1.2.24. The binary code $\phi_k(C)$ has a generator matrix of the following form:* $\begin{pmatrix} I_{12} & A \end{pmatrix}$ *where* $A = \begin{pmatrix} 1&0&1&1&0&0&1&0&1&1&0&1 \\ 1&1&1&0&0&1&1&0&1&0&1&0 \\ 1&1&1&1&1&0&0&0&0&1&1&0 \\ 1&0&1&0&1&0&0&1&1&0&1&1 \\ 1&0&0&1&1&1&1&0&0&0&1&1 \\ 1&1&0&0&1&1&0&0&1&1&0&1 \\ 1&1&0&1&0&1&1&1&0&1&0&0 \\ 0&1&1&0&1&0&1&1&1&1&0&0 \\ 0&1&0&1&1&1&0&1&1&0&1&0 \\ 0&0&1&1&1&1&0&1&0&1&0&1 \\ 0&1&1&1&0&0&1&1&0&0&1&1 \\ 0&0&0&0&0&1&1&1&1&1&1&1 \end{pmatrix}$. *It is a simple computation to see that $\phi_k(C_v)$ is the $[24, 12, 8]$ Golay code.*

Lemma 3.1.12 *Let R be a finite commutative Frobenius ring and let G be a group of order n. If $v = \sum \alpha_i g_i$ and $w = \alpha_i g_i h$ for some $h \in G$ then C_v and C_w are equivalent codes.*

Proof. The generator matrix for C_w is formed from the generator matrix of C_v by permuting the columns corresponding to multiplication of the elements of G by h. Hence, the codes are equivalent. ■

Example 3.1.13 *Let $v_1 = 1 + xz + yz + xyz \in \mathbb{F}_2(C_2 \times C_2 \times C_2)$ where $\langle x, y, z\rangle \cong C_2 \times C_2 \times C_2$. Now $\sigma(v_1)$ is equivalent to* $\begin{pmatrix} 1&0&0&0&0&1&1&1 \\ 0&1&0&0&1&0&1&1 \\ 0&0&1&0&1&1&0&1 \\ 0&0&0&1&1&1&1&0 \end{pmatrix}$. *The code $C(v_1)$ is the the $[8, 4, 4]$ extended Hamming code. Next, let us consider $v_2 = (1 + xz + yz + xyz)y = y + xz + z + xyz \in \mathbb{F}_2(C_2 \times C_2 \times C_2)$. Then $\sigma(v_2)$ is equivalent to* $\begin{pmatrix} 1&0&0&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1 \\ 0&0&1&1&0&1&1&0 \\ 0&0&0&0&1&1&1&1 \end{pmatrix}$. *Clearly $C(v_1)$ is equivalent to $C(v_2)$.*

3.2 The Extended Binary Golay Code

Next, we consider constructing the extended binary Golay code from certain group algebras. We shall now consider constructions of the $[24, 12, 8]$ binary Golay code from $\mathbb{F}_2G$ for various groups G.

It is well known that the automorphism group of the $[24, 12, 8]$ code is the Mathieu group M_{24}. Therefore, the only possible groups that can work for our construction are

$$SL(2,3),\ S_4,\ D_{24},\ (C_6 \times C_2) \rtimes C_2, C_3 \times D_8, C_2 \times A_4 \text{ and } C_2^2 \times D_6.^1$$

Initially, it was shown in [15] that the $[24, 12, 8]$ code could be constructed from ideals in the group algebra $\mathbb{F}_2 S_4$ where S_4 is the symmetric group on 4 elements. In [84], the $[24, 12, 8]$ code was constructed from $\mathbb{F}_2 D_{24}$. We shall now separately consider the remaining cases.

3.2.1 The Group $C_3 \times D_8$

We begin by considering the group $C_3 \times D_8$. Let v be the element

$$v = \sum_{i=1}^{4} [a^{i-1}(\alpha_i + \alpha_{i+4}z + \alpha_{i+8}z^2) + ba^{i-1}(\alpha_{i+12} + \alpha_{i+16}z + \alpha_{i+20}z^2)] \in \mathbb{F}_2(C_3 \times D_8)$$

where $\langle z \rangle = C_3$, $\langle a, b \rangle = D_8$ and $\alpha_i \in \mathbb{F}_2$. Now

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

where $A = \begin{pmatrix} A_1 & A_2 & A_3 \\ A_3 & A_1 & A_2 \\ A_2 & A_3 & A_1 \end{pmatrix}$, $B = \begin{pmatrix} B_1 & B_2 & B_3 \\ B_3 & B_1 & B_2 \\ B_2 & B_3 & B_1 \end{pmatrix}$,

$$\begin{aligned} A_1 &= cir(\alpha_1, \alpha_2, \alpha_3, \alpha_4), \\ A_2 &= cir(\alpha_5, \alpha_6, \alpha_7, \alpha_8), \\ A_3 &= cir(\alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12}), \\ B_1 &= rcir(\alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha_{16}), \\ B_2 &= rcir(\alpha_{17}, \alpha_{18}, \alpha_{19}, \alpha_{20}), \\ B_3 &= rcir(\alpha_{21}, \alpha_{22}, \alpha_{23}, \alpha_{24}) \end{aligned}$$

and $cir(\alpha_1, \alpha_2, \ldots, \alpha_n)$, $rcir(\alpha_1, \alpha_2, \ldots, \alpha_n)$ are circulant and reverse circulant matrices respectively and $\alpha_1, \alpha_2, \ldots, \alpha_n$ is the first row of the respective matrices. Clearly $\langle \sigma(v) \rangle$ is self-dual if $\sigma(v)^T = \sigma(v)$. Now, $\sigma(v)^T = \sigma(v)$ if and only if $a_2 = a_4$, $a_5 = a_9$, $a_6 = a_{12}$, $a_7 = a_{11}$, $a_8 = a_{10}$, $a_{17} = a_{21}$, $a_{18} = a_{22}$, $a_{19} = a_{23}$ and $a_{20} = a_{24}$. Next, consider elements of $\mathbb{F}_2(C_3 \times D_8)$ of the form

$$\begin{aligned} &\{\, \alpha_1 + \alpha_2(a + a^3) + \alpha_3 a^2 + \alpha_4(z + z^2) + \alpha_5 az(1 + a^2 z) + \alpha_6 a^2 z(1 + z) + \alpha_7 az(a^2 + z) \\ &\quad + \sum_{i=1}^{4} b(\alpha_{i+7} + \alpha_{i+11}(z + z^2))a^{i-1} \mid \alpha_i \in \mathbb{F}_2 \,\} \end{aligned}$$

[1] These groups are SmallGroup(24,i) for $i \in \{3, 6, 8, 10, 12, 13, 14\}$ according to the GAP system [97].

and in particular the element $v_1 = 1 + b[(\hat{a}+1) + (1+a)(\hat{z}+1)]$ of this set where $\hat{a} = \sum_{i=0}^{3} a^i$ and $\hat{z} = \sum_{i=0}^{2} z^i$. The matrix $\sigma(v_1)$ is equivalent to

$$\begin{pmatrix} I & A \\ A & I \end{pmatrix}$$

where

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

It is a small computation to see that $C(v_1)$ is the $[24, 12, 8]$ code. The full calculation using Magma is given in Appendix A.1. Moreover, it can be shown that the above set contains 128 elements that generate the $[24, 12, 8]$ code.

3.2.2 The Group $C_2 \times A_4$

Next we consider the group $C_2 \times A_4$. Let v be the element

$$\begin{aligned} v = &\sum_{i=1}^{3} (\alpha_{4i-3} + \alpha_{4i-2}a + \alpha_{4i-1}b + \alpha_{4i}ab + \alpha_{4i+9}x + \alpha_{4i+10}xa + \alpha_{4i+11}xb + \alpha_{4i+21}xab)c^{i-1} \\ &\in \mathbb{F}_2(C_2 \times A_4) \end{aligned}$$

where $\langle x \rangle = C_2$, $a = (1,2)(3,4)$, $b = (1,3)(2,4)$ and $c = (1,2,3)$ and $\alpha_i \in \mathbb{F}_2$. Now

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

where $A = \begin{pmatrix} A_2 & A_2 & A_3 \\ A_4 & A_5 & A_6 \\ A_7 & A_8 & A_9 \end{pmatrix}$, $B = \begin{pmatrix} B_2 & B_2 & B_3 \\ B_4 & B_5 & B_6 \\ B_7 & B_8 & B_9 \end{pmatrix}$,
$A_1 = bc(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, $A_2 = bc(\alpha_5, \alpha_6, \alpha_7, \alpha_8)$, $A_3 = bc(\alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12})$,
$A_4 = bc(\alpha_9, \alpha_{12}, \alpha_{10}, \alpha_{11})$, $A_5 = bc(\alpha_1, \alpha_4, \alpha_2, \alpha_3)$, $A_6 = bc(\alpha_5, \alpha_8, \alpha_6, \alpha_7)$,
$A_7 = bc(\alpha_5, \alpha_7, \alpha_8, \alpha_6)$, $A_8 = bc(\alpha_9, \alpha_{11}, \alpha_{12}, \alpha_{10})$, $A_9 = bc(\alpha_1, \alpha_3, \alpha_4, \alpha_2)$,
$B_1 = bc(\alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha_{16})$, $B_2 = bc(\alpha_{17}, \alpha_{18}, \alpha_{19}, \alpha_{20})$, $B_3 = bc(\alpha_{21}, \alpha_{22}, \alpha_{23}, \alpha_{24})$,
$B_4 = bc(\alpha_{21}, \alpha_{24}, \alpha_{22}, \alpha_{23})$, $B_5 = bc(\alpha_{13}, \alpha_{16}, \alpha_{14}, \alpha_{15})$, $B_6 = bc(\alpha_{17}, \alpha_{20}, \alpha_{18}, \alpha_{19})$,
$B_7 = bc(\alpha_{17}, \alpha_{19}, \alpha_{20}, \alpha_{18})$, $B_8 = bc(\alpha_{21}, \alpha_{23}, \alpha_{24}, \alpha_{22})$ and $B_9 = bc(\alpha_{13}, \alpha_{15}, \alpha_{16}, \alpha_{14})$
where $bc(a, b, c, d)$ is a matrix that takes the form $\begin{pmatrix} a&b&c&d \\ b&a&d&c \\ c&d&a&b \\ d&c&b&a \end{pmatrix}$. Now, $\sigma(v) = \sigma(v)^T$ if and only if $a_5 = a_9$, $a_6 = a_{12}$, $a_7 = a_{10}$, $a_8 = a_{11}$, $a_{17} = a_{21}$, $a_{18} = a_{24}$, $a_{19} = a_{24}$ and $a_{20} = a_{23}$. Next, consider elements of $\mathbb{F}_2(C_2 \times A_4)$ of the form

$$\begin{aligned} \{ \sum_{i=0}^{1} x^i ((&\alpha_{8i+1} + \alpha_{8i+2}a + \alpha_{8i+3}b + \alpha_{8i+4}ab) + \\ &(\alpha_{8i+5} + \alpha_{8i+6}a + \alpha_{8i+7}b + \alpha_{8i+8}ab)(c + c^2)) \mid \alpha_i \in \mathbb{F}_2 \}, \end{aligned}$$

and in particular the element $v_1 = 1 + x(1 + b(1 + a)(1 + c^2)) + xa(1 + b)c$ of this set. The matrix $\sigma(v_1)$ is equivalent to

$$\begin{pmatrix} I & A \\ A & I \end{pmatrix}$$

where

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

It is a small computation to see that $C(v_1)$ is the $[24, 12, 8]$ code. Moreover, it can be shown that the above set contains 384 elements that generate the $[24, 12, 8]$ code.

3.2.3 The Group $(C_6 \times C_2) \rtimes C_2$

Next we consider the group $G = (C_6 \times C_2) \rtimes C_2$. Let v be the element

$$\begin{aligned} v = &\sum_{i=1}^{4} (\alpha_i y^{i-1} + \alpha_{i+4} x y^{i-1} + \alpha_{i+8} x^2 y^{i-1} + \alpha_{i+12} y^{i-1} z + \alpha_{i+16} x y^{i-1} z + \alpha_{i+20} x^2 y^{i-1} z) \\ &\in \mathbb{F}_2((C_6 \times C_2) \rtimes C_2) \end{aligned}$$

where $(C_6 \times C_2) \rtimes C_2 = \langle x, y, z \,|\, x^3 = y^4 = z^2 = 1,\ xy = yx^2,\ xz = zx,\ yz = zy^3 \rangle$ and $\alpha_i \in \mathbb{F}_2$. Now,

$$\sigma(v) = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \alpha_9 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_{13} & \alpha_{14} & \alpha_{15} & \alpha_{16} & \alpha_{17} & \alpha_{18} & \alpha_{19} & \alpha_{20} & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} \\ \alpha_2 & \alpha_1 & \alpha_{13} & \alpha_{10} & \alpha_{14} & \alpha_{12} & \alpha_9 & \alpha_{18} & \alpha_7 & \alpha_4 & \alpha_{24} & \alpha_6 & \alpha_3 & \alpha_5 & \alpha_{17} & \alpha_{22} & \alpha_{15} & \alpha_8 & \alpha_{21} & \alpha_{23} & \alpha_{19} & \alpha_{16} & \alpha_{20} & \alpha_{11} \\ \alpha_3 & \alpha_{13} & \alpha_1 & \alpha_{14} & \alpha_{10} & \alpha_{16} & \alpha_{17} & \alpha_{23} & \alpha_{15} & \alpha_5 & \alpha_{21} & \alpha_{22} & \alpha_2 & \alpha_4 & \alpha_9 & \alpha_6 & \alpha_7 & \alpha_{20} & \alpha_{24} & \alpha_{18} & \alpha_{11} & \alpha_{12} & \alpha_8 & \alpha_{19} \\ \alpha_{14} & \alpha_{10} & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_7 & \alpha_{16} & \alpha_{24} & \alpha_{12} & \alpha_{13} & \alpha_{18} & \alpha_{15} & \alpha_5 & \alpha_3 & \alpha_{22} & \alpha_{17} & \alpha_6 & \alpha_{21} & \alpha_8 & \alpha_{11} & \alpha_{20} & \alpha_9 & \alpha_{19} & \alpha_{23} \\ \alpha_5 & \alpha_4 & \alpha_{10} & \alpha_2 & \alpha_1 & \alpha_9 & \alpha_{22} & \alpha_{11} & \alpha_6 & \alpha_3 & \alpha_8 & \alpha_{17} & \alpha_{14} & \alpha_{13} & \alpha_{16} & \alpha_{15} & \alpha_{12} & \alpha_{19} & \alpha_{18} & \alpha_{24} & \alpha_{23} & \alpha_7 & \alpha_{21} & \alpha_{20} \\ \alpha_{24} & \alpha_{11} & \alpha_{19} & \alpha_{17} & \alpha_9 & \alpha_1 & \alpha_8 & \alpha_4 & \alpha_{18} & \alpha_{15} & \alpha_{22} & \alpha_2 & \alpha_{21} & \alpha_7 & \alpha_{20} & \alpha_3 & \alpha_{23} & \alpha_{10} & \alpha_6 & \alpha_5 & \alpha_{12} & \alpha_{13} & \alpha_{14} & \alpha_{16} \\ \alpha_{17} & \alpha_9 & \alpha_7 & \alpha_{19} & \alpha_{21} & \alpha_{23} & \alpha_1 & \alpha_6 & \alpha_{13} & \alpha_{11} & \alpha_5 & \alpha_{18} & \alpha_{15} & \alpha_{24} & \alpha_2 & \alpha_8 & \alpha_3 & \alpha_{22} & \alpha_{14} & \alpha_{12} & \alpha_{10} & \alpha_{20} & \alpha_{16} & \alpha_4 \\ \alpha_{23} & \alpha_{18} & \alpha_8 & \alpha_6 & \alpha_{12} & \alpha_{14} & \alpha_{24} & \alpha_1 & \alpha_{21} & \alpha_{22} & \alpha_9 & \alpha_{10} & \alpha_{20} & \alpha_{16} & \alpha_{11} & \alpha_4 & \alpha_{19} & \alpha_{13} & \alpha_7 & \alpha_2 & \alpha_{15} & \alpha_5 & \alpha_3 & \alpha_{17} \\ \alpha_9 & \alpha_{17} & \alpha_{15} & \alpha_{11} & \alpha_{24} & \alpha_{18} & \alpha_{13} & \alpha_{22} & \alpha_1 & \alpha_{19} & \alpha_4 & \alpha_{23} & \alpha_7 & \alpha_{21} & \alpha_3 & \alpha_{20} & \alpha_2 & \alpha_6 & \alpha_{10} & \alpha_{16} & \alpha_{14} & \alpha_8 & \alpha_{12} & \alpha_5 \\ \alpha_{10} & \alpha_{14} & \alpha_5 & \alpha_{13} & \alpha_3 & \alpha_{15} & \alpha_{12} & \alpha_{21} & \alpha_{16} & \alpha_1 & \alpha_{23} & \alpha_7 & \alpha_4 & \alpha_2 & \alpha_6 & \alpha_9 & \alpha_{22} & \alpha_{24} & \alpha_{20} & \alpha_{19} & \alpha_8 & \alpha_{17} & \alpha_{11} & \alpha_{18} \\ \alpha_{12} & \alpha_6 & \alpha_{22} & \alpha_{18} & \alpha_{23} & \alpha_{21} & \alpha_5 & \alpha_9 & \alpha_{14} & \alpha_8 & \alpha_1 & \alpha_{19} & \alpha_{16} & \alpha_{20} & \alpha_4 & \alpha_{11} & \alpha_{10} & \alpha_7 & \alpha_{13} & \alpha_{17} & \alpha_3 & \alpha_{24} & \alpha_{15} & \alpha_2 \\ \alpha_{11} & \alpha_{24} & \alpha_{21} & \alpha_{15} & \alpha_7 & \alpha_2 & \alpha_{18} & \alpha_{10} & \alpha_8 & \alpha_{17} & \alpha_{16} & \alpha_1 & \alpha_{19} & \alpha_9 & \alpha_{23} & \alpha_{13} & \alpha_{20} & \alpha_4 & \alpha_{12} & \alpha_{14} & \alpha_6 & \alpha_3 & \alpha_5 & \alpha_{22} \\ \alpha_{13} & \alpha_3 & \alpha_2 & \alpha_5 & \alpha_4 & \alpha_{22} & \alpha_{15} & \alpha_{20} & \alpha_{17} & \alpha_{14} & \alpha_{19} & \alpha_{16} & \alpha_1 & \alpha_{10} & \alpha_7 & \alpha_{12} & \alpha_9 & \alpha_{23} & \alpha_{11} & \alpha_8 & \alpha_{24} & \alpha_6 & \alpha_{18} & \alpha_{21} \\ \alpha_4 & \alpha_5 & \alpha_{14} & \alpha_3 & \alpha_{13} & \alpha_{17} & \alpha_6 & \alpha_{19} & \alpha_{22} & \alpha_2 & \alpha_{20} & \alpha_9 & \alpha_{10} & \alpha_1 & \alpha_{12} & \alpha_7 & \alpha_{16} & \alpha_{11} & \alpha_{23} & \alpha_{21} & \alpha_{18} & \alpha_{15} & \alpha_{24} & \alpha_8 \\ \alpha_{15} & \alpha_7 & \alpha_9 & \alpha_{21} & \alpha_{19} & \alpha_{20} & \alpha_2 & \alpha_{12} & \alpha_3 & \alpha_{24} & \alpha_{14} & \alpha_8 & \alpha_{17} & \alpha_{11} & \alpha_1 & \alpha_{18} & \alpha_{13} & \alpha_{16} & \alpha_5 & \alpha_6 & \alpha_4 & \alpha_{23} & \alpha_{22} & \alpha_{10} \\ \alpha_{19} & \alpha_{21} & \alpha_{24} & \alpha_7 & \alpha_{15} & \alpha_3 & \alpha_{23} & \alpha_{14} & \alpha_{20} & \alpha_9 & \alpha_{12} & \alpha_{13} & \alpha_{11} & \alpha_{17} & \alpha_{18} & \alpha_1 & \alpha_8 & \alpha_5 & \alpha_{16} & \alpha_{10} & \alpha_{22} & \alpha_2 & \alpha_4 & \alpha_6 \\ \alpha_7 & \alpha_{15} & \alpha_{17} & \alpha_{24} & \alpha_{11} & \alpha_8 & \alpha_3 & \alpha_{16} & \alpha_2 & \alpha_{21} & \alpha_{10} & \alpha_{20} & \alpha_9 & \alpha_{19} & \alpha_{13} & \alpha_{23} & \alpha_1 & \alpha_{12} & \alpha_4 & \alpha_{22} & \alpha_5 & \alpha_{18} & \alpha_6 & \alpha_{14} \\ \alpha_{18} & \alpha_{23} & \alpha_{20} & \alpha_{22} & \alpha_{16} & \alpha_{10} & \alpha_{21} & \alpha_{13} & \alpha_{24} & \alpha_6 & \alpha_{17} & \alpha_{14} & \alpha_8 & \alpha_{12} & \alpha_{19} & \alpha_5 & \alpha_{11} & \alpha_1 & \alpha_{15} & \alpha_3 & \alpha_7 & \alpha_4 & \alpha_2 & \alpha_9 \\ \alpha_{16} & \alpha_{22} & \alpha_6 & \alpha_{23} & \alpha_{18} & \alpha_{24} & \alpha_4 & \alpha_{17} & \alpha_{10} & \alpha_{20} & \alpha_{13} & \alpha_{11} & \alpha_{12} & \alpha_8 & \alpha_5 & \alpha_{19} & \alpha_{14} & \alpha_{15} & \alpha_1 & \alpha_9 & \alpha_2 & \alpha_{21} & \alpha_7 & \alpha_3 \\ \alpha_{20} & \alpha_8 & \alpha_{18} & \alpha_{12} & \alpha_6 & \alpha_5 & \alpha_{11} & \alpha_2 & \alpha_{19} & \alpha_{16} & \alpha_7 & \alpha_4 & \alpha_{23} & \alpha_{22} & \alpha_{24} & \alpha_{10} & \alpha_{21} & \alpha_3 & \alpha_9 & \alpha_1 & \alpha_{17} & \alpha_{14} & \alpha_{13} & \alpha_{15} \\ \alpha_{22} & \alpha_{16} & \alpha_{12} & \alpha_{20} & \alpha_8 & \alpha_{11} & \alpha_{10} & \alpha_{15} & \alpha_4 & \alpha_{23} & \alpha_3 & \alpha_{24} & \alpha_6 & \alpha_{18} & \alpha_{14} & \alpha_{21} & \alpha_5 & \alpha_{17} & \alpha_2 & \alpha_7 & \alpha_1 & \alpha_{19} & \alpha_9 & \alpha_{13} \\ \alpha_{21} & \alpha_{19} & \alpha_{11} & \alpha_9 & \alpha_{17} & \alpha_{13} & \alpha_{20} & \alpha_5 & \alpha_{23} & \alpha_7 & \alpha_6 & \alpha_3 & \alpha_{24} & \alpha_{15} & \alpha_8 & \alpha_2 & \alpha_{18} & \alpha_{14} & \alpha_{22} & \alpha_4 & \alpha_{16} & \alpha_1 & \alpha_{10} & \alpha_{12} \\ \alpha_8 & \alpha_{20} & \alpha_{23} & \alpha_{16} & \alpha_{22} & \alpha_4 & \alpha_{19} & \alpha_3 & \alpha_{11} & \alpha_{12} & \alpha_{15} & \alpha_5 & \alpha_{18} & \alpha_6 & \alpha_{21} & \alpha_{14} & \alpha_{24} & \alpha_2 & \alpha_{17} & \alpha_{13} & \alpha_9 & \alpha_{10} & \alpha_1 & \alpha_7 \\ \alpha_6 & \alpha_{12} & \alpha_{16} & \alpha_8 & \alpha_{20} & \alpha_{19} & \alpha_{14} & \alpha_7 & \alpha_5 & \alpha_{18} & \alpha_2 & \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{10} & \alpha_{24} & \alpha_4 & \alpha_9 & \alpha_3 & \alpha_{15} & \alpha_{13} & \alpha_{11} & \alpha_{17} & \alpha_1 \end{pmatrix}$$

and $\sigma(v) = \sigma(v)^T$ if and only if $a_4 = a_{14}$, $a_6 = a_{24}$, $a_7 = a_{17}$, $a_8 = a_{23}$, $a_{11} = a_{12}$, $a_{16} = a_{19}$ and $a_{21} = a_{22}$. Next, consider elements of $\mathbb{F}_2((C_6 \times C_2) \rtimes C_2)$ of the form

$$\begin{aligned} \{&\sum_{i=1}^{4} (\alpha_i y^{i-1} + \alpha_{i+4} x y^{i-1}) + \sum_{i=1}^{2} (\alpha_{i+8} x^2 y^{i-1} + \alpha_{i+12} y^{i+1} z) + (\alpha_{11} x^2 y^2 + \alpha_{17} x^2 z)(1 + y) \\ &+ \alpha_4 yz + \alpha_6 x^2 y^3 z + \alpha_7 xz + x^2 y^2 z \alpha_8 + \alpha_{12} z + \alpha_{14} x y^2 z + \alpha_{15} xyz + \alpha_{16} x y^3 z\} \end{aligned}$$

and in particular the element $v_1 = 1 + [a + b + b^3 + (a + a^2)(b^2 + b^3)]c$ of this set. The matrix $\sigma(v_1)$ is equivalent to

$$\begin{pmatrix} I & A \end{pmatrix}$$

where

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

It is a small computation to see that $C(v_1)$ is the $[24, 12, 8]$ code. Moreover, it can be shown that the above set contains 576 elements that generate the $[24, 12, 8]$ code.

3.2.4 The Group $SL(2, 3)$

Next we consider the group $SL(2, 3)$. Let v be the element

$$v = \sum_{i=1}^{6} x^{i-1} \left(\alpha_i + \alpha_{6+i}y + \alpha_{12+i}y^2 + \alpha_{18+i}y^2x\right) \in \mathbb{F}_2 SL(2, 3)$$

where $SL(2, 3) = \langle x, y \,|\, x^3 = y^3 = (xy)^2 \rangle$ and $\alpha_i \in \mathbb{F}_2$. Now,

$$\sigma(v) = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_5 & A_6 & A_7 & A_8 \\ A_9 & A_{10} & A_{11} & A_{12} \\ A_{13} & A_{14} & A_{15} & A_{16} \end{pmatrix},$$

where $A_1 = circ(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6)$, $A_2 = circ(\alpha_7, \alpha_8, \alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12})$,
$A_3 = circ(\alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha_{16}, \alpha_{17}, \alpha_{18})$, $A_4 = circ(\alpha_{19}, \alpha_{20}, \alpha_{21}, \alpha_{22}, \alpha_{23}, \alpha_{24})$,
$A_5 = circ(\alpha_{16}, \alpha_{22}, \alpha_8, \alpha_{13}, \alpha_{19}, \alpha_{11})$, $A_6 = circ(\alpha_1, \alpha_{21}, \alpha_{14}, \alpha_4, \alpha_{24}, \alpha_{17})$,
$A_7 = circ(\alpha_7, \alpha_{20}, \alpha_5, \alpha_{10}, \alpha_{23}, \alpha_2)$, $A_8 = circ(\alpha_{18}, \alpha_{12}, \alpha_6, \alpha_{15}, \alpha_9, \alpha_3)$,
$A_9 = circ(\alpha_{10}, \alpha_{15}, \alpha_{21}, \alpha_7, \alpha_{18}, \alpha_{24})$, $A_{10} = circ(\alpha_{16}, \alpha_6, \alpha_{20}, \alpha_{13}, \alpha_3, \alpha_{23})$,
$A_{11} = circ(\alpha_1, \alpha_{12}, \alpha_{19}, \alpha_4, \alpha_9, \alpha_{22})$, $A_{12} = circ(\alpha_2, \alpha_{17}, \alpha_{11}, \alpha_5, \alpha_{14}, \alpha_8)$,
$A_{13} = circ(\alpha_9, \alpha_{14}, \alpha_{20}, \alpha_{12}, \alpha_{17}, \alpha_{23})$, $A_{14} = circ(\alpha_{15}, \alpha_5, \alpha_{19}, \alpha_{18}, \alpha_2, \alpha_{22})$,
$A_{15} = circ(\alpha_6, \alpha_{11}, \alpha_{24}, \alpha_3, \alpha_8, \alpha_{21})$, $A_{16} = circ(\alpha_1, \alpha_{16}, \alpha_{10}, \alpha_4, \alpha_{13}, \alpha_7)$.

Now, $\sigma(v) = \sigma(v)^T$ if and only if $\alpha_2 = \alpha_6$, $\alpha_3 = \alpha_5$, $\alpha_7 = \alpha_{16}$, $\alpha_8 = \alpha_{11}$, $\alpha_9 = \alpha_{19}$, $\alpha_{10} = \alpha_{13}$, $\alpha_{12} = \alpha_{22}$, $\alpha_{14} = \alpha_{24}$, $\alpha_{15} = \alpha_{18}$, $\alpha_{17} = \alpha_{21}$ and $\alpha_{20} = \alpha_{23}$. Next, consider elements of $\mathbb{F}_2 SL(2, 3)$ of the form:

$$\begin{aligned} \{&\alpha_1 + \alpha_2(x + x^5) + \alpha_3(x^2 + x^4) + \alpha_4 x^3 + \alpha_5(y + x^3y^2) + \alpha_6(xy + x^4y) + \alpha_7(x^2y + y^2x) \\ &+ \alpha_8(x^3y + y^2) + \alpha_9(x^5y + x^3y^2x) + \alpha_{10}(xy^2 + x^5y^2x) + \alpha_{11}(x^2y^2 + x^5y^2) \\ &+ \alpha_{12}(x^4y^2 + x^2y^2x) + \alpha_{13}(xy^2x + x^4y^2x) \,|\, \alpha_i \in \mathbb{F}_2\}. \end{aligned}$$

It can be shown that it is not possible to construct the $[24, 12, 8]$ from any element of this set.

3.2.5 The Group $C_2^2 \times D_6$

Next we consider the group $C_2^2 \times D_6$. Let v be the element

$$v = \sum_{i=0}^{2}[(\alpha_{i+1} + \alpha_{i+4}z + \alpha_{i+7}w + \alpha_{i+10}zw) + b(\alpha_{i+13} + \alpha_{i+16}z + \alpha_{i+19}w + \alpha_{i+22}zw)]a^i \in \mathbb{F}_2(C_2^2 \times D_6)$$

where $\langle z, w\rangle = C_2^2$, $\langle a, b\rangle = D_6$ and $\alpha_i \in \mathbb{F}_2$. Now

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

where $A = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_2 & A_1 & A_4 & A_3 \\ A_3 & A_4 & A_1 & A_2 \\ A_4 & A_3 & A_2 & A_1 \end{pmatrix}$, $B = \begin{pmatrix} B_1 & B_2 & B_3 & B_4 \\ B_2 & B_1 & B_4 & B_3 \\ B_3 & B_4 & B_1 & B_2 \\ B_4 & B_3 & B_2 & B_1 \end{pmatrix}$, $A_1 = cir(\alpha_1, \alpha_2, \alpha_3)$, $A_2 = cir(\alpha_4, \alpha_5, \alpha_6)$, $A_3 = cir(\alpha_7, \alpha_8, \alpha_9)$, $A_4 = cir(\alpha_{10}, \alpha_{11}, \alpha_{12})$, $B_1 = rcir(\alpha_{13}, \alpha_{14}, \alpha_{15})$, $B_2 = rcir(\alpha_{16}, \alpha_{17}, \alpha_{18})$, $B_3 = rcir(\alpha_{19}, \alpha_{20}, \alpha_{21})$ and $B_4 = rcir(\alpha_{22}, \alpha_{23}, \alpha_{24})$.
Now, $\sigma(v) = \sigma(v)^T$ if and only if $\alpha_2 = \alpha_3$, $\alpha_5 = \alpha_6$, $\alpha_8 = \alpha_9$ and $\alpha_{11} = \alpha_{12}$. Next, consider elements of $\mathbb{F}_2(C_2^2 \times D_6)$ of the form

$$\{\alpha_1 + \alpha_3 z + \alpha_5 w + \alpha_7 zw + (a + a^2)(\alpha_2 + \alpha_4 z + \alpha_6 w + \alpha_8 zw) + \sum_{i=0}^{2} + ba^i(\alpha_{i+13} + \alpha_{i+16}z + \alpha_{i+19}w + \alpha_{i+22}zw)\}.$$

It can be shown that it is not possible to construct the $[24, 12, 8]$ Golay code from any element of this set.

We summarize these results in the following: The $[24, 12, 8]$ Type II code can be constructed in $\mathbb{F}_2 G$ precisely for the following groups of order 24: S_4, D_{24}, $C_3 \times D_8$, $C_2 \times A_4$ and $(C_6 \times C_2) \rtimes C_2$.

3.3 The Dihedral Group

In this section, we shall describe these techniques for generating codes for the dihedral group. Let D_{2k} be the dihedral group of order $2k$. We describe the group by $D_{2k} = \langle a, b \mid a^2 = b^k = 1, ab = b^{-1}a\rangle$. The ordering of the elements for the map σ is $1, b, b^2, \ldots, b^{k-1}, a, ab, ab^2, \ldots, ab^{k-1}$. It is this group that McLoughlin used in [85] to give a construction of the binary $[48, 24, 12]$ extremal Type II code.

Let $v = \sum \alpha_{a^i,b^j} a^i b^j$. In this case, the matrix $\sigma(v)$ is of the form:

$$\begin{pmatrix}
\alpha_1 & \alpha_b & \alpha_{b^2} & \dots & \alpha_{b^{k-1}} & \alpha_a & \alpha_{ab} & \alpha_{ab^2} & \dots & \alpha_{ab^{k-1}} \\
\alpha_{b^{k-1}} & \alpha_1 & \alpha_b & \dots & \alpha_{b^{k-2}} & \alpha_{ab} & \alpha_{ab^2} & \alpha_{ab^3} & \dots & \alpha_a \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\alpha_b & \alpha_{b^2} & \alpha_{b^3} & \dots & \alpha_1 & \alpha_{ab^{k-1}} & \alpha_a & \alpha_{ab} & \dots & \alpha_{ab^{k-2}} \\
\alpha_a & \alpha_{ab} & \alpha_{ab^2} & \dots & \alpha_{ab^{k-1}} & \alpha_1 & \alpha_b & \alpha_{b^2} & \dots & \alpha_{b^{k-1}} \\
\alpha_{ab} & \alpha_{ab^2} & \alpha_{ab^3} & \dots & \alpha_a & \alpha_{b^{k-1}} & \alpha_1 & \alpha_b & \dots & \alpha_{b^{k-2}} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\alpha_{ab^{k-1}} & \alpha_a & \alpha_{ab} & \dots & \alpha_{ab^{k-2}} & \alpha_b & \alpha_{b^2} & \alpha_{b^3} & \dots & \alpha_1
\end{pmatrix}. \tag{3.6}$$

This gives that $\sigma(v)$ is of the form:

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix}$$

where A is a circulant matrix and B is a reverse circulant matrix.

We begin by proving a lemma.

Lemma 3.3.1 *Let R be a finite commutative Frobenius ring of characteristic 2. Let C be the code generated by a matrix M of the form*

$$\begin{pmatrix} I_k & B \\ B & I_k \end{pmatrix},$$

where B is a symmetric k by k matrix. If the free rank of C is k then C is self-dual.

Proof. Let $D = \langle (I_k|B) \rangle$ and $D' = \langle (B|I_k) \rangle$. The inner-product of the i-th row of $(I_k|B)$ and the j-th row of $(B|I_k)$ is $B_{i,j} + B_{j,i} = 0$ since $B_{i,j} = B_{j,i}$ and the characteristic is 2. Therefore $D' = D^\perp$ since $|D||D'| = |R|^n$.

The code $C = \langle D, D^\perp \rangle$. If $D \neq D^\perp$ then $|C| > |D|$. However, we are assuming that the free rank of C is k. Hence $C = D = D^\perp$. This gives that C is a self-dual code. ■

In [60], Hurley proves that C_v is self-dual over $\mathbb{F}_2$ if $v \in \mathbb{F}_2 D_{24}$, $v^2 = 0$ and the dimension is $\frac{n}{2}$. We can expand this by showing the following which eliminates the need for v to satisfy $v^2 = 0$.

Theorem 3.3.2 *Let R be a finite commutative Frobenius ring of characteristic 2 and let $v \in RD_n$ with $v = \sum \alpha_i h_i$ where only one $\alpha_{a^0 b^i}$ is 1 and the rest are 0. If C_v has free rank k, then C_v is a self-dual code.*

Proof. Since only one α_{2i} is 1 and the rest are 0, the generator matrix of C_v is permutation equivalent to a matrix of the form:

$$\begin{pmatrix} I_k & B \\ B & I_k \end{pmatrix}$$

where B is a reverse circulant matrix and hence symmetric. Then, by Lemma 3.3.1, we have the result. ■

To show the importance of the strengthening of this result, consider the element $v = 1 + ab \in \mathbb{F}_2 D_{2k}$ where k is greater than 2. Then $(1e_{D_{2k}} + ab)^2 \neq 0$ but C_v is a self-dual code. We continue with a larger example.

Example 3.3.3 *Consider $v \in \mathbb{F}_2 D_{48}$ such that $dim(C_v) = 24$ and the minimum distance of C_v is 10. There are 192 elements v which produce equivalent self-dual codes using the technique.*

A common technique for producing self-dual codes is to generate a code with the matrix $(I_{\frac{n}{2}}|A)$ where A is a reverse circulant matrix. Given a code C generated by this matrix we have that $C^{\perp}$ is generated by $(A^T|I_{\frac{n}{2}})$ which is equal to $(A|I_{\frac{n}{2}})$ since A is symmetric. If C is a self-dual code then $\langle (A|I_{\frac{n}{2}}) \rangle \subseteq \langle (I_{\frac{n}{2}}|A) \rangle$. This means that the code generated by $\begin{pmatrix} I_{\frac{n}{2}} & A \\ A & I_{\frac{n}{2}} \end{pmatrix}$ is the code C. Consider the first row of this matrix. Reading this as an element $v \in \mathbb{F}_2 D_{2k}$ we have that $C = C(v)$. This gives the following:

Theorem 3.3.4 *Let C be a binary self-dual code generated by $(I_{\frac{n}{2}}|A)$ where A is a reverse circulant matrix then $C = C(v)$ for some $v \in \mathbb{F}_2 D_{2k}$.*

Applying Corollary 3.1.5, we now have,

Corollary 3.3.5 *The putative $[72, 36, 16]$ Type II code cannot be produced by $(I_{\frac{n}{2}}|A)$ where A is a reverse circulant matrix.*

Proof. Corollary 3.1.5 gives that the $[72, 36, 16]$ Type II code is not formed from an element in a group algebra and so Theorem 3.3.4 gives the result. ■

This corollary eliminates a commonly used technique in the attempt to construct this putative code. Namely, many computational approaches to this problem have been to construct a reverse circulant matrix A and generate the code $(I_{\frac{n}{2}}|A)$. Of course, this technique has not yet produced the code. This corollary gives a reason why these attempts have not been successful.

3.4 The Cyclic Group Cross the Dihedral Group

In this section, we shall use the group $G = C_s \times D_{2k}$. Let $C_s = \langle h \rangle$ and let $D_{2k} = \langle a, b \mid a^2 = b^k = 1, ab = b^{-1}a \rangle$. We shall order the elements as follows:

$$\{(1,1),(1,b),\ldots,(1,b^{k-1}),(h,1),(h,b),\ldots,(h,b^{k-1}),\ldots,(h^{s-1},1),$$
$$(h^{s-1},b),\ldots,(h^{s-1},b^{k-1}),(1,ab),\ldots,(1,ab^{k-1}),(h,1),(h,ab),\ldots,(h,ab^{k-1}),$$
$$\ldots,(h^{s-1},1),(h^{s-1},ab),\ldots,(h^{s-1},ab^{k-1})\}.$$

We see that if we choose $v \in RG$ such that only 1 of $\alpha_{(h^i,a^0b^j)}$ is 1 and the rest are 0. Then we get a matrix $\sigma(v)$ of the form:

$$\begin{pmatrix} I_k & B \\ B & I_k \end{pmatrix},$$

where B is of the following form:

$$B = \begin{pmatrix} 1A & hA & h^2A & \dots & h^{s-1}A \\ h^{s-1}A & 1A & hA & \dots & h^{s-2}A \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ hA & h^2A & h^3A & \dots & 1A \end{pmatrix}$$

where h^kA indicates the matrix where the i,j-th element is $(h^k, A_{i,j})$ and A is a reverse circulant matrix.

Theorem 3.4.1 *Let R be a Frobenius ring and let $v \in RC_sD_{2k}$ with $v = \sum \alpha_i h_i$ where only 1 of $\alpha_{(h^i,)a^0b^j}$ is 1 and the rest are 0. Let R be a finite commutative Frobenius ring of characteristic 2. If $|C_v| = |R|^{\frac{n}{2}}$, then C_v is isodual and hence formally self-dual with respect to any weight enumerator.*

Proof. We have that the code $C(v)$ is generated by $(I_k|B)$ and then its orthogonal is generated by $(B^T|I_k)$. Then we have that B is equivalent to B^T. Therefore $C(v)$ and $C(v)^\perp$ are equivalent and therefore, by Lemma 1.2.17, formally self-dual with respect to any weight enumerator. ■

Note that if R is a finite field, then the condition in the previous theorem becomes that $dim(C_v) = \frac{n}{2}$.

Example 3.4.2 *Let G be the group C_3D_8. There are exactly $2^{12} = 4096$ elements in $\mathbb{F}_2G$ with the property that $\alpha_{(h^i,a^0b^j)}$ is equal to 1 when $i = j = 0$ and equal to 0 otherwise. Of these 256 have $dim(C_v) = 12$, and 192 of these codes are formally self-dual but not self-dual and 64 are self-dual. Of the 192 formally self-dual codes, 80 have minimum distance 6 which is optimal for Type I codes. As an example, if $v_1 = 1+a(b+b(1+b)(bh+h^2))$ then C_{v_1} is a formally self-dual code with minimum distance 6. The remaining 112 formally self-dual codes have have minimum distance 4 and C_{v_2} is an example of such a code where $v_2 = 1 + a(b^2 + h + b^3h + h^2 + bh^2)$.*

Example 3.4.3 *Let G be the group C_4D_8 and consider elements of $\mathbb{F}_2G$ with the property that $\alpha_{(h^i,a^0b^j)}$ is equal to 1 when $i = j = 0$ and equal to 0 otherwise. Of these elements, there are 2048 that have $dim(C_v) = 16$, of these 512 are self-dual and the remaining 1536 are formally self-dual. Let $v_1 = 1 + a(\hat{b} + h)h$, $v_2 = 1 + a(b + b^3 + h + h^3 + (b^2 + \hat{b})h^2 + (1 + \hat{b})h^3)$ and $v_3 = 1 + a(b(1 + h) + \hat{b}h^2 + (b + \hat{b})h^3)$. The code C_{v_1} is an example of a formally self-dual with minimum distance 4, the code C_{v_2} is an example of a formally self-dual with minimum distance 6 and the code C_{v_3} is an example of a formally self-dual with minimum distance 8. Of the 1536 formally self-dual codes, there are 896 with minimum distance 4, 192 with minimum distance 6 and 448 with minimum distance 8.*

Example 3.4.4 *Let G be C_5D_8 and $v = 1 + a((u + ub + ub^2 + b^3) + (u + b + b^2 + ub^3)(h + h^4) + (1 + b + ub^3)(h^2 + h^3)) \in R_1C_5D_8$. Then $C_v = \langle \sigma(v), u\sigma(v) \rangle$ is a self-dual code and its image under ϕ_1 is a binary self-dual $[80, 40, 12]$ code with an automorphism group of order 160.*

Example 3.4.5 *Let G be the group C_2D_{26} and consider the elements $\mathbb{F}_2$ with the properties that $\alpha_{(h^i,a^0b^j)}$ is equal to 1 when $i = j = 0$ and equal to 0 otherwise. Of these elements, there are six inequivalent self-dual $[52, 26, 10]$ codes. These six elements are as follows:*

i	$v_i \in \mathbb{F}_2(C_2D_{26})$	$\lvert Aut(C_{v_i})\rvert$
1	$1 + a((b^8 + b^{10} + b^{11} + b^{12}) + (b + b^2 + b^3 + b^4 + b^5 + b^6 + b^8 + b^9 + b^{11})h)$	52
2	$1 + a((b^7 + b^9 + b^{10} + b^{11}) + (1 + b + b^2 + b^3 + b^5 + b^7 + b^8 + b^{10} + b^{11})h)$	52
3	$1 + a((b^6 + b^8 + b^{10} + b^{11} + b^{12}) + (1 + b + b^2 + b^3 + b^5 + b^7 + b^8 + b^{11})h)$	52
4	$1 + a((b^6 + b^8 + b^9 + b^{10} + b^{11} + b^{12}) + (1 + b^2 + b^3 + b^4 + b^6 + b^7 + b^8)h)$	52
5	$1 + a((b^5 + b^8 + b^9 + b^{10} + b^{12}) + (b + b^3 + b^4 + b^6 + b^7 + b^9 + b^{10} + b^{11})h)$	52
6	$1 + a((b^5 + b^7 + b^8 + b^9 + b^{10} + b^{11} + b^{12}) + (1 + b + b^2 + b^3 + b^7 + b^{11})h)$	52

3.5 The Cyclic Case

In this section, we shall set $G = C_n$ the cyclic group of order n. Since the inception of cyclic codes, it has been an open question to determine which cyclic codes are self-dual. We shall describe when this occurs.

We focus on the case when $n = 2k$. Let $G = \langle h \rangle$, and let $h_i = h^i$. We then use, as the ordering of the elements of G:

$$(h_0, h_2, \ldots, h_{2k}, h_1, h_3, \ldots, h_{2k-1}).$$

That is $g_i = h_{2(i-1)}$ for $i = 1$ to k and $g_{k+j} = h_{2(j-1)+1}$ for $j = 1$ to k.

It follows that the form of $\sigma(v)$ is:

$$\begin{pmatrix}
\alpha_{h_0} & \alpha_{h_2} & \cdots & \alpha_{h_{2k}} & \alpha_{h_1} & \alpha_{h_3} & \cdots & \alpha_{h_{2k-1}} \\
\alpha_{h_{2k}} & \alpha_{h_0} & \cdots & \alpha_{h_{2k-2}} & \alpha_{h_{2k-1}} & \alpha_{h_1} & \cdots & \alpha_{h_{2k-3}} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
\alpha_{h_4} & \alpha_{h_6} & \cdots & \alpha_{h_2} & \alpha_{h_3} & \alpha_{h_5} & \cdots & \alpha_{h_1} \\
\alpha_{h_{2k-1}} & \alpha_{h_1} & \cdots & \alpha_{h_{2k-3}} & \alpha_{h_0} & \alpha_{h_2} & \cdots & \alpha_{h_{2k}} \\
\alpha_{h_{2k-3}} & \alpha_{h_{2k-1}} & \cdots & \alpha_{h_{2k-5}} & \alpha_{h_{2k}} & \alpha_{h_0} & \cdots & \alpha_{h_{2k-2}} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
\alpha_{h_1} & \alpha_{h_3} & \cdots & \alpha_{h_{2k-1}} & \alpha_{h_4} & \alpha_{h_6} & \cdots & \alpha_{h_2}
\end{pmatrix}.$$

Hence $\sigma(v)$ is of the form

$$\begin{pmatrix} A & B \\ D & A \end{pmatrix}$$

where A, B and D are circulant matrices.

Choose an element of v such that $v = \sum \alpha_i h_i$ where only one of $\alpha_{2i} = 1$ and the rest of α_{2i} are 0. Then the generating matrix is permutation equivalent to a matrix where A is I_k and B and D are circulant matrices. Namely, we get a matrix of the form

$$\begin{pmatrix} I_{\frac{n}{2}} & B \\ D & I_{\frac{n}{2}} \end{pmatrix}.$$

Theorem 3.5.1 *Let R be a Frobenius ring of characteristic 2 and let $v \in RC_n$ with $v = \sum \alpha_i h_i$ where only one $\alpha_{2i} = 1$ and the rest of α_{2i} are 0. If $v_{2k-i} = v_i$ for odd i and $|C| = |R|^k$ then $C(v)$ is a self-dual code.*

Proof. By the construction, we have that $\sigma(v)$ is of the form

$$\begin{pmatrix} I_k & B \\ D & I_k \end{pmatrix}.$$

If $v_{2k-i} = v_i$ for odd i then $D = B^T$. We have that $|C| = |R|^k$. However, the form of the matrix gives that C contains a free code isomorphic to R^k, namely the code generated by the matrix $(I_k|B)$. This means that $C = \langle (I_k|B) \rangle$.

Consider the code generated by the matrix $(B^T|I_k)$. This code must be $C^\perp$. However, this code is contained in $C(v)$ as well, so we have that $C = C^\perp$. ■

Notice that we did not have to determine the cardinality of the code to see that the code was self-dual. Note that it is certainly more difficult to use this technique to construct self-dual codes with the cyclic group. That is, we had to put more restrictions on v to obtain a self-dual code. This is certainly to be expected since it is fairly difficult to find cyclic self-dual codes.

Moreover, note that a code over R_k constructed with this technique is cyclic, which gives that its image under the Gray map is quasi-cyclic of index 2^k.

Example 3.5.2 *Let G be the cyclic group of order 10 and $v = 1 + uh + h^5 + uh^9 \in R_1C_{10}$. Then $C_v = \langle \sigma(v), u\sigma(v) \rangle$ is cyclic self-dual code and its image under ϕ_1 is a binary quasi-cyclic self-dual $[20, 10, 4]$ code of index 2.*

We note that this is a standard construction of self-dual codes, namely you take a vector $\mathbf{v}$ and generate a circulant matrix B from it with $BB^T = -I_k$, with $n = 2k$, and generate the code $(I_k|B)$. Hence, we have another of the standard constructions of self-dual codes within our general framework.

We can now use our general construction to produce isodual codes.

Theorem 3.5.3 *Let R be a finite commutative Frobenius ring with characteristic 2. Let $v \in RC_n$ with $v = \sum \alpha_i h_i$ where only one $\alpha_{2i} = 1$ and the rest of α_{2i} are 0. If $|C(v)| = |R|^{\frac{n}{2}}$ then $C(v)$ is a formally self-dual code with respect to any weight enumerator.*

Proof. If $|C(v)| = |R|^{\frac{n}{2}}$ then C is generated by the matrix $(I_k|B)$ where B is a circulant matrix. Then its orthogonal is of the form $(B^T|I_k)$. Since B is a circulant code, then by permuting the rows and columns of B we can form B^T. This gives that $C(v)^\perp$ is equivalent to $C(V)$ and hence isodual and therefore formally self-dual code with respect to any weight enumerator. ■

Example 3.5.4 *Let G be the cyclic group of order 6 and $v = 1 + u_2h + (1 + u_1 + u_1u_2)h^3 + u_1h^5 \in R_2C_6$. Then $C_v = \langle \sigma(v), u_1\sigma(v), u_1u_2\sigma(v) \rangle$ is a cyclic formally self-dual code and its image under ϕ_2 is a binary quasi-cyclic self-dual $[24, 12, 6]$ code of index 4.*

Example 3.5.5 *Let G be the cyclic group of order* 10*. The following elements of R_2C_{10} generate four inequivalent binary self-dual* $[40, 20, 8]$ *codes:*

i	$v_i \in R_2C_{10}$	$\lvert Aut(C_{v_i})\rvert$
1	$1 + u_1(h + h^9) + u_2(h^3 + h^7) + h^5$	$2^{16} \cdot 3^3 \cdot 5^2$
2	$1 + u_1(h + h^9) + u_2(h^3 + h^7) + (u_1u_2 + 1)h^5$	$2^{14} \cdot 3 \cdot 5$
4	$1 + u_1(h + h^9) + u_2(h^3 + h^7) + (u_2 + 1)h^5$	$2^{14} \cdot 3 \cdot 5$
5	$1 + u_1(h + h^9) + u_2(h^3 + h^7) + (u_1 + u_1 + 1)h^5$	$2^{16} \cdot 3^3 \cdot 5^2$

Chapter 4

Constructions for Self-Dual Codes Induced from Group Rings

Self-dual codes are a special class of codes that have connections to and applications in many fields such as Lattices, Designs, Cryptography, Invariant Theory, etc. The natural upper bound on the minimum distances of binary self-dual codes have led to the notion of extremal self-dual codes; where self-dual codes have the largest possible minimum distance. There are numerous papers on construction and classification of extremal binary self-dual codes of certain lengths. Many different techniques have been utilized in the search for extremal binary self-dual codes. A common theme in these methods of construction is the use of a computer search. In order to make this search feasible, special construction methods are used in order to reduce the search field.

The double circulant construction is one of the most extensively used techniques to construct extremal binary self-dual codes. The double circulant construction assumes that the generator matrix takes the form $(I_n|A)$ where A is a circulant matrix. If this matrix generates a self-dual code, then, $AA^T = -I_n$. This technique was first introduced in the 1960's ([17, 76]). Since then, it has been extensively and successfully demonstrated to find many extremal self-dual codes, ([48, 49, 51–53]).

In this chapter, we consider constructing self-dual codes generated by matrices of the form $[I_n|\sigma(v)]$ where the image of v under σ, defined in Theorem 1.1.15, is described in [60]. We show that under certain conditions, unitary units in RG correspond to self-dual codes. Furthermore, we find a correspondence between certain well-known techniques, namely double circulant and four circulant, and certain well-known classes of groups, cyclic and dihedral groups, respectively. Next, we demonstrate this construction for all groups of orders 8 and 16 over $\mathbb{F}_2$, $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$. Following the construction of many codes of length 64, we extend certain codes to result in new codes of length 68.

4.0.1 The General Idea

Let G be a group of order n, where the elements of the group G are assigned a label, $G = \{g_1, g_2, \ldots, g_n\}$. Then, for a given element of the group ring, $v = \alpha_1 g_1 + \alpha_2 g_2 + \cdots + \alpha_n g_n \in RG$,

we consider the image of v under the σ map described previously. Based on the structure of the group, these $n \times n$ matrices can have special block-structures. After identifying the block structure of $\sigma(v)$, we form the $n \times 2n$ matrix, $[I_n|\sigma(v)]$. The code generated by this matrix will have size $|R|^n$. Thus, if it is self-orthogonal, then we would have obtained a self-dual code. We can summarize this idea in the following main theorem:

Theorem 4.0.1 *Let G be a group of order n and $v = \alpha_1 g_1 + \alpha_2 g_2 + \cdots + \alpha_n g_n \in RG$ be an element of the group ring RG. The matrix $[I_n|\sigma(v)]$ generates a self-dual code over R if and only if $\sigma(v)\sigma(v)^T = -I_n$.*

Using the previous theorem, we can relate self-dual codes to elements in a group ring in a strong way. To do this, recall the canonical involution $* : RG \to RG$ on a group ring RG is given by $v^* = \sum_g a_g g^{-1}$, for $v = \sum_g a_g g \in RG$. If v satisfies $vv^* = 1$, then we say that v is a unitary unit in RG. An important connection between v^* and v appears when we take their images under the σ map:

$$\sigma(v^*) = \sigma(v)^T. \tag{4.1}$$

Now, using Theorem 4.0.1, the fact that σ is a ring homomorphism and that $\sigma(v) = -I_n$ if and only if $v = -1$, we get the following corollary:

Corollary 4.0.2 *Let RG be a group ring, where R is a commutative Frobenius ring. For $v \in RG$, the matrix $[I_n|\sigma(v)]$ 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 important result:

Corollary 4.0.3 *Let RG be a group ring where R is a commutative Frobenius ring of characteristic 2. Then, the matrix $[I_n|\sigma(v)]$ generates a self-dual code over R if and only if v satisfies $vv^* = 1$, namely v is a unitary unit in RG.*

Before moving on to the construction methods arising from certain groups, we would like to consider two special cases.

4.0.2 Two Special Cases

We would like to demonstrate, with the following examples, that many of the well-known construction methods in the literature of self-dual codes are just special cases of the idea we have described above.

If we take $G = C_n = \langle c \rangle$, the cyclic group of order n, then for $v = a_0 e + a_1 c + \cdots + a_{n-1} c^{n-1}$, we have $\sigma(v)$ is a circulant matrix. Thus the construction that is induced by the cyclic group is the well-known double-circulant construction, that has been used frequently in constructing self-dual codes.

If we take $G = D_{2n}$, the dihedral group of order n and we label it as

$$G = \{e, x, \ldots, x^{n-1}, y, xy, \ldots, x^{n-1}y\},$$

then the companion matrix of a typical element $v \in RD_{2n}$ will be of the form

$$G = \begin{bmatrix} A & B \\ B^T & A^T \end{bmatrix},$$

which leads to another well-known construction in the literature of self-dual codes; when the characteristic of R is 2 and we place I_{2n} next to G, we have the four-circulant construction.

In what follows, we will take groups of order 8 and 16 to describe the construction methods arising from these groups for self-dual codes.

4.1 Constructions coming from groups of order 8

In this section, we will use Theorem 4.0.1 and Hurley's map to describe the construction methods coming from groups of order 8. Following this, the constructions will be applied to find extremal binary self-dual codes.

4.1.1 Constructions

For the groups below, we give the structure of the companion matrix $\sigma(v)$ for a typical element $v \in \mathbb{F}_2 G$. We then take the matrices of the form $[I_8|\sigma(v)]$ to construct binary self-dual codes of length 16. Recall that $cir(a_1, a_2, \ldots, a_n)$ means the circulant matrix whose first row is $(a_1, a_2, \ldots, a_n)$, while $rcir(a_1, a_2, \ldots, a_n)$ means the reverse circulant matrix. Let $CIR(A_1, A_2, \ldots, A_n)$ represent a block circulant matrix whose first row of block matrices are A_1, A_2,..., A_n. Additionally, let P_τ be the $n \times n$ permutation matrix for the permutation $\tau \in \mathcal{G}$ where $n = |\mathcal{G}|$.

▪ Let $G = \langle x_1, x_2, x_3 \,|\, x_i^2 = 1, x_j x_k = x_k x_j \ (j \neq k) \rangle \cong C_2^3$. If

$$\alpha = a_1 + a_2 x_1 + a_3 x_2 + a_4 x_1 x_2 + a_5 x_3 + a_6 x_1 x_3 + a_7 x_2 x_3 + a_8 x_1 x_2 x_3 \in RC_2^3,$$

then

$$\sigma(\alpha) = P_e \otimes CIR(A, B) + P_{(1,2)} \otimes CIR(C, D)$$

where $\mathcal{G} = \{e, (1, 2)\}$, $A = cir(a_1, a_2)$, $B = cir(a_3, a_4)$, $C = cir(a_5, a_6)$, $D = cir(a_7, a_8)$ and $a_i \in R$.

▪ Let $G = \langle x_1, x_2 \,|\, x^4 = y^2 = 1, xy = yx \rangle \cong C_2 \times C_4$. If

$$\alpha = \sum_{i=0}^{3} a_{i+1} x^i + a_{i+5} x^i y \in R(C_2 \times C_4),$$

then

$$\sigma(\alpha) = CIR(A, B)$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = cir(a_5, a_6, a_7, a_8)$ and $a_i \in R$.

▪ Let $G = \langle x, y \,|\, x^4 = y^2 = 1, xy = yx \rangle \cong C_2 \times C_4$. If

$$\alpha = \sum_{i=0}^{3} a_{2i+1}x^i + a_{2i+2}x^i y \in R(C_2 \times C_4),$$

then

$$\sigma(\alpha) = CIR(A, B, C, D)$$

where $A = cir(a_1, a_2)$, $B = cir(a_3, a_4)$, $C = cir(a_5, a_6)$, $D = cir(a_7, a_8)$ and $a_i \in R$.

▪ Let $G = \langle x, y \,|\, x^4 = y^2 = 1, x^y = x^{-1} \rangle \cong D_8$. If

$$\alpha = \sum_{i=0}^{3} a_{i+1}x^i + a_{i+5}x^i y \in RD_8,$$

then

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

where $A = cir(a_1, a_2, a_3, a_4)$, $B = cir(a_5, a_6, a_7, a_8)$ and $a_i \in R$. Note that this corresponds to the four-circulant construction when $char(R) = 2$, as we mentioned above.

▪ Let $G = \langle x, y \,|\, x^4 = y^2 = 1, x^y = x^{-1} \rangle \cong D_8$. If

$$\alpha = \sum_{i=0}^{3} a_{i+1}x^i + a_{i+5}yx^i \in RD_8,$$

then

$$\sigma(\alpha) = CIR(A, B)$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = rcir(a_5, a_6, a_7, a_8)$ and $a_i \in R$. This second construction from D_8 will be denoted by D_8' in subsequent examples.

▪ Let $G = \langle x, y \mid x^4 = 1,\ y^2 = x^2,\ x^y = x^{-1} \rangle \cong Q_8$. If

$$\alpha = \sum_{i=0}^{3} a_{i+1}x^i + a_{i+5}yx^i \in RQ_8,$$

then

$$\sigma(\alpha) = \begin{pmatrix} A & B \\ C & A \end{pmatrix}$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = rcir(a_5, a_6, a_7, a_8)$, $C = rcir(a_7, a_8, a_5, a_6)$ and $a_i \in R$.

▪ Let $G = \langle x, y \mid x^4 = 1,\ y^2 = x^2,\ x^y = x^{-1} \rangle \cong Q_8$. If

$$\alpha = \sum_{i=0}^{3} a_{i+1}x^i + a_{i+5}x^i y \in RQ_8,$$

then

$$\sigma(\alpha) = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = cir(a_5, a_6, a_7, a_8)$, $C = cir(a_7, a_6, a_5, a_8)$, $D = cir(a_1, a_4, a_3, a_2)$ and $a_i \in R$. This second construction from Q_8 will be denoted by Q_8' in subsequent examples.

4.1.2 Examples of Extremal Binary Self-dual Codes obtained from the Constructions

We will focus on the new construction methods, with double-circulant and four-circulant cases being already done in the literature. We apply the constructions over the alphabets $\mathbb{F}_4+u\mathbb{F}_4$, $\mathbb{F}_4$, R_1 and $\mathbb{F}_2$.

In [20] the possible weight enumerators for a self-dual Type I $[64, 32, 12]_2$-code were obtained in two forms as:

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

Recently, 10 new codes with new weight enumerators in $W_{64,2}$ have been constructed in [74] by considering the R_3-lifts of the extended binary Hamming code. In [71], 15 new codes of length 64 with new weight enumerators have been constructed, and most recently in [1], 5 new codes were found. Together with these the existence of codes is known for β =14, 16, 18, 20, 22, 24, 25, 26, 28, 29, 30, 32, 34, 35, 36, 38, 39, 44, 46, 53, 59, 60, 64 and 74 in $W_{64,1}$ and for β =0,..., 18, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 40, 41, 42, 44, 45, 48, 50, 51, 52, 56, 58, 64, 72, 80, 88, 96, 104, 108, 112, 114, 118, 120 and 184 in $W_{64,2}$.

Throughout the text extremal Type I binary self-dual codes of length 64 have weight enumerators in $W_{64,2}$. Hence, β values in the upcoming tables correspond to $W_{64,2}$. In this section, we construct self-dual codes with weight enumerators β =0, 2, 4, 6, 8, 9, 10, 12, 13, 14, 16, 17, 18, 20, 21, 24, 26, 28, 29, 30, 32, 36, 40, 44, 48 and 52 in $W_{64,2}$. Recently, codes with weight enumerators β = 13, 17, 21, 26, 29 and 52 in $W_{64,2}$ have been constructed in [71, 74] for the first time in the literature. We give an alternative construction for these.

The constructions emerging from groups of order 8 results in self-dual codes of length 16.

We need a brief notation for the elements of $\mathbb{F}_4 + u\mathbb{F}_4$. We use the ordered basis $\{u\omega, \omega, u, 1\}$ to express the elements of $\mathbb{F}_4 + u\mathbb{F}_4$ as binary strings of length 4, which then are transformed into the well-known hexadecimal notation. For instance, $1 + u\omega$ corresponds to 1001, which is represented by the hexadecimal 9.

Example 4.1.1 *Applying the first method of construction coming from the group Q_8 to the binary field, we get the following extremal binary self-dual codes of length 16: The same codes are also obtained from the second construction as well.*

In Table 4.2, extremal binary self-dual codes of length 64 have been constructed by D_8' for $\mathbb{F}_4 + u\mathbb{F}_4$.

The results for the group Q_8 have been listed in Table 4.3.

Table 4.1: Extremal binary self-dual codes from Q_8

(a_1, a_2, a_3, a_4)	(a_5, a_6, a_7, a_8)	$\lvert Aut(C)\rvert$	Type
$(0,0,0,0)$	$(0,1,1,1)$	$2^{13} \times 3^2 \times 7^2$	Type II
$(0,0,0,1)$	$(1,1,1,1)$	$2^{13} \times 3^2$	Type I
$(0,1,1,1)$	$(1,1,1,1)$	$2^{14} \times 3^2 \times 5 \times 7$	Type II

Table 4.2: The construction D_8' over $\mathbb{F}_4 + u\mathbb{F}_4$

r_A	r_B	$\lvert Aut(C)\rvert$	β
$(036E)$	$(83B0)$	2^4	0
$(0FB4)$	$(137E)$	2^5	0
$(2F34)$	$(9BD6)$	2^4	4
$(16F1)$	(4455)	2^5	4
$(3FC7)$	(4620)	2^4	8
$(45BF)$	$(C022)$	2^5	8
$(8AB1)$	$(B6E8)$	2^4	12
$(66FF)$	(3846)	2^5	12
$(6FC1)$	$(8C09)$	2^4	16
$(6FB1)$	$(03B0)$	2^4	20
$(773D)$	$(F30B)$	2^4	24
$(996B)$	(8408)	2^5	24
$(2DBE)$	(1174)	2^4	28
$(CCDD)$	$(B066)$	2^5	28
$(25B6)$	$(91F4)$	2^4	32
$(3E2D)$	$(B855)$	2^5	32
$(0C17)$	$(648B)$	2^4	36
$(44FF)$	$(984E)$	2^5	36
$(8FA8)$	$(B47C)$	2^5	40
$(CCDD)$	$(3AEC)$	2^5	44
$(66F5)$	$(304C)$	$2^4 \times 3$	44
$(E65F)$	$(1AC4)$	2^5	48
$(C47D)$	$(90E6)$	2^5	52

Table 4.3: The construction Q_8 over $\mathbb{F}_4 + u\mathbb{F}_4$

r_A	r_B	r_C	$\lvert Aut(C)\rvert$	β
$(55EE)$	$(C522)$	$(7E99)$	2^4	0
$(5FE6)$	$(4F28)$	(2146)	2^4	2
$(FFEE)$	$(C7AA)$	$(7C11)$	2^4	4
(4273)	$(5E28)$	$(6F19)$	2^3	6
$(F566)$	(1855)	$(A9E4)$	2^3	8
$(DBCA)$	$(6EB8)$	$(B365)$	2^3	10
$(DD44)$	$(E588)$	$(5E33)$	2^4	12
$(D544)$	$(CF88)$	$(A3E4)$	2^3	14
$(5FC4)$	$(6D0A)$	$(A9AE)$	2^4	16
(7162)	$(CE10)$	$(19C7)$	2^3	18
$(73E0)$	(6418)	(3945)	2^3	20
$(F7EE)$	$(185F)$	$(89CE)$	2^3	26
$(7D6E)$	$(45A8)$	$(DE33)$	2^5	28
$(55EE)$	$(4F22)$	$(5E33)$	2^4	30

Table 4.4: Extremal binary self-dual codes from C_2^3

(a_1, a_2)	(a_3, a_4)	(a_5, a_6)	(a_7, a_8)	$\lvert Aut(C)\rvert$	Type
$(0,0)$	$(0,0)$	$(0,1)$	$(1,1)$	$2^{13} \times 3^2 \times 7^2$	Type II
$(0,0)$	$(0,1)$	$(1,1)$	$(1,1)$	$2^{13} \times 3^2$	Type I
$(0,1)$	$(1,1)$	$(1,1)$	$(1,1)$	$2^{14} \times 3^2 \times 5 \times 7$	Type II

Example 4.1.2 *We apply the construction method coming from C_2^3 over the binary case, with length* 16*. The results are listed in Table 4.4 and the full calculation on Magma is shown in Appendix A.2.*

Example 4.1.3 *We can apply these constructions to higher lengths as well. For example, if we take blocks of length* 4 *in the construction coming from C_2^3, we can form self-dual codes of length* 32*. Taking $A = cir(0,0,0,1)$, $B = cir(0,0,0,1)$, $C = cir(0,0,0,1)$ and $D = cir(1,1,1,1)$ in C_2^3 construction, we get the extremal Type II binary self-dual code of length* 8 *with automorphism group of order $2^9 \times 3^2 \times 5$.*

The construction Q_8' have been used for $\mathbb{F}_4 + u\mathbb{F}_4$ in Table 4.5

Table 4.5: The construction Q_8' over $\mathbb{F}_4 + u\mathbb{F}_4$

r_A	r_B	r_C	r_D	$\lvert Aut(C)\rvert$	β
(0577)	$(B179)$	$(79B1)$	$(7F0D)$	2^4	8
$(275F)$	$(33F9)$	$(519B)$	$(7F07)$	2^3	9
$(2DFF)$	(9179)	$(D991)$	$(7F8D)$	2^3	12
$(A57D)$	$(33D9)$	$(F913)$	$(F72F)$	2^3	13
$(ADDF)$	$(9BF3)$	$(FB93)$	$(DDAF)$	2^4	16
$(8D75)$	$(9BD1)$	$(F993)$	$(DFA7)$	2^3	17
$(8F57)$	$(915B)$	$(5B31)$	$(F50D)$	2^3	21
$(8F5D)$	$(937B)$	(5911)	(7587)	2^3	28
$(07FF)$	(9359)	$(F913)$	$(FF87)$	2^3	29

4.2 Constructions coming from groups of order 16

In this section, we will apply the same approach that we used in the previous section to describe construction methods coming from groups of order 16 and to apply these construction methods to find extremal self-dual binary codes. For the constructions in this section, we need the definition of a so-called g-circulant matrix from [22]:

Definition 4.2.1 *Let $0 \leq g \leq n$. A g-circulant matrix B of order n is a matrix of the form*

$$B = g - cir(a_1, a_2, \ldots, a_n) = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_{n-g+1} & a_{n-g+2} & \cdots & a_{n-g} \\ a_{n-2g+1} & a_{n-2g+2} & \cdots & a_{n-2g} \\ \vdots & \vdots & \ddots & \vdots \\ a_{g+1} & a_{g+2} & \cdots & a_g \end{pmatrix}$$

where each subscript are calculated modulo n.

Note that,each row of B is the previous row moved g places to the right.

▪ Let $G = \langle x, y \mid x^4 = y^4 = 1,\ xy = yx \rangle \cong C_4 \times C_4$. If $\alpha = \sum_{i=0}^{3}\sum_{j=0}^{3} a_{1+i+4j}x^i y^j \in R(C_4 \times C_4)$, then

$$\sigma(\alpha) = CIR(A, B, C, D)$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = cir(a_5, a_6, a_7, a_8)$, $C = cir(a_9, a_{10}, a_{11}, a_{12})$, $D = cir(a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y \mid x^4 = y^4 = 1,\ xyxy = 1,\ yx^3 = xy^3 \rangle \cong G_{4,4}$. If $\alpha = \sum_{i=0}^{3}\sum_{j=0}^{3} a_{1+i+4j}x^i y^j \in RG_{4,4}$, then

$$\sigma(\alpha) = CIR(A, B, C, D)$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = 3 - cir(a_5, a_6, a_7, a_8)$, $C = cir(a_9, a_{10}, a_{11}, a_{12})$, $D = 3 - cir(a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y \mid x^4 = y^4 = 1,\ yx = x^{-1}y \rangle \cong C_4 \rtimes C_4$. If $\alpha = \sum_{i=0}^{3}\sum_{j=0}^{3} a_{1+i+4j}x^i y^j \in R(C_4 \rtimes C_4)$, then

$$\sigma(\alpha) = CIR(A, B, C, D)$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = rcir(a_5, a_6, a_7, a_8)$, $C = cir(a_9, a_{10}, a_{11}, a_{12})$,
$D = rcir(a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y \mid x^8 = y^2 = 1,\ xy = yx \rangle \cong C_2 \times C_8$. If $\alpha = \sum_{i=0}^{7}\sum_{j=0}^{1} a_{1+i+8j}x^i y^j \in R(C_2 \times C_8)$, then

$$\sigma(\alpha) = CIR(A, B)$$

where $A = cir(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$, $B = cir(a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y \mid x^8 = y^2 = 1,\ xy = yx \rangle \cong C_2 \times C_8$. If $\alpha = \sum_{i=0}^{7}\sum_{j=0}^{1} a_{1+2i+j}x^i y^j \in R(C_2 \times C_8)$, then

$$\sigma(\alpha) = CIR(A, B, C, D, E, F, G, H)$$

where $A = cir(a_1, a_2)$, $B = cir(a_3, a_4)$, $C = cir(a_5, a_6)$, $D = cir(a_7, a_8)$, $E = cir(a_9, a_{10})$, $F = cir(a_{11}, a_{12})$, $G = cir(a_{13}, a_{14})$, $H = cir(a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y \mid x^8 = y^2 = 1,\ x^y = x^5 \rangle \cong M_{16}$. If $\alpha = \sum_{i=0}^{7}\sum_{j=0}^{1} a_{1+i+8j}y^j x^i \in RM_{16}$, then

$$\sigma(\alpha) = CIR(A, B)$$

where $A = cir(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$, $B = 3 - cir(a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y \mid x^8 = y^2 = 1, x^y = x^{-1} \rangle \cong D_{16}$. If $\alpha = \sum_{i=0}^{7}\sum_{j=0}^{1} a_{1+i+8j}x^i y^j \in RD_{16}$, then

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

where $A = cir(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$, $B = cir(a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y \mid x^8 = y^2 = 1, x^y = x^{-1} \rangle \cong D_{16}$. If $\alpha = \sum_{i=0}^{7}\sum_{j=0}^{1} a_{1+i+8j}y^j x^i \in RD_{16}$, then

$$\sigma(\alpha) = CIR(A, B)$$

where $A = cir(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$, $B = rcir(a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$. This second construction coming from D_{16} will be denoted by D'_{16}.

▪ Let $G = \langle x, y \,|\, x^8 = y^2 = 1,\, x^y = x^3 \rangle \cong SD_{16}$, the semidihedral group of order 16. If $\alpha = \sum_{i=0}^{7} \sum_{j=0}^{1} a_{1+i+8j} y^j x^i \in RSD_{16}$, then

$$\sigma(\alpha) = CIR(A, B)$$

where $A = cir(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$, $B = 5 - cir(a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y \mid x^8 = 1,\ y^2 = x^8,\ x^y = x^{-1} \rangle \cong Q_{16}$. If $\alpha = \sum_{i=0}^{7} \sum_{j=0}^{1} a_{1+i+8j} y^j x^i \in RQ_{16}$, then

$$\sigma(\alpha) = \begin{pmatrix} A & B \\ C & A \end{pmatrix}$$

where $A = cir(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$, $B = rcir(a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16})$,
$C = rcir(a_{13}, a_{14}, a_{15}, a_{16}, a_9, a_{10}, a_{11}, a_{12})$ and $a_i \in R$.

▪ Let $G = \langle x, y, z \mid x^4 = y^2 = z^2 = 1, xy = yx, xz = zx,\ yz = zy \rangle \cong C_4 \times C_2 \times C_2$. If $\alpha = \sum_{i=0}^{3} x^i (a_{i+1} + a_{i+5} y + a_{i+9} z + a_{i+13} yz) \in R(C_4 \times C_2 \times C_2)$, then

$$\sigma(\alpha) = P_e \otimes CIR(A, B) + P_{(1,2)} \otimes CIR(C, D)$$

where $\mathcal{G} = \{e, (1,2)\}$, $A = cir(a_1, a_2, a_3, a_4)$, $B = cir(a_5, a_6, a_7, a_8)$, $C = cir(a_9, a_{10}, a_{11}, a_{12})$,
$D = cir(a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y, z \mid x^4 = y^2 = z^2 = 1, xy = yx, xz = zx,\ yz = zy \rangle \cong C_4 \times C_2 \times C_2$. If $\alpha = \sum_{i=0}^{3} x^i (a_{1+4i} + a_{2+4i} y + a_{3+4i} z + a_{4+4i} yz) \in R(C_4 \times C_2 \times C_2)$, then

$$\sigma(\alpha) = CIR(A, B, C, D)$$

where $A = CIR(A_1, A_2)$, $B = CIR(B_1, B_2)$, $C = CIR(C_1, C_2)$, $D = CIR(D_1, D_2)$, $A_1 = cir(a_1, a_2)$, $A_2 = cir(a_3, a_4)$, $B_1 = cir(a_5, a_6)$, $B_2 = cir(a_7, a_8)$, $C_1 = cir(a_9, a_{10})$, $C_2 = cir(a_{11}, a_{12})$, $D_1 = cir(a_{13}, a_{14})$, $D_2 = cir(a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y, z \,|\, x^4 = y^2 = z^2 = 1, x^y = x^{-1}, xz = zx, yz = zy \rangle \cong C_2 \times D_8$. If

$$\alpha = \sum_{i=0}^{3} x^i (a_{i+1} + a_{i+5} y + a_{i+9} z + a_{i+13} yz) \in R(C_2 \times D_8),$$

then

$$\sigma(\alpha) = \begin{pmatrix} A & B & C & D \\ B^T & A^T & D^T & C^T \\ C & D & A & B \\ D^T & C^T & B^T & A^T \end{pmatrix}$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = cir(a_5, a_6, a_7, a_8)$, $C = cir(a_9, a_{10}, a_{11}, a_{12})$, $D = cir(a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y, z \,|\, x^4 = y^2 = z^2 = 1, x^y = x^{-1}, xz = zx, yz = zy \rangle \cong C_2 \times D_8$. If

$$\alpha = \sum_{i=0}^{3} (a_{i+1} + a_{i+5}y + a_{i+9}z + a_{i+13}yz)x^i \in R(C_2 \times D_8),$$

then

$$\sigma(\alpha) = P_e \otimes CIR(A, B) + P_{(1,2)} \otimes CIR(C, D)$$

where $\mathcal{G} = \{e, (1,2)\}$, $A = cir(a_1, a_2, a_3, a_4)$, $B = rcir(a_5, a_6, a_7, a_8)$, $C = cir(a_9, a_{10}, a_{11}, a_{12})$, $D = rcir(a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y, z \mid x^4 = z^2 = 1,\ y^2 = x^2,\ x^y = x^{-1}\, xz = zx,\ yz = zy \rangle \cong C_2 \times Q_8$. If

$$\alpha = \sum_{i=0}^{3} (a_{i+1} + a_{i+5}y + a_{i+9}z + a_{i+13}yz)x^i \in R(C_2 \times Q_8),$$

then

$$\sigma(\alpha) = \begin{pmatrix} A & B & D & E \\ C & A & F & D \\ D & E & A & B \\ F & D & C & A \end{pmatrix},$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = rcir(a_5, a_6, a_7, a_8)$, $C = rcir(a_7, a_8, a_5, a_6)$, $D = cir(a_9, a_{10}, a_{11}, a_{12})$, $E = rcir(a_{13}, a_{14}, a_{15}, a_{16})$, $F = rcir(a_{15}, a_{16}, a_{13}, a_{14})$ and $a_i \in R$.

▪ Let $G = \langle x, y, z \mid x^4 = z^2 = 1,\ y^2 = x^2,\ x^y = x^{-1}\, xz = zx,\ yz = zy \rangle \cong C_2 \times Q_8$. If

$$\alpha = \sum_{i=0}^{3} x^i(a_{i+1} + a_{i+5}y + a_{i+9}z + a_{i+13}yz) \in R(C_2 \times Q_8),$$

then

$$\sigma(\alpha) = \begin{pmatrix} A & B & D & E \\ C & A^T & F & D^T \\ D & E & A & B \\ F & D^T & C & A^T \end{pmatrix}$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = cir(a_5, a_6, a_7, a_8)$, $C = cir(a_7, a_6, a_5, a_8)$, $D = cir(a_9, a_{10}, a_{11}, a_{12})$, $E = cir(a_{13}, a_{14}, a_{15}, a_{16})$, $F = cir(a_{15}, a_{14}, a_{13}, a_{16})$ and $a_i \in R$. This second construction coming from $C_2 \times Q_8$ will be denoted by $(C_2 \times Q_8)'$.

▪ Let $G = \langle x, y, z \mid x^4 = y^2 = z^2 = 1,\ zyzx^2y = 1,\ yxyx^3 = 1,\ zxzx^3 = 1\rangle \cong \mathcal{P}_{16}$. If $\alpha = \sum_{i=0}^{3} x^i(a_{i+1} + a_{i+5}y + a_{i+9}z + a_{i+13}yz) \in R\mathcal{P}_{16}$, then

$$\sigma(\alpha) = \begin{pmatrix} A & B & C & D \\ B & A & E & F \\ C & D & A & B \\ E & F & B & A \end{pmatrix},$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = cir(a_5, a_6, a_7, a_8)$, $C = cir(a_9, a_{10}, a_{11}, a_{12})$, $D = cir(a_{13}, a_{14}, a_{15}, a_{16})$, $E = cir(a_{15}, a_{16}, a_{13}, a_{14})$, $F = cir(a_{11}, a_{12}, a_9, a_{10})$ and $a_i \in R$.

▪ Let $G = \langle x_i \,|\, x_i^2 = 1, x_ix_j = x_jx_i\ (i \neq i)\rangle \cong C_2^4$ where $1 \leq i, j \leq 4$. If

$$\begin{aligned}\alpha = a_1 + a_2x_1 + a_3x_2 + a_4x_1x_2 + a_5x_3 + a_6x_1x_3 + a_7x_2x_3 + a_8x_1x_2x_3 + a_9x_4 + a_{10}x_1x_4 \\ + a_{11}x_2x_4 + a_{12}x_1x_2x_4 + a_{13}x_3x_4 + a_{14}x_1x_3x_4 + a_{15}x_2x_3x_4 + a_{16}x_1x_2x_3x_4 \in RC_2^4\end{aligned}$$

then

$$\sigma(\alpha) = P_e \otimes CIR(A, B) + P_{(1,2)(3,4)} \otimes CIR(C, D) + P_{(1,3)(2,4)} \otimes CIR(E, F) + P_{(1,4)(2,3)} \otimes CIR(G, H)$$

where $\mathcal{G} = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$, $A = cir(a_1, a_2)$, $B = cir(a_3, a_4)$, $C = cir(a_5, a_6)$, $D = cir(a_7, a_8)$, $E = cir(a_9, a_{10})$, $F = cir(a_{11}, a_{12})$, $G = cir(a_{13}, a_{14})$, $H = cir(a_{15}, a_{16})$ and $a_i \in R$.

4.2.1 Examples of Extremal Binary Self-dual Codes obtained from the constructions

In this section, we give examples obtained from group of order $16\dot{}$. The construction is applied over the binary alphabet and to the ring R_1. Using g-circulant matrices to construct self-dual codes is a distinctive method. In the following example we use the construction SD_{16}. Note that, here we present a new way of constructing codes. Using this construction means that we can extend these codes to produces new codes in the following section.

Example 4.2.2 *Applying the semidihedral construction to the binary case length 32, up to equivalence, we get one extremal binary self-dual code of length 32 and one binary self-dual code of parameter* $[32, 16, 6]$. *Lifting these to the ring* R_1, *in other words, applying the semidihedral construction to the ring* R_1 *we get the following results:*

Lifts of [32,16,6]: *Up to equivalence we get 14 extremal binary self-dual codes of length* 64. *Out of these, 11 are of Type II. The three Type I codes have two different weight enumerators. If we take*

$$(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8) = (u, u, 0, 0, 0, 1, u, 1)$$

and

$$(a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}) = (u, 0, u, 0, 1, 1, 1, u),$$

then the code obtained with the semidhedral construction over R_1 *with these values has as its Gray image, a Type I extremal binary self-dual code that has a weight enumerator with* $\beta = 0$ *in* $W_{64,2}$.

Table 4.6: The constructions D'_{16} and SD_{16} over $\mathbb{F}_2 + u\mathbb{F}_2$

Construction	r_A	r_B	$\lvert Aut(C)\rvert$	β
D'_{16}	(22221113)	(22130131)	2^5	0
D'_{16}	(22201111)	(02130311)	2^5	16
D'_{16}	(22001113)	(20132111)	2^5	32
D'_{16}	(22001131)	(22110133)	2^5	48
SD_{16}	(00332312)	(23331102)	2^5	32

If we take

$$(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8) = (u, u, u, 0, 0, 1, 0, 1)$$

and

$$(a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}) = (u, 0, u, u, 1, 1, 1, 0),$$

then we get a code with the same weight enumerator($\beta = 0$ in $W_{64,2}$.)

If we take

$$(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8) = (u, u, u, 0, 0, 1, 0, 1)$$

and

$$(a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}) = (u, 0, u, 0, 1, 1, 1, u),$$

then we get a Type I extremal binary self-dual code that has a weight enumerator with $\beta = 16$ in $W_{64,2}$.

Lifts of [32,16,8]: *Up to equivalence we get 13 extremal binary self-dual codes, of which 12 are Type II and the one Type I code has a weight enumerator with $\beta = 16$ in $W_{64,2}$.*

The constructions $G_{4,4}$ and M_{16} use 3-circulant and 5-circulant matrices, respectively. When these are applied over the binary alphabet we obtain self-dual binary codes of length 32. Those are not listed in order to save space.

In order to simplify the notation in tables we use 2 and 3 for u and $1 + u$, respectively. When we apply the constructions D'_{16} and SD_{16} over $\mathbb{F}_2 + u\mathbb{F}_2$ we obtain extremal binary self-dual codes of length 64 as binary images. Those are listed in Table 4.6.

In Tables 4.7, 4.8 and 4.9 we apply the constructions Q_{16}, C_2Q_8, P_{16} and $(C_2Q_8)'$, respectively.

4.3 New Extremal binary self-dual codes of length 68

We will now explain how we find new extremal binary self-dual codes of length 68 by combining the construction methods in sections 4 and 5 and an extension theorem. We first recall that, he possible weight enumerators of an extremal self-dual binary code of length 68 are determined in

Table 4.7: The construction Q_{16} over $\mathbb{F}_2 + u\mathbb{F}_2$

r_A	r_B	r_C	$\lvert Aut(C)\rvert$	β
(20131120)	(11023321)	(00112232)	2^4	0
(03003112)	(21103301)	(02311020)	2^5	0
(10110221)	(33231212)	(22320303)	2^4	12
(01221112)	(21323321)	(20313222)	2^4	16
(10130021)	(31231032)	(00122103)	2^4	20
(23021312)	(01121303)	(22333022)	2^4	32
(21223310)	(21103303)	(00331220)	2^5	32
(32110203)	(13013012)	(22300123)	2^5	36

Table 4.8: Codes by C_2Q_8 and P_{16} over $\mathbb{F}_2 + u\mathbb{F}_2$

Construction	r_A	r_B	r_C	r_D	r_E	r_F	$\lvert Aut(C)\rvert$	β
C_2Q_8	(1213)	(2331)	(3123)	(0021)	(1230)	(0220)	2^4	8
C_2Q_8	(1233)	(0311)	(1301)	(0003)	(3032)	(0200)	2^4	24
C_2Q_8	(2221)	(3210)	(2301)	(3312)	(0221)	(1330)	2^5	24
C_2Q_8	(2001)	(1032)	(2103)	(1310)	(2003)	(1132)	2^4	40
P_{16}	(2010)	(0320)	(3103)	(1230)	(3311)	(3301)	2^4	8
P_{16}	(2310)	(0220)	(3320)	(1123)	(1231)	(2011)	2^5	8
P_{16}	(3021)	(1331)	(0211)	(0223)	(3022)	(3302)	2^6	8
P_{16}	(0212)	(0322)	(3123)	(3212)	(1333)	(3321)	2^4	24
P_{16}	(3223)	(3113)	(0031)	(2003)	(1220)	(1300)	2^5	24

Table 4.9: Type I extremal self-dual binary codes of length 64 via $(C_2Q_8)'$

r_A	r_B	r_C	r_D	r_E	r_F	r_G	r_H	$\lvert Aut(C)\rvert$	β
(1331)	(0033)	(0330)	(0220)	(0023)	(0233)	(0332)	(3013)	2^4	8
(1331)	(2013)	(2130)	(0220)	(2003)	(0013)	(0130)	(3011)	2^4	24

[28] as follows:

$$\begin{aligned} W_{68,1} &= 1 + (442 + 4\beta)\, y^{12} + (10864 - 8\beta)\, y^{14} + \cdots, 104 \leq \beta \leq 1358, \\ W_{68,2} &= 1 + (442 + 4\beta)\, y^{12} + (14960 - 8\beta - 256\gamma)\, y^{14} + \ldots \end{aligned}$$

where $0 \leq \gamma \leq 9$ by [56]. The existence of codes is known for many parameters for both of the cases. In $W_{68,2}$ codes exist for $\gamma = 0, 1, 2, 3, 4$ and 6. For a list of known codes in $W_{68,2}$ we refer to [72]. In order to save space, we list only the parameters for $\gamma = 4$ in $W_{68,2}$, which is;

$$\beta \in \left\{ 2m \;\middle|\; \begin{array}{c} 43, 48, 49, 51, 52, 54, 55, 56, 58, 60, 61, 62, \\ 64, 65, 67, \ldots, 71, 75, \ldots, 88, 90, 97, 98 \end{array} \right\}.$$

In this section, we obtain 10 new extremal binary self-dual codes of length 68. More precisely, we construct codes whose weight enumerators have $\gamma = 4$ and β =126, 129, 132, 141, 144, 145, 146, 148, 157 and 161 in $W_{68,2}$.

In order to construct new codes of length 68 we use the following Theorem 1.2.27 over $\mathbb{F}_2 + u\mathbb{F}_2$.

By using groups of order 8 we obtain codes of length 16 over $\mathbb{F}_4 + u\mathbb{F}_4$ with binary images as $[64, 32, 12]_2$ self-dual codes. We map the codes to the ring $\mathbb{F}_2 + u\mathbb{F}_2$ via the Gray map $\psi_{\mathbb{F}_4 + u\mathbb{F}_4}$ and extend the $\mathbb{F}_2 + u\mathbb{F}_2$-image. Consider the following codes over $\mathbb{F}_4 + u\mathbb{F}_4$:

$\mathcal{C}_i$	Construction	r_A	r_B	β in $W_{64,2}$	$\lvert Aut\,(\mathcal{C}_i)\rvert$
$\mathcal{C}_1$	D_8	$(6ED7)$	$(D40A)$	24	2^5
$\mathcal{C}_2$	${D_8}'$	$(2DBE)$	(1174)	28	2^4

We now extend these codes to find new codes of length 68. The new codes are tabulated in Table 4.10. In order to save space the element $1 + u$ of $\mathbb{F}_2 + u\mathbb{F}_2$ is denoted by 3 in the extension vector X. Thus we have the following main theorem about the existence of extremal binary self-dual codes of length 68.

Theorem 4.3.1 *Together with the codes in Table 4.10 the existence of extremal self-dual binary codes is known for* 46 *parameters with* $\gamma = 4$ *in* $W_{68,2}$.

Table 4.10: Ten new extremal self-dual codes of length 68 with $\gamma = 4$

$\mathcal{C}_{68,i}$	$\mathcal{C}_j$	c	X	β
$\mathcal{C}_{68,1}$	$\mathcal{C}_1$	$1+u$	$(u31uu0uuu0uu0u303u3033333011uu3u)$	126
$\mathcal{C}_{68,2}$	$\mathcal{C}_2$	1	$(300u11331003u1130333110u0301110u)$	129
$\mathcal{C}_{68,3}$	$\mathcal{C}_1$	$1+u$	$(u33u000000uu0u30303013311u11uu3u)$	132
$\mathcal{C}_{68,4}$	$\mathcal{C}_1$	$1+u$	$(033uuuuu000uuu3u103u13331013u030)$	144
$\mathcal{C}_{68,5}$	$\mathcal{C}_2$	1	$(1uu011313u01u331033333u0u3u131u0)$	145
$\mathcal{C}_{68,6}$	$\mathcal{C}_1$	1	$(011u0uuu0u0uu03u303031111033uu1u)$	146
$\mathcal{C}_{68,7}$	$\mathcal{C}_1$	1	$(0130uuu0000u00303u1011311u13u010)$	148
$\mathcal{C}_{68,8}$	$\mathcal{C}_2$	$1+u$	$(3uu011331003u113u31131u0u30313uu)$	155
$\mathcal{C}_{68,9}$	$\mathcal{C}_2$	$1+u$	$(1u00131330u3u131u313310u0303310u)$	157
$\mathcal{C}_{68,10}$	$\mathcal{C}_2$	$1+u$	$(1uuu33133u03u133u13313u0u3u1130u)$	161

Chapter 5

Double Bordered Constructions for Self-Dual Codes Induced from Group Rings

In previous chapters, we have discussed the double circulant construction as a technique for constructing self-dual codes over a ring R, from a generator matrix of the form $(I \,|\, A)$ where A is an $n \times n$ circulant matrix over R. As previously mentioned, the double circulant construction is one of the most extensively used techniques for producing self-dual codes. This technique can be modified to a bordered-double circulant construction by considering generator matrices of the form ([59, 67]):

$$\left[\begin{array}{c|c|c} & \alpha & \beta \cdots \beta \\ \hline & \beta & \\ I_n & \vdots & A \\ & \beta & \end{array}\right]$$

where $\alpha, \beta \in R$. We can think of this technique as essentially extending a self-dual code of $2n$ to a self-dual code of length $2n+2$. In [50], new self-dual codes of length $2n+2$ were constructed using the following construction

$$\left(\begin{array}{cc|ccc|ccc} 1 & 0 & z_1 & \dots & z_n & z_{n+1} & \dots & z_{2n} \\ \hline y_1 & y_1 & & & & & & \\ \vdots & \vdots & & I & & & A & \\ y_n & y_n & & & & & & \end{array}\right).$$

where $z = (z_1, \dots, z_{2n}) \in R^{2n}$, $y_i = r_i$ and r_i is the i^{th} row of the generator matrix $(I \,|\, A)$ and A is an $n \times n$ circulant matrix over a ring R. Additionally, in [9], self-dual codes of length $2n+2$ were constructed from the following generator matrix:

$$\left(\begin{array}{ccc|ccc|cc} x_1 & \cdots & x_n & 0 & \cdots & 0 & 1 & 0 \\ \hline & & & & & & x_1 & x_1 \\ & I & & & A & & \vdots & \vdots \\ & & & & & & x_n & x_n \end{array}\right).$$

where $x_1 \in R$ and A is an $n \times n$ circulant matrix over a ring R. In [55], self-dual codes of length $2n+4$ were constructed from generator matrices of the form:

$$\left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & x_1 \\ 0 & 1 & 0 & 0 & x_2 \\ \hline & y_1 & & & r_1 \\ & \vdots & & & \vdots \\ & y_n & & & r_n \end{array}\right)$$

where x_i are vectors of length $2n$, y_i are vectors of length 4, r_i is the i^{th} row of the genertor matrix $(I \,|\, A)$ and A is an $n \times n$ circulant matrix over a ring R.

In [27], the authors combine a bordered double-circulant construction and group rings to construct self-dual codes from the construction:

$$\left(\begin{array}{c|ccc|c|ccc} \gamma_1 & \alpha_1 & \cdots & \alpha_1 & \gamma_2 & \alpha_2 & \cdots & \alpha_2 \\ \hline \alpha_1 & & & & \alpha_2 & & & \\ \vdots & & I_n & & \vdots & & \sigma(v) & \\ \alpha_1 & & & & \alpha_2 & & & \end{array}\right).$$

Considering techniques previously used and the success from each method, a logical question would be whether these techniques can be extended and/or combined to construct more self-dual codes. In this chapter, we consider constructing self-dual codes from the following generator matrix:

$$\left[\begin{array}{cc|ccc|cc|ccc} \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_3 \; \alpha_4 \cdots \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \cdots & \alpha_7 \; \alpha_8 \cdots \alpha_8 \\ \alpha_2 & \alpha_1 & \alpha_4 & \cdots & \alpha_4 \; \alpha_3 \cdots \alpha_3 & \alpha_6 & \alpha_5 & \alpha_8 & \cdots & \alpha_8 \; \alpha_7 \cdots \alpha_7 \\ \hline \alpha_3 & \alpha_4 & & & & \alpha_7 & \alpha_8 & & & \\ \vdots & \vdots & & & & \vdots & \vdots & & & \\ \alpha_3 & \alpha_4 & & & & \alpha_7 & \alpha_8 & & & \\ \alpha_4 & \alpha_3 & & I_n & & \alpha_8 & \alpha_7 & & \sigma(v) & \\ \vdots & \vdots & & & & \vdots & \vdots & & & \\ \alpha_4 & \alpha_3 & & & & \alpha_8 & \alpha_7 & & & \end{array}\right]$$

This chapter is organised as follows: The first section describes cyclic and dihedral groups using a different listing of elements. The corresponding structure of $\sigma(v)$ is also given here. In Section 2, we consider the new double bordered construction and look at the theory surrounding its effectiveness. We specify conditions on the construction in order to maximise its practicality and effectiveness. The final sections are allocated to the results, computed using MAGMA ([5]) and proving the

efficiency of the theory. The new extremal binary self-dual codes are listed in numerous tables and summarised in the final section. Notably, this research includes new self-dual codes of length 64, 68 and 80.

5.1 Notation

The two main groups that we use in this chapter are cyclic and dihedral groups. For these groups, we consider circulant $n \times n$ matrices denoted $cir(\alpha_1, \alpha_2, \cdots, \alpha_n)$, where each row vector is rotated one element to the right relative to the preceding row vector [22]. Furthermore, the notation $CIR(A_1, A_2, \cdots, A_m)$ denotes the $nm \times nm$ circulant matrix constructed of m smaller $n \times n$ circulant matrices, A_i. We will now look at the structure of the matrix $\sigma(v)$ where v is an element of the cyclic or dihedral group of order $2p$ where p is an odd integer.

Recall that $C'_{2p} = \langle x \mid x^{2p} = 1 \rangle$ and

$$v = \sum_{i=0}^{p-1} \sum_{j=0}^{1} \alpha_{i+pj+1} x^{2i+j} \in RC'_{2p}$$

then,

$$\sigma(v) = \begin{pmatrix} A_1 & A_2 \\ A'_2 & A_1 \end{pmatrix}$$

where $A_j = cir(\alpha_{(j-1)p+1}, \alpha_{(j-1)p+2}, \ldots, \alpha_{jp})$ and $A'_j = cir(\alpha_{jp}, \alpha_{(j-1)p+1}, \ldots, \alpha_{jp-1})$.

Alternatively, let $D_{2p} = \langle x, y \mid x^p = y^2 = 1, x^y = y^{-1} \rangle$ and

$$v = \sum_{i=0}^{p-1} \sum_{j=0}^{1} \alpha_{i+pj+1} x^i y^j \in RD_{2p}$$

then,

$$\sigma(v) = \begin{pmatrix} A_1 & A_2 \\ A_2^T & A_1^T \end{pmatrix}$$

where $A_j = cir(\alpha_{(j-1)p+1}, \alpha_{(j-1)p+2}, \ldots, \alpha_{jp})$.

5.2 Construction

Let $v \in RG$ where R is a finite Frobenius ring of characteristic 2 and G is a finite group of order $2p$ where p is odd. Define the following matrix:

$$M(\sigma) = \left[\begin{array}{cc|ccccc|cc|ccccc} \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_3 & \alpha_4 & \cdots & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \cdots & \alpha_7 & \alpha_8 & \cdots & \alpha_8 \\ \alpha_2 & \alpha_1 & \alpha_4 & \cdots & \alpha_4 & \alpha_3 & \cdots & \alpha_3 & \alpha_6 & \alpha_5 & \alpha_8 & \cdots & \alpha_8 & \alpha_7 & \cdots & \alpha_7 \\ \hline \alpha_3 & \alpha_4 & & & & & & & \alpha_7 & \alpha_8 & & & & & & \\ \vdots & \vdots & & & & & & & \vdots & \vdots & & & & & & \\ \alpha_3 & \alpha_4 & & & & I_{2p} & & & \alpha_7 & \alpha_8 & & & & \sigma(v) & & \\ \alpha_4 & \alpha_3 & & & & & & & \alpha_8 & \alpha_7 & & & & & & \\ \vdots & \vdots & & & & & & & \vdots & \vdots & & & & & & \\ \alpha_4 & \alpha_3 & & & & & & & \alpha_8 & \alpha_7 & & & & & & \end{array}\right]$$

where $\alpha_i \in R$. Let C_σ be a code that is generated by the matrix $M(\sigma)$. Then, the code C_σ has length $4p + 4$. Throughout this paper, we assume that G is a group of order $2p$ that contains a subgroup of order p where p is odd. If we fix a listing of G where the first p elements of G are the elements of H, then $\sigma(v)$ takes a certain form. The next result states the form that $\sigma(v)$ takes in this case. It also provides an important property that enables us to prove our main result.

Lemma 5.2.1 *Let R be a commutative ring. If $H = \{g_1, g_2, \ldots, g_p\}$ is a subgroup of the finite group $G = \{g_1, g_2, \ldots, g_p, g_{p+1}, \ldots, g_{2p}\}$ of order $2p$ (p is odd), then*

$$\sigma(v) = \left(\begin{array}{c|c} M_1 & M_2 \\ \hline M_2' & M_1' \end{array}\right),$$

where M_1, M_2 are $p \times p$ matrices, M_1' is permutation similar to M_1 and M_2' is permutation to M_2. Moreover

$$M_k \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = M_k^T \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = M_k' \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = {M_k'}^T \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} \mu_k \\ \vdots \\ \mu_k \end{pmatrix} \quad (k = 1, 2),$$

where $\mu_1 = \sum_{g \in H} \alpha_g$, $\mu_2 = \sum_{g \in G \backslash H} \alpha_g$.

Proof. Clearly, $M_1 = (\alpha_{g_i^{-1} g_j})_{i,j=1,\ldots,p}$, $M_2 = (\alpha_{g_i^{-1} g_{p+j}})_{i,j=1,\ldots,p}$ $M_2' = (\alpha_{g_{p+i}^{-1} g_j})_{i,j=1,\ldots,p}$ and $M_1' = (\alpha_{g_{p+i}^{-1} g_{p+j}})_{i,j=1,\ldots,p}$. Let $a \in G \backslash H$. Then, for any $1 \leq i \leq p$, $g_{p+i} \in aH$ and $g_{p+i} = a g_{\delta(i)}$ for some $1 \leq \delta(i) \leq p$. Moreover $\delta : i \to \delta(i)$ is a permutation of degree p and

$$M_1' = (\alpha_{g_{p+i}^{-1} g_{p+j}})_{i,j=1,\ldots,p} = (\alpha_{(a g_{\delta(i)})^{-1} a g_{\delta(j)}})_{i,j=1,\ldots,p} =$$

$$(\alpha_{g_{\delta(i)}^{-1} a^{-1} a g_{\delta(j)}})_{i,j=1,\ldots,p} = (\alpha_{g_{\delta(i)}^{-1} g_{\delta(j)}})_{i,j=1,\ldots,p}.$$

If we rearrange the rows and columns of the matrix $M_1 = (\alpha_{g_i^{-1} g_j})_{i,j=1,\ldots,p}$ in the order $\delta(1), \ldots \delta(p)$ we will obtain M_1'. So, M_1 is permutation similar to M_1'.

It is well known that group G of order $2p$ contains a subgroup of order 2. So there is $a \in G$ $a \neq e_G$, $a^2 = e_G$. Thus $|H| = p$, $a \notin H$. Again, let $g_{p+i} = ag_{\delta(i)}$ for some $1 \leq \delta(i) \leq p$. Moreover, $\delta : i \to \delta(i)$ is a permutation of degree p and

$$M_2 = (\alpha_{g_i^{-1}g_{p+j}})_{i,j=1,\dots,p} = (\alpha_{g_i^{-1}ag_{\delta(j)}})_{i,j=1,\dots,p},$$

$$M_2' = (\alpha_{g_{p+i}^{-1}g_j})_{i,j=1,\dots,p} = (\alpha_{(ag_{\delta(i)})^{-1}g_j})_{i,j=1,\dots,p} = (\alpha_{g_{\delta(i)}^{-1}a^{-1}g_j})_{i,j=1,\dots,p} = (\alpha_{g_{\delta(i)}^{-1}ag_j})_{i,j=1,\dots,p}.$$

Now, if we rearrange the rows of the matrix $M_2 = (\alpha_{g_i^{-1}ag_{\delta(j)}})_{i,j=1,\dots,p}$ in the order $\delta(1), \dots \delta(p)$ and if we rearrange the its columns in the order $\delta^{-1}(1), \dots \delta^{-1}(p)$ we will obtain

$$(\alpha_{g_{\delta(i)}^{-1}ag_{\delta(\delta^{-1}(j))}})_{i,j=1,\dots,p} = (\alpha_{g_{\delta(i)}^{-1}ag_j})_{i,j=1,\dots,p} = M_2'.$$

This implies that $SM_2S = M_2'$ for a permutation matrix S, which contains ones in positions $(i, \delta(i))$ $(i = 1, \dots, p)$ or, which is the same, in positions $(\delta^{-1}(j), j)$ $(j = 1, \dots, p)$.

Now, the i-th element of column $M_1 \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ is

$$\sum_{j=1}^{p} \alpha_{g_i^{-1}g_j} = \sum_{g \in H} \alpha_{g_i^{-1}g} = \sum_{g \in H} \alpha_g = \mu_1, \quad g_i \in H,\ g_i^{-1} \in H,$$

and the i-th element of column $M_1^T \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ is

$$\sum_{j=1}^{p} \alpha_{g_j^{-1}g_i} = \sum_{g \in H} \alpha_{g^{-1}g_i} = \sum_{g \in H} \alpha_{gg_i} = \sum_{g \in H} \alpha_g = \mu_1, \quad g_i \in H.$$

Thus,

$$M_1 \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = M_1^T \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_1 \end{pmatrix},$$

since we have $S \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ for any permutation matrix S, and M_1 is permutation similar to M_1'. Furthermore,

$$M_1' \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = M_1'^T \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_1 \end{pmatrix}.$$

Now, the i-th elements of columns $M_2 \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ and $M_2^T \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ respectively, are

$$\sum_{j=1}^{p} \alpha_{g_i^{-1}g_{p+j}} = \sum_{g \in G \setminus H} \alpha_{g_i^{-1}g} = \sum_{g \in G \setminus H} \alpha_g = \mu_2,$$

$$\sum_{j=1}^{p} \alpha_{g_{p+j}^{-1} g_i} = \sum_{g \in G \setminus H} \alpha_{g^{-1} g_i} = \sum_{g \in G \setminus H} \alpha_{g g_i} = \sum_{g \in G \setminus H} \alpha_g = \mu_2,$$

where $g_i \in H$ and $g_i^{-1} \in H$.

Thus,

$$M_2 \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = M_2^T \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} \mu_2 \\ \vdots \\ \mu_2 \end{pmatrix}$$

Therefore, we have $SM_1S = M_1'$ for some permutation matrix S, $S \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$, and

$$M_2' \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = M_2'^T \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} \mu_2 \\ \vdots \\ \mu_2 \end{pmatrix}.$$

■

We can now state and prove our main result.

Theorem 5.2.2 *Let R be a finite commutative Frobenius ring of characteristic 2. Let $G = \{g_1, g_2, \ldots, g_p, g_{p+1}$, be a finite group of order $2p$ and $H = \{g_1, g_2, \ldots, g_p\}$ be a subgroup of group G. Then, C_σ is a self-dual code of length $4p+4$ if and only if*

- $\sum_{i=1}^{8} \alpha_i = 0$,
- $vv^* = 1 + \sum_{i=1}^{2} (\alpha_{i+2}^2 + \alpha_{i+6}^2)\widehat{g}$,
- $(\alpha_1 + 1)\alpha_3 + \alpha_2\alpha_4 + (\alpha_5 + \mu_1)\alpha_7 + (\alpha_6 + \mu_2)\alpha_8 = 0$,
- $(\alpha_1 + 1)\alpha_4 + \alpha_2\alpha_3 + (\alpha_5 + \mu_1)\alpha_8 + (\alpha_6 + \mu_2)\alpha_7 = 0$ *and*
- $\begin{pmatrix} \alpha_1+\alpha_3^2+\alpha_4^2 & \alpha_2 & \alpha_5+\alpha_3\alpha_7+\alpha_4\alpha_8 & \alpha_6+\alpha_3\alpha_8+\alpha_4\alpha_7 & \alpha_7+\mu_1\alpha_3+\mu_2\alpha_4 & \alpha_8+\mu_1\alpha_4+\mu_2\alpha_3 \\ \alpha_2 & \alpha_1+\alpha_3^2+\alpha_4^2 & \alpha_6+\alpha_3\alpha_8+\alpha_4\alpha_7 & \alpha_5+\alpha_3\alpha_7+\alpha_4\alpha_8 & \alpha_8+\mu_1\alpha_4+\mu_2\alpha_3 & \alpha_7+\mu_1\alpha_3+\mu_2\alpha_4 \end{pmatrix}$ *has free rank 2*

where $\widehat{g} = \sum_{i=1}^{p} g_i$, $\mu_1 = \sum_{g \in H} \alpha_g$ and $\mu_2 = \sum_{g \in G \setminus H} \alpha_g$.

Proof. Let $M(\sigma) = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_2^T & I_{2p} & A_4^T & \sigma(v) \end{pmatrix}$ where $A_1 = \mathrm{circ}(\alpha_1, \alpha_2)$, $A_2 = \mathrm{CIRC}(B_1, B_2)$, $A_3 = \mathrm{circ}(\alpha_1, \alpha_2)$, $A_4 = \mathrm{CIRC}(B_3, B_4)$, $B_1 = (\alpha_3, \ldots, \alpha_3) \in R^p$, $B_2 = (\alpha_4, \ldots, \alpha_4) \in R^p$, $B_3 = (\alpha_7, \ldots, \alpha_7) \in R^p$ and $B_4 = (\alpha_8, \ldots, \alpha_8) \in R^p$. Then

$$M(\sigma)M(\sigma)^T = \begin{pmatrix} A_1A_1^T + A_2A_2^T + A_3A_3^T + A_4A_4^T & A_1A_2 + A_2 + A_3A_4 + A_4\sigma(v)^T \\ A_2^TA_1^T + A_2^T + A_4^TA_3^T + \sigma(v)A_4^T & A_2^TA_2 + I_{2p} + A_4^TA_4 + \sigma(v)\sigma(v)^T \end{pmatrix}.$$

Now,

$$A_1A_1^T + A_2A_2^T + A_3A_3^T + A_4A_4^T = \text{circ}\left(\sum_{i=1}^{2}(\alpha_i^2 + p\alpha_{i+2}^2 + \alpha_{i+4}^2 + p\alpha_{i+6}^2), 0\right) = \text{circ}\left(\sum_{i=1}^{8}\alpha_i^2, 0\right)$$

and

$$A_2^TA_2 + I_{2p} + A_4^TA_4 + \sigma(v)\sigma(v)^T = \sum_{i=1}^{2}(\alpha_{i+2}^2 + \alpha_{i+6}^2)\text{CIRC}(\mathbf{A}, \mathbf{0}) + I_{2p} + \sigma(vv^*)$$

where $\mathbf{A} = \text{circ}(\underbrace{1, \ldots, 1}_{p-\text{times}})$ and $\mathbf{0} = \text{circ}(\underbrace{0, \ldots, 0}_{p-\text{times}})$. It follows from Lemma 5.2.1 that

$$\sigma(v)A_4^T = \begin{pmatrix} M_1 & M_2 \\ M_2' & M_1' \end{pmatrix} \begin{pmatrix} \alpha_7 & \alpha_8 \\ \vdots & \vdots \\ \alpha_7 & \alpha_8 \\ \alpha_8 & \alpha_7 \\ \vdots & \vdots \\ \alpha_8 & \alpha_7 \end{pmatrix} = \begin{pmatrix} \mu_1\alpha_7+\mu_2\alpha_8 & \mu_1\alpha_8+\mu_2\alpha_7 \\ \vdots & \vdots \\ \mu_1\alpha_7+\mu_2\alpha_8 & \mu_1\alpha_8+\mu_2\alpha_7 \\ \mu_1\alpha_8+\mu_2\alpha_7 & \mu_1\alpha_7+\mu_2\alpha_8 \\ \vdots & \vdots \\ \mu_1\alpha_8+\mu_2\alpha_7 & \mu_1\alpha_7+\mu_2\alpha_8 \end{pmatrix} = \text{CIRC}((\mu_1\alpha_7+\mu_2\alpha_8)c, (\mu_1\alpha_8+\mu_2\alpha_7)c)$$

where $c = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$. Additionally,

$$\begin{aligned} A_2^TA_1^T + A_2^T + A_4^TA_3^T + \sigma(v)A_4^T =& \text{CIRC}((\alpha_1\alpha_3 + \alpha_2\alpha_4)c, (\alpha_1\alpha_4 + \alpha_2\alpha_3)c) + \text{CIRC}(\alpha_3c, \alpha_4c) \\ &+ \text{CIRC}((\alpha_5\alpha_7 + \alpha_6\alpha_8)c, (\alpha_5\alpha_8 + \alpha_6\alpha_7)c) \\ &+ \text{CIRC}((\mu_1\alpha_7 + \mu_2\alpha_8)c, (\mu_1\alpha_8 + \mu_2\alpha_7)c) \end{aligned}$$

$$= \text{CIRC}(((\alpha_1 + 1)\alpha_3 + \alpha_2\alpha_4 + (\alpha_5 + \mu_1)\alpha_7 + (\alpha_6 + \mu_2)\alpha_8)c, ((\alpha_1 + 1)\alpha_4 + \alpha_2\alpha_3 + (\alpha_5 + \mu_1)\alpha_8 + (\alpha_6 + \mu_2)\alpha_7)c)$$

.

Clearly, $M(\sigma)M(\sigma)^T$ is a symmetric matrix and C_σ is self orthogonal if $\sum_{i=1}^{8}\alpha_i^2 = 0$, $vv^* = 1 + \sum_{i=1}^{2}(\alpha_{i+2}^2 + \alpha_{i+6}^2)\widehat{g}$,

$$\begin{aligned} (\alpha_1 + 1)\alpha_3 + \alpha_2\alpha_4 + (\alpha_5 + \mu_1)\alpha_7 + (\alpha_6 + \mu_2)\alpha_8 &= 0 \text{ and} \\ (\alpha_1 + 1)\alpha_4 + \alpha_2\alpha_3 + (\alpha_5 + \mu_1)\alpha_8 + (\alpha_6 + \mu_2)\alpha_7 &= 0. \end{aligned}$$

Moreover,

$$\text{rank}(M(\sigma)) = \text{rank}\left(\begin{array}{cc|ccccc|cc|ccccc} \alpha_1 & \alpha_2 & \multicolumn{5}{c|}{\alpha_3 \cdots \alpha_3\ \alpha_4 \cdots \alpha_4} & \alpha_5 & \alpha_6 & \multicolumn{5}{c}{\alpha_7 \cdots \alpha_7\ \alpha_8 \cdots \alpha_8} \\ \alpha_2 & \alpha_1 & \multicolumn{5}{c|}{\alpha_4 \cdots \alpha_4\ \alpha_3 \cdots \alpha_3} & \alpha_6 & \alpha_5 & \multicolumn{5}{c}{\alpha_8 \cdots \alpha_8\ \alpha_7 \cdots \alpha_7} \\ \hline \alpha_3 & \alpha_4 & & & & & & \alpha_7 & \alpha_8 & & & & & \\ \vdots & \vdots & & & & & & \vdots & \vdots & & & & & \\ \alpha_3 & \alpha_4 & & & & & & \alpha_7 & \alpha_8 & & & & & \\ \alpha_4 & \alpha_3 & \multicolumn{5}{c|}{I_{2p}} & \alpha_8 & \alpha_7 & \multicolumn{5}{c}{\sigma(v)} \\ \vdots & \vdots & & & & & & \vdots & \vdots & & & & & \\ \alpha_4 & \alpha_3 & & & & & & \alpha_8 & \alpha_7 & & & & & \end{array}\right)$$

$$= \operatorname{rank}\left(\begin{array}{cc|c|cc|c} \begin{matrix}\alpha_1+\alpha_3^2\\ \alpha_2+\alpha_4\alpha_3\end{matrix} & \begin{matrix}\alpha_2+\alpha_3\alpha_4\\ \alpha_1+\alpha_4^2\end{matrix} & \begin{matrix}\alpha_3 & \cdots & \alpha_3 & \alpha_4 & \cdots & \alpha_4\\ \alpha_4 & \cdots & \alpha_4 & \alpha_3 & \cdots & \alpha_3\end{matrix} & \begin{matrix}\alpha_5+\alpha_3\alpha_7\\ \alpha_6+\alpha_4\alpha_7\end{matrix} & \begin{matrix}\alpha_6+\alpha_3\alpha_8\\ \alpha_5+\alpha_4\alpha_8\end{matrix} & \begin{matrix}\alpha_7 & \cdots & \alpha_7 & \alpha_8 & \cdots & \alpha_8\\ \alpha_8 & \cdots & \alpha_8 & \alpha_7 & \cdots & \alpha_7\end{matrix} \\ \hline 0 & 0 & & 0 & 0 & \\ \vdots & \vdots & & \vdots & \vdots & \\ 0 & 0 & & 0 & 0 & \\ \alpha_4 & \alpha_3 & I_{2p} & \alpha_8 & \alpha_7 & \sigma(v) \\ \vdots & \vdots & & \vdots & \vdots & \\ \alpha_4 & \alpha_3 & & \alpha_8 & \alpha_7 & \end{array}\right)$$

$$= \operatorname{rank}\left(\begin{array}{cc|c|cc|c} \begin{matrix}\alpha_1+\alpha_3^2+\alpha_4^2\\ \alpha_2\end{matrix} & \begin{matrix}\alpha_2\\ \alpha_1+\alpha_3^2+\alpha_4^2\end{matrix} & \begin{matrix}\alpha_3 & \cdots & \alpha_3 & \alpha_4 & \cdots & \alpha_4\\ \alpha_4 & \cdots & \alpha_4 & \alpha_3 & \cdots & \alpha_3\end{matrix} & \begin{matrix}\alpha_5+\alpha_3\alpha_7+\alpha_4\alpha_8\\ \alpha_6+\alpha_3\alpha_8+\alpha_4\alpha_7\end{matrix} & \begin{matrix}\alpha_6+\alpha_3\alpha_8+\alpha_4\alpha_7\\ \alpha_5+\alpha_3\alpha_7+\alpha_4\alpha_8\end{matrix} & \begin{matrix}\alpha_7 & \cdots & \alpha_7 & \alpha_8 & \cdots & \alpha_8\\ \alpha_8 & \cdots & \alpha_8 & \alpha_7 & \cdots & \alpha_7\end{matrix} \\ \hline 0 & 0 & & 0 & 0 & \\ \vdots & \vdots & & \vdots & \vdots & \\ 0 & 0 & & 0 & 0 & \\ 0 & 0 & I_{2p} & 0 & 0 & \sigma(v) \\ \vdots & \vdots & & \vdots & \vdots & \\ 0 & 0 & & 0 & 0 & \end{array}\right)$$

$$= \operatorname{rank}\left(\begin{array}{cc|c|cc|c} \begin{matrix}\alpha_1+\alpha_3^2+\alpha_4^2 & \alpha_2\\ \alpha_2 & \alpha_1+\alpha_3^2+\alpha_4^2\end{matrix} & & \begin{matrix}0 & \cdots & 0 & \alpha_4 & \cdots & \alpha_4\\ 0 & \cdots & 0 & \alpha_3 & \cdots & \alpha_3\end{matrix} & \begin{matrix}\alpha_5+\alpha_3\alpha_7+\alpha_4\alpha_8 & \alpha_6+\alpha_3\alpha_8+\alpha_4\alpha_7\\ \alpha_6+\alpha_3\alpha_8+\alpha_4\alpha_7 & \alpha_5+\alpha_3\alpha_7+\alpha_4\alpha_8\end{matrix} & & \begin{matrix}\alpha_7+\mu_1\alpha_3 & \cdots & \alpha_7+\mu_1\alpha_3 & \alpha_8+\mu_2\alpha_3 & \cdots & \alpha_8+\mu_2\alpha_3\\ \alpha_8+\mu_1\alpha_4 & \cdots & \alpha_8+\mu_1\alpha_4 & \alpha_7+\mu_2\alpha_4 & \cdots & \alpha_7+\mu_2\alpha_4\end{matrix} \\ \hline 0 & 0 & & 0 & 0 & \\ \vdots & \vdots & & \vdots & \vdots & \\ 0 & 0 & & 0 & 0 & \\ 0 & 0 & I_{2p} & 0 & 0 & \begin{array}{c|c} M_1 & M_2 \\ \hline M_2' & M_1' \end{array} \\ \vdots & \vdots & & \vdots & \vdots & \\ 0 & 0 & & 0 & 0 & \end{array}\right)$$

$$= \operatorname{rank}\left(\begin{array}{cc|c|cc|c} \begin{matrix}\alpha_1+\alpha_3^2+\alpha_4^2 & \alpha_2\\ \alpha_2 & \alpha_1+\alpha_3^2+\alpha_4^2\end{matrix} & & \begin{matrix}0 & \ldots & 0\\ 0 & \ldots & 0\end{matrix} & \begin{matrix}\alpha_5+\alpha_3\alpha_7+\alpha_4\alpha_8 & \alpha_6+\alpha_3\alpha_8+\alpha_4\alpha_7\\ \alpha_6+\alpha_3\alpha_8+\alpha_4\alpha_7 & \alpha_5+\alpha_3\alpha_7+\alpha_4\alpha_8\end{matrix} & & \begin{matrix}\gamma_1 & \cdots & \gamma_1 & \gamma_2 & \cdots & \gamma_2\\ \gamma_2 & \cdots & \gamma_2 & \gamma_1 & \cdots & \gamma_1\end{matrix} \\ \hline 0 & 0 & & 0 & 0 & \\ \vdots & \vdots & & \vdots & \vdots & \\ 0 & 0 & & 0 & 0 & \\ 0 & 0 & I_{2p} & 0 & 0 & \begin{array}{c|c} M_1 & M_2 \\ \hline M_2' & M_1' \end{array} \\ \vdots & \vdots & & \vdots & \vdots & \\ 0 & 0 & & 0 & 0 & \end{array}\right)$$

where $\gamma_1 = \alpha_7 + \mu_1\alpha_3 + \mu_2\alpha_4$ and $\gamma_2 = \alpha_8 + \mu_1\alpha_4 + \mu_2\alpha_3$. Therefore $M(\sigma)$ has free rank $2p+2$ if and only if:

$$\begin{pmatrix} \alpha_1+\alpha_3^2+\alpha_4^2 & \alpha_2 & \alpha_5+\alpha_3\alpha_7+\alpha_4\alpha_8 & \alpha_6+\alpha_3\alpha_8+\alpha_4\alpha_7 & \alpha_7+\mu_1\alpha_3+\mu_2\alpha_4 & \alpha_8+\mu_1\alpha_4+\mu_2\alpha_3 \\ \alpha_2 & \alpha_1+\alpha_3^2+\alpha_4^2 & \alpha_6+\alpha_3\alpha_8+\alpha_4\alpha_7 & \alpha_5+\alpha_3\alpha_7+\alpha_4\alpha_8 & \alpha_8+\mu_1\alpha_4+\mu_2\alpha_3 & \alpha_7+\mu_1\alpha_3+\mu_2\alpha_4 \end{pmatrix}$$

has free rank 2. ■

The next two results provide conditions when units/non units in RG can be used to be used to yield self-dual codes using the above construction.

Corollary 5.2.3 *Let R be a finite commutative Frobenius ring of characteristic 2, let G be a finite group of order $2p$ where p is odd, and let C_σ be a self-dual code. If $\sum_{i=1}^{2}(\alpha_{i+2} + \alpha_{i+6}) = 0$ then $v \in RG$ is a unit.*

Proof. If $\sum_{i=1}^{2}(\alpha_{i+2} + \alpha_{i+6}) = 0$, then $\sigma(vv^*) = I_{2p}$ and $vv^* = 1$. Therefore v is unitary. ■

Corollary 5.2.4 *Let R be a finite commutative Frobenius ring of characteristic 2, let G be a finite group of order $2p$ where p is odd, and let C_σ be a self-dual code. If $\sum_{i=1}^{2}(\alpha_{i+2} + \alpha_{i+6}) = 1$ then $v \in RG$ is a non-unit.*

Proof. If $\sum_{i=1}^{2}(\alpha_{i+2}+\alpha_{i+6})=1$, then

$$\sum_{i=1}^{2}(\alpha_{i+2}^2+\alpha_{i+6}^2)\mathrm{CIRC}(\mathbf{A},\mathbf{0})+I_{2p}+\sigma(vv^*)=\mathrm{CIRC}(\mathbf{A},\mathbf{0})+\sigma(vv^*)=0$$

where $\mathbf{A}=\mathrm{circ}(0,\underbrace{1,\ldots,1}_{(p-1)-\text{times}})$ and $\mathbf{0}=\mathrm{circ}(\underbrace{0,\ldots,0}_{p-\text{times}})$. Now $det(\mathrm{CIRC}(\mathbf{A},\mathbf{0}))=det(\mathbf{A})^2$ and

$$det(A)=det\begin{pmatrix}0&1&1&\ldots&1\\1&0&1&\cdots&1\\1&1&0&\cdots&1\\\vdots&\vdots&\vdots&\ddots&\vdots\\1&1&1&\ldots&0\end{pmatrix}=(p-1)det\begin{pmatrix}1&1&1&\ldots&1\\0&1&0&\cdots&0\\0&0&1&\cdots&0\\\vdots&\vdots&\vdots&\ddots&\vdots\\0&0&0&\ldots&1\end{pmatrix}=0.$$

Therefore, $det(\sigma(vv^*))=0$ and vv^* is a non-unit by Corollary 3 in [60]. Hence, $v\in RG$ is a non-unit. ■

Now, we will construct self-dual codes of various lengths (64, 68, 80) using groups of order 6, 14, 18, 30 and 38.

5.2.1 Constructions coming from D_6

In this section, we implement the above construction using $G=D_6$. We construct self-dual codes of length 64 by considering this construction over $\mathbb{F}_4+u\mathbb{F}_4$. Using this construction, we were able to construct one new code of length 64.

The possible weight enumerators for a self-dual Type I $[64,32,12]$-code is given in [20, 28] as:

$$\begin{aligned}W_{64,1}&=1+(1312+16\beta)\,y^{12}+(22016-64\beta)\,y^{14}+\cdots,14\leq\beta\leq284,\\W_{64,2}&=1+(1312+16\beta)\,y^{12}+(23040-64\beta)\,y^{14}+\cdots,0\leq\beta\leq277.\end{aligned}$$

With the most updated information, the existence of codes is known for β =14, 18, 22, 25, 29, 32, 35, 36, 39, 44, 46, 53, 59, 60, 64 and 74 in $W_{64,1}$ and for β =0, 1, 2, 4, 5, 6, 8, 9, 10, 12, 13, 14, 16, ..., 25, 28, 19, 30, 32, 33, 34, 36, 37, 38, 40, 41, 42, 44, 45, 48, 50, 51, 52, 56, 58, 64, 72, 80, 88, 96, 104, 108, 112, 114, 118, 120 and 184 in $W_{64,2}$.The new code that we have constructed is $\beta=57$ in $W_{64,2}$.

Table 5.1: Self-dual code of length 64 from D_6 over $\mathbb{F}_4+u\mathbb{F}_4$.

$\mathcal{A}_i$	$(\alpha_1,\ldots,\alpha_8)$	$(a_1,\ldots,a_6)$	$\lvert Aut(A_i)\rvert$	Type
1	$(0,B,2,A,2,4,1,4)$	$(A,1,3,2,B,7)$	$2^3\cdot3$	$\beta=\mathbf{57}$ $(W_{64,2})$
2	$(0,1,0,0,0,2,6,7)$	$(0,B,B,3,6,7)$	$2^4\cdot3$	$\beta=64$ $(W_{64,2})$

5.2.2 Constructions coming from groups of order 14

Here we present the results for the above construction using $G \in \{D_{14}, C_{14}\}$. We construct self-dual codes of length 64 by considering this construction over $\mathbb{F}_2 + u\mathbb{F}_2$.

Table 5.2: Self-dual codes of length 64 from D_{14} over $\mathbb{F}_2 + u\mathbb{F}_2$.

$\mathcal{B}_i$	$(\alpha_1, \alpha_2, \ldots, \alpha_8)$	$(a_1, a_2, \ldots, a_{14})$	$\lvert Aut(C)\rvert$	Type
1	$(u, 1, u, u, 0, 0, u, 1)$	$(u, u, 0, u, u, 1, 1, 0, 0, 1, 3, 0, 3, 1)$	$2^3 \cdot 7$	$\beta = 46$ $(W_{64,1})$
2	$(u, 1, u, u, 0, 0, u, 1)$	$(u, u, 0, 0, 0, 1, 1, u, 0, 1, 1, u, 1, 1)$	$2^2 \cdot 7$	$\beta = 60$ $(W_{64,1})$

Table 5.3: Self-dual codes of length 64 from C'_{14} over R_1.

$\mathcal{C}_i$	$(\alpha_1, \alpha_2, \ldots, \alpha_8)$	$(a_1, a_2, \ldots, a_{14})$	$\lvert Aut(C)\rvert$	Type
1	$(u, 1, u, u, 0, 0, u, 1)$	$(u, 0, 0, 0, u, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	$2^3 \cdot 7$	$\beta = 46$ $(W_{64,1})$

5.2.3 Constructions coming from a groups of order 18

Now, we implement the above construction using $G \in \{D_{18}, C_{18}\}$. We construct self-dual codes of length 80 by considering this construction over $\mathbb{F}_2 + u\mathbb{F}_2$. In [101], the possible weight enumerators for a self-dual Type I $[80, 40, 14]$-code is given in as:

$$W_{80,2} = 1 + (3200 + 4\alpha)\, y^{14} + (47645 - 8\alpha + 256\beta)\, y^{16} + \cdots,$$

where α and β are integers. A $[80, 40, 14]$ code was constructed in [23], however its weight enumerator was not stated. A $[80, 40, 14]$ code was constructed in [54] with $\alpha = -280$, $\beta = 10$ and $[80, 40, 14]$ codes were constructed for $\beta = 0$ and $\alpha = -17k$ where $k \in \{2, \ldots, 25, 27\}$ in [101]. None of the codes presented here have been previously constructed.

Table 5.4: Self-dual codes of length 80 from D_{18} over $\mathbb{F}_2 + u\mathbb{F}_2$ where $(\alpha_1, \ldots, \alpha_8) = (u, 1, u, u, 0, 0, u, 1)$

$\mathcal{D}_i$	$(a_1, \ldots, a_9)$	$(a_{10}, \ldots, a_{18})$	$\lvert Aut(C_i)\rvert$	Type
1	$(u, 0, u, 1, 1, 1, 1, 1, 1)$	$(u, u, 1, 3, 0, 1, 1, 1, 3)$	$2^2 \cdot 3^2$	$\alpha = \mathbf{-229}$, $\beta = \mathbf{18}$ $(W_{80,2})$
2	$(u, u, u, 0, 1, u, 3, 3, 1)$	$(0, 0, 1, u, 3, u, 0, 3, 1)$	$2^2 \cdot 3^2$	$\alpha = \mathbf{-256}$, $\beta = \mathbf{18}$ $(W_{80,2})$
3	$(0, u, 0, 0, u, 0, 0, 1, 1)$	$(0, 0, 1, 3, 1, 0, 3, 3, 3)$	$2^2 \cdot 3^2$	$\alpha = \mathbf{-274}$, $\beta = \mathbf{18}$ $(W_{80,2})$
4	$(0, u, 0, 0, 0, 0, 0, 1, 3)$	$(u, 0, 1, 1, 1, 0, 3, 3, 3)$	$2^2 \cdot 3^2$	$\alpha = \mathbf{-310}$, $\beta = \mathbf{18}$ $(W_{80,2})$
5	$(0, 0, 0, 1, 1, 3, 3, 3, 3)$	$(u, u, 1, 1, 0, 1, 3, 1, 3)$	$2^2 \cdot 3^2$	$\alpha = \mathbf{-355}$, $\beta = \mathbf{18}$ $(W_{80,2})$

5.2.4 Constructions coming from D_{38}

In this section, we implement the construction on $G = D_{38}$. We construct self-dual codes of length 80 by considering this construction over $\mathbb{F}_2$. The full calculation on Magma is shown in Appendix A.3.

Table 5.5: Self-dual codes of length 80 from D_{38} over $\mathbb{F}_2$ where $(\alpha_1, \ldots, \alpha_8) = (0, 1, 0, 0, 1, 1, 0, 1)$

$\mathcal{E}_i$	$(a_1, \ldots, a_{19})$	$(a_{20}, \ldots, a_{38})$	$\lvert Aut(C_i)\rvert$	Type
1	$(0,0,0,0,0,0,0,0,0,0,1,1,1,0,0,1,1,1,1)$	$(0,0,0,0,1,0,1,1,0,1,0,0,1,0,0,1,1,1,1)$	$2 \cdot 19$	$\alpha = \mathbf{-211}$, $\beta = \mathbf{18}$ $(W_{80,2})$
2	$(0,0,0,0,0,0,0,0,0,1,0,1,1,1,1,1,1,1,1)$	$(0,0,0,0,1,0,1,0,1,0,0,1,1,0,0,0,0,1,1)$	$2 \cdot 19$	$\alpha = \mathbf{-249}$, $\beta = \mathbf{18}$ $(W_{80,2})$
3	$(0,0,0,0,0,0,0,0,0,0,0,1,1,1,0,1,1,1,1)$	$(0,0,0,0,1,1,1,0,1,0,0,0,1,0,1,0,1,1,1)$	$2 \cdot 19$	$\alpha = \mathbf{-287}$, $\beta = \mathbf{18}$ $(W_{80,2})$
4	$(0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,1,1,1,1)$	$(0,0,0,0,0,0,1,0,1,0,0,1,1,0,0,1,0,1,1)$	$2 \cdot 19$	$\alpha = \mathbf{-306}$, $\beta = \mathbf{18}$ $(W_{80,2})$
5	$(0,0,0,0,0,0,1,0,0,0,0,0,0,1,1,1,1,1,1)$	$(0,0,0,0,0,1,0,1,0,0,1,1,0,1,0,1,1,1,1)$	$2^2 \cdot 19$	$\alpha = \mathbf{-325}$, $\beta = \mathbf{18}$ $(W_{80,2})$
5	$(0,0,0,0,0,0,0,0,0,0,1,0,0,0,1,1,0,1,1)$	$(0,0,0,0,1,1,1,0,0,1,0,1,1,1,0,1,1,1,1)$	$2 \cdot 19$	$\alpha = \mathbf{-363}$, $\beta = \mathbf{18}$ $(W_{80,2})$
7	$(0,0,0,0,0,0,0,0,0,0,1,0,1,1,1,1,0,1,1)$	$(0,0,0,1,0,0,1,1,1,1,0,0,1,0,0,0,1,1,1)$	$2^2 \cdot 19$	$\alpha = \mathbf{-401}$, $\beta = \mathbf{18}$ $(W_{80,2})$

5.3 New Codes of Length 68

In this section, we implement Theorem 1.2.27 to construct new extremal self-dual codes. We extend the codes previously constructed in Tables 5.2.1, 5.2.2 and 5.2.2.

The known weight enumerators of a self-dual $[68, 34, 12]_I$-code are as follows:

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

where $0 \leq \gamma \leq 9$. Codes have been obtained for $W_{68,2}$ when

$$\begin{aligned} \gamma &= 2,\ \beta \in \{2m \,|m = 29, \ldots, 100, 103, 104\} \text{ or } \beta \in \{2m + 1 \,|m = 32, 34, \ldots, 79\}; \\ \gamma &= 3,\ \beta \in \{2m \,|m = 40, \ldots, 98, 101, 102\} \text{ or} \\ \beta &\in \{2m + 1 | m = 41, 43, \ldots, 77, 79, 80, 83, 96\}; \\ \gamma &= 4,\ \beta \in \{2m \,|m = 43, 44, 48, \ldots, 92, 97, 98\} \text{ or} \\ \beta &\in \{2m + 1 \,|m = 48, \ldots, 55, 58, 60, \ldots, 78, 80, 83, 84, 85\}; \\ \gamma &= 5 \text{ with } \beta \in \{m | m = 113, 116, \ldots, 181\}; \end{aligned}$$

Recall that the codes constructed in Tables 5.2.1, 5.2.2 and 5.2.2 are codes over $\mathbb{F}_4 + u\mathbb{F}_4$. Consequently, we converted these codes to codes over $\mathbb{F}_2 + u\mathbb{F}_2$ (using the Gray map $\psi_{\mathbb{F}_4 + u\mathbb{F}_4}$) before applying Theorem 1.2.27. The following table displays the newly constructed extremal codes of length 68. We replace $u + 1$ with 3 to save space.

Two self-dual binary codes of dimension k are said to be neighbours if their intersection has dimension $k - 1$. We consider the standard form of the generator matrix of C to reduce the search field. Let $x \in \mathbb{F}_2^n - C$ then $D = \left\langle \langle x \rangle^{\perp} \cap C, x \right\rangle$ is a neighbour of C. Without loss of generality, the

Table 5.6: Self-dual codes of length 68 from extending $[64, 32, 12]_I$

$\mathcal{C}_{68,i}$	Code	c	X	γ	β
$\mathcal{C}_{68,1}$	$\mathcal{B}_1$	$u+1$	$(3, u, 0, u, 0, 3, u, u, 1, 0, u, 3, 0, 1, u, 1, 1, 1, u, u, u, u, u, 1, u, u, 0, 0, 1, u, 0, 3)$	**2**	**161**
$\mathcal{C}_{68,2}$	$\mathcal{B}_1$	$u+1$	$(u, 3, u, 3, u, 1, 0, 0, 1, 3, u, 0, u, u, 1, 0, 1, 3, 1, 0, 1, 3, u, 0, 3, 3, 0, 0, 0, u, 1, 3)$	**2**	**163**
$\mathcal{C}_{68,3}$	$\mathcal{A}_1$	1	$(0, 1, u, u, 1, 1, 3, u, 3, 1, 3, 0, 0, 0, 3, 1, 3, 0, 1, 0, 1, 1, u, u, 1, u, 3, 3, 0, 0, 3, u)$	**2**	**169**
$\mathcal{C}_{68,4}$	$\mathcal{B}_2$	$u+1$	$(0, u, 0, 1, 0, 0, 3, 0, 0, 0, 0, 3, 0, 0, 0, 1, 0, 1, u, 3, 1, 0, u, u, 3, 1, 1, 1, 1, 1, 0, u)$	**2**	**171**
$\mathcal{C}_{68,5}$	$\mathcal{C}_1$	$u+1$	$(1, 3, u, 0, 1, 3, 1, 3, 1, 0, 1, u, 0, 0, u, 3, 3, 0, u, 0, 3, u, 1, 0, 3, 1, 1, 0, u, 1, 1, u)$	**2**	**173**
$\mathcal{C}_{68,6}$	$\mathcal{A}_2$	1	$(3, 0, 0, 0, 3, 0, u, 3, 3, 3, u, 3, 0, 1, 1, 0, 3, u, 1, u, 0, 3, 0, u, u, 3, 0, 0, u, u, u, 1)$	**4**	**200**

first 34 entries of x are set to be 0, the rest of the vectors are listed in Table 5.7. As neighbours of codes in Table 5.3 we obtain 12 new codes with weight enumerators in $W_{68,2}$. Note that all the codes have an automorphism group of order 2.

Table 5.7: New codes of length 68 as neighbours of $\mathcal{C}_{68,6}$

$\mathcal{N}_{68,i}$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
$\mathcal{N}_{68,1}$	(11110001100011100000101111110001011)	**3**	**163**
$\mathcal{N}_{68,2}$	(10111000000000010111000000010011001)	**3**	**175**
$\mathcal{N}_{68,3}$	(00111000100011110011000000010110111)	**3**	**177**
$\mathcal{N}_{68,4}$	(10000100011010101110110011111101111)	**4**	**159**
$\mathcal{N}_{68,5}$	(10010001011000101111111100110010011)	**4**	**175**
$\mathcal{N}_{68,6}$	(11100011001101110100001110000010100)	**4**	**186**
$\mathcal{N}_{68,7}$	(11001011011001110100111011101111110)	**4**	**191**
$\mathcal{N}_{68,8}$	(11010011010111101001100010001101101)	**5**	**182**
$\mathcal{N}_{68,9}$	(10010010010111010111111011100001001)	**5**	**187**
$\mathcal{N}_{68,10}$	(00000001100001011011010011001000001)	**5**	**189**
$\mathcal{N}_{68,11}$	(01111001110110001100001110110101111)	**5**	**191**
$\mathcal{N}_{68,12}$	(00001011100011101011110101001111111)	**5**	**193**

Chapter 6

New Self-dual Codes from 2×2 block circulant matrices, Group Rings and Neighbours of Neighbours

Let A and B be $n \times n$ circulant matrices over $\mathbb{F}_q$. The four circulant construction, introducted by [3], considers generator matrices of the form:

$$\left(I_{2n} \middle| \begin{array}{cc} A & B \\ -B^T & A^T \end{array} \right).$$

This construction was then applied to the ring $\mathbb{F}_2 + u\mathbb{F}_2$; consequently, many new extremal self-dual codes were obtained, [70]. More recently, in [43], the four circulant construction was generalized by including another reverse construction in the generator matrix:

$$\left(\begin{array}{c|cc} & A & B+C \\ I_{2n} & B^T + C & A^T \end{array} \right)$$

where A and B are $n \times n$ circulant matrices, and C is a $n \times n$ reverse circulant matrix. In [73], the four circulant construction was modified to:

$$\left(I_{2n} \middle| \begin{array}{cc} A & B \\ -B & A \end{array} \right)$$

where A is an $n \times n$ λ-circulant matrix and B is a $n \times n$ λ-reverse circulant matrix over a finite Frobenius ring R. In addition to this construction, they also construct new self-dual codes from the construction:

$$\left(\begin{array}{c|cccc} & 1 & 1 & x & y \\ & 1 & 1 & y & x \\ I_{2n} & z^T & t^T & A & B \\ & t^T & z^T & B & A \end{array} \right)$$

where A is an $n \times n$ circulant matrix over a finite Frobenius ring R, B is a $n \times n$ reverse circulant matrix over a finite Frobenius ring R and x, y, z, t are vectors over a finite Frobenius ring R. In [35], the double circulant construction was extended to the following:

$$\left(\begin{array}{c|cccc} & A_1 & A_2 & \cdots & A_k \\ & A_n & A_1 & \cdots & A_{k-1} \\ I_{2n} & \vdots & \vdots & \ddots & \vdots \\ & A_2 & A_3 & \cdots & A_1 \end{array}\right)$$

where A_i are $n \times n$ circulant matrices over $\mathbf{F}_q$. In this work, we construct self-dual codes by considering generator matrices as a unique combination of 2×2 block circulant construction, group rings and reverse circulant matrices. Specifically, we construct self-dual codes from generator matrices of the form:

$$\left[\begin{array}{c|cc} & A & B+C \\ I & & \\ & B+C & A \end{array}\right]$$

where A and B are matrices that arise from a group ring construction and C is a reverse circulant matrix.

The main group discussed in this chapter is the cyclic group. Recall that $C_{2p} = \langle x \mid x^{2p} = 1 \rangle$ and

$$v = \sum_{i=0}^{p-1} \sum_{j=0}^{1} \alpha_{i+pj+1} x^{2i+j} \in RC_{2p}$$

then,

$$\sigma(v) = \begin{pmatrix} A_1 & A_2 \\ A_2' & A_1 \end{pmatrix}$$

where $A_j = cir(\alpha_{(j-1)p+1}, \alpha_{(j-1)p+2}, \ldots, \alpha_{jp})$ and $A_j' = cir(\alpha_{jp}, \alpha_{(j-1)p+1}, \ldots, \alpha_{jp-1})$.

Furthermore, recall the canonical involution $* : RG \to RG$ on a group ring RG is given by $v^* = \sum_g \alpha_g g^{-1}$, for $v = \sum_g \alpha_g g \in RG$. If v satisfies $vv^* = 1$, then we say that v is a unitary unit in RG. We also note that $\sigma(v^*) = \sigma(v)^T$.

For the remainder of this chapter, we describe the construction itself. We present the structure of the generator matrix and discuss associated theory in order to put some restrictions on unknowns. These restrictions aim to maximise the practicality of the construction method by reducing the search field. Following the theory, we look at the numerical results from certain groups of order 4, 8 and 17. We then apply extensions and consider neighbours of codes as methods of finding new codes.

6.1 Construction

Consider the following matrix $M(\sigma)$, where v_1 and v_2 are distinct group ring elements from the same group ring RG where R is a finite Frobenius commutative ring of characteristic 2 and G is a finite group of order n. $\sigma(v)$ is a matrix generated from a group ring element and A denotes a reverse circulant matrix.

$$M(\sigma) = \left[\begin{array}{c|cc} & \sigma(v_1) & \sigma(v_2)+A \\ I_{2n} & & \\ & \sigma(v_2)+A & \sigma(v_1) \end{array}\right]$$

Let C_σ be the code generated by the matrix $M(\sigma)$. Clearly, C_σ has length $4n$. We will now establish conditions when C_σ generates a self-dual code. We will also create a link between unitary units in RG and the above construction yielding self-dual codes.

Lemma 6.1.1 *Let R be a finite commutative Frobenius ring of characteristic 2 and let B and C be $n \times n$ matrices over R. Then, the matrix*

$$M = \left[\begin{array}{c|cc} & B & C \\ I_{2n} & & \\ & C & B \end{array}\right]$$

generates a self-dual code iff $(B+C)(B+C)^T = I_n$ and $BC^T = CB^T$.

Proof. Clearly, the code generated by M has free rank $2n$, as the left-hand side of the matrix M is the $2n \times 2n$ identity matrix. The code generated by M is self-dual if and only if the code generated by M is self-orthogonal. Now,

$$MM^T = I_{2n} + \begin{pmatrix} B & C \\ C & B \end{pmatrix}\begin{pmatrix} B^T & C^T \\ C^T & B^T \end{pmatrix} = \begin{pmatrix} I_n + BB^T + CC^T & BC^T + CB^T \\ CB^T + BC^T & I_n + CC^T + BB^T \end{pmatrix}$$

and $MM^T = 0$ iff $I_n + BB^T + CC^T = 0$ and $BC^T + CB^T = 0$. Adding these equations, we obtain

$$I_n + BB^T + CC^T + BC^T + CB^T = 0 \Longleftrightarrow (B+C)(B+C)^T = I_n.$$

■

Theorem 6.1.2 *Let R be a finite commutative Frobenius ring of characteristic 2 and let G be a finite group of order n. Then, C_σ generates a self-dual code of length $4n$ iff $(\sigma(v_1+v_2)+A)(\sigma((v_1+v_2)^*)+A) = I_n$ and $\sigma(v_1)(\sigma((v_1+v_2)^*)+A) = (\sigma(v_1+v_2)+A)\sigma(v_1^*)$.*

Proof. By the previous result, C_σ generates a self-dual code iff

$$(\sigma(v_1)+\sigma(v_2)+A)(\sigma(v_1)+\sigma(v_2)+A)^T = I_n \text{ and } \sigma(v_1)(\sigma(v_2)+A)^T = (\sigma(v_2)+A)\sigma(v_1)^T.$$

Now, $\sigma(v_1) + \sigma(v_2) + A = \sigma(v_1 + v_2) + A$ and

$$\begin{aligned}(\sigma(v_1) + \sigma(v_2) + A)^T &= \sigma(v_1)^T + \sigma(v_2)^T + A^T \\ &= \sigma(v_1^*) + \sigma(v_2^*) + A \\ &= \sigma(v_1^* + v_2^*) + A \\ &= \sigma((v_1 + v_2)^*) + A.\end{aligned}$$

Clearly, $\sigma(v_1)(\sigma(v_2) + A)^T = (\sigma(v_2) + A)\sigma(v_1)^T$ is equivalent to

$$\sigma(v_1)\sigma(v_1)^T + \sigma(v_1)(\sigma(v_2) + A)^T = \sigma(v_1)\sigma(v_1)^T + (\sigma(v_2) + A)\sigma(v_1)^T.$$

Considering the left-and right-hand sides separately, we obtain:

$$\begin{aligned}\sigma(v_1)\sigma(v_1)^T + \sigma(v_1)(\sigma(v_2) + A)^T &= \sigma(v_1)\sigma(v_1^*) + \sigma(v_1)(\sigma(v_2)^T + A^T) \\ &= \sigma(v_1)\sigma(v_1^*) + \sigma(v_1)\sigma(v_2^*) + \sigma(v_1)A \\ &= \sigma(v_1)(\sigma(v_1^*) + \sigma(v_2^*) + A) \\ &= \sigma(v_1)(\sigma(v_1^* + v_2^*) + A) \\ &= \sigma(v_1)(\sigma((v_1 + v_2)^*) + A).\end{aligned}$$

and

$$\begin{aligned}(\sigma(v_2) + A)\sigma(v_1)^T + \sigma(v_1)\sigma(v_1)^T &= \sigma(v_1)\sigma(v_1^*) + (\sigma(v_2) + A)\sigma(v_1^*) \\ &= \sigma(v_1)\sigma(v_1^*) + \sigma(v_2)\sigma(v_1^*) + A\sigma(v_1^*) \\ &= (\sigma(v_1) + \sigma(v_2) + A)\sigma(v_1^*) \\ &= (\sigma(v_1 + v_2) + A)\sigma(v_1^*).\end{aligned}$$

■

Lemma 6.1.3 *Let R be a finite commutative Frobenius ring of characteristic 2, A be a $n \times n$ reverse circulant over R, and let V be a $n \times n$ circulant matrix over R. Then,*

$$AV^T + VA^T = 0. \tag{6.1}$$

Proof. Let $V = \mathrm{cir}(v_1, v_n, v_{n-1}, \ldots, v_3, v_2)$. Clearly, $V = v_1 I_n + v_2 P + v_3 P^2 + \cdots + v_n P^{n-1}$ where $P = \mathrm{cir}(0, 0, \ldots, 0, 1)$ and $A = \mathrm{rcir}(a_1, a_2, \ldots, a_{n-1}, a_n)$. Now,

$$\begin{aligned}V^T &= v_1 I_n^T + v_2 P^T + v_3 (P^2)^T + \cdots + v_n (P^{n-1})^T \\ &= v_1 I_n + v_2 P^T + v_3 (P^T)^2 + \cdots + v_n (P^T)^{n-1}.\end{aligned}$$

As $A = A^T$, it remains to show that $AP^T + PA = 0$. Finally,

$$PA = \mathrm{cir}(0, 0, \ldots, 0, 1) \cdot \mathrm{rcir}(a_1, a_2, \ldots, a_{n-1}, a_n) = \mathrm{rcir}(a_n, a_1, \ldots, a_{n-1})$$

and

$$AP^T = \mathrm{rcir}(a_1, a_2, \ldots, a_{n-1}, a_n) \cdot \mathrm{cir}(0, 1, \ldots, 0, 0) = \mathrm{rcir}(a_n, a_1, \ldots, a_{n-1}).$$

■

Lemma 6.1.4 *Let R be a commutative ring and let $G = \{g_1 = e, \ldots, g_n\}$ be a finite group of order $n > 1$. The $\sigma(v)$ is symmetric for any $v \in RG$ if and only if G is an abelian group of exponent 2.*

Proof. Clearly, $\sigma(v)$ is symmetric for any $v \in RG$ if and only if $\alpha_{g_i^{-1}g_j} = \alpha_{g_j^{-1}g_i}$ $(i, j = 1, \ldots, n)$ for any $v = \sum_{g \in G} \alpha_g g \in RG$. Furthermore, we have $g_i^{-1}g_j = g_j^{-1}g_i$ $(i = 1, \ldots, n)$ $(i, j = 1, \ldots, n)$ or $xy = y^{-1}x^{-1}$ for any $x, y \in G$. Note that for an abelian group of exponent 2, $yxy = x^{-1}$ or $xyxy = e$ or $(xy)^2 = e$ for any $x, y \in G$. Therefore, we have that $g^2 = e$ for any $g \in G$; thus, G has exponent 2.

It is interesting to note that any group of exponent 2 is abelian because $xyxy = e$ and $xxyy = ee = e$ since x and y are commutative for any $x, y \in G$. ■

Lemma 6.1.5 *Let R be a commutative ring. An $n \times n$-matrix X satisfies $XA = AX^T$ for any $n \times n$ reverse circulant matrix A over R if and only if X is a circulant matrix.*

Proof. This proof follows from lemma 6.1.3. Let X be a $n \times n$-matrix which satisfies $XA = AX^T$. Then

$$XA = A^T X^T$$

and

$$XA = (XA)^T$$

for any $n \times n$ reverse circulant matrix A over R. This implies that XA is symmetric. Let $D = \begin{pmatrix} 0 & \ldots & 0 & 1 \\ 0 & \ldots & 1 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 1 & \ldots & 0 & 0 \end{pmatrix} = \mathrm{rcir}(0, 0, \ldots, 0, 1)$, $X = (x_{i,j})$. Clearly, we have $D^2 = I_n$ and $XDDA$ is symmetric for any $n \times n$ reverse circulant matrix A over R. Therefore, $(x_{i,n-j})DA$ is symmetric.

So we have $(x_{i,n-j})B$ is symmetric for any $n \times n$ circulant matrix B over R. This is equivalent to the fact that $(x_{i,n-j})P^k$ is symmetric for any $k \in \{1, \ldots, n\}$ and $n \times n$ matrix $P = \mathrm{cir}(0, 0, \ldots, 0, 1)$. Thus, $(x_{i,(k-j) \bmod n+1})$ is symmetric for any $k \in \{1, \ldots, n\}$. We have

$$x_{i,(k-j) \bmod n+1} = x_{j,(k-i) \bmod n+1} \; i, j, k \in \{1, \ldots, n\}$$

It is easy to see that $j' = (k - j) \bmod (n + 1)$ equivalent to $j = (k - j') \bmod (n + 1)$ where $i, j, j', k \in \{1, \ldots, n\}$. So

$$x_{i,j'} = x_{(k-j') \bmod n+1,(k-i) \bmod n+1} \; i, j', k \in \{1, \ldots, n\}$$

Thus $((k-j') \bmod (n+1)) - ((k-i) \bmod (n+1)) \equiv i-j \pmod{n}$. Therefore, we have that $x_{i,j'}$ is constant if $(i-j) \bmod n$ is fixed. Thus, X is circulant. ■

Lemma 6.1.6 *Let R be a finite commutative Frobenius ring of characteristic 2 and let G be a finite abelian group of order n of exponent 2. Then, C_σ generates a self-dual code of length $4n$ if $\sigma(v_1), \sigma(v_2)$ are circulant matrices, $\sigma((v_1+v_2)^2) + A^2 = I_n$.*

Proof. We note that $A\sigma(v_1^*) = \sigma(v_1)A$, $A\sigma(v_2^*) = \sigma(v_2)A$ by lemma 6.1.3. By lemma 6.1.4 for any $v \in RG$ $\sigma(v)$ is symmetric, so $\sigma(v^*) = \sigma(v)^T = \sigma(v)$. We also know by theorem 6.1.2 that C_σ generates a self-dual code iff

$$(\sigma(v_1)+\sigma(v_2)+A)(\sigma(v_1)+\sigma(v_2)+A)^T = I_n \text{ and } \sigma(v_1)(\sigma(v_2)+A)^T = (\sigma(v_2)+A)\sigma(v_1)^T.$$

Now,

$$\begin{aligned}(\sigma(v_1)+\sigma(v_2)+A)(\sigma(v_1)+\sigma(v_2)+A)^T &= (\sigma(v_1+v_2)+A)(\sigma((v_1+v_2)^*)+A)\\ &= \sigma(v_1+v_2)\sigma((v_1+v_2)^*) + [\sigma(v_1+v_2)A + A\sigma((v_1+v_2)^*)] + A^2\\ &= \sigma((v_1+v_2)(v_1+v_2)^*) + A^2 = \sigma((v_1+v_2)^2) + A^2 = I_n.\end{aligned}$$

and

$$\begin{aligned}\sigma(v_1)(\sigma(v_2)+A)^T + (\sigma(v_2)+A)\sigma(v_1)^T &= \sigma(v_1)\sigma(v_2^*) + [\sigma(v_1)A + A\sigma(v_1^*)] + \sigma(v_2)\sigma(v_1^*)\\ &= \sigma(v_1v_2) + \sigma(v_2v_1)\\ &= \sigma(v_1v_2) + \sigma(v_1v_2) = 0.\end{aligned}$$

■

Lemma 6.1.7 *Let R be a finite commutative Frobenius ring of characteristic 2 and let G be a finite cyclic group of order n. Then, C_σ generates a self-dual code of length $4n$ iff $\sigma((v_1+v_2)(v_1+v_2)^*) + A^2 = I_n$ and $v_1v_2^* = v_2v_1^*$.*

Proof. We note that $A\sigma(v^*) = \sigma(v)A$ for all $v \in RG$ by the previous result. We also know that C_σ generates a self-dual code iff

$$(\sigma(v_1)+\sigma(v_2)+A)(\sigma(v_1)+\sigma(v_2)+A)^T = I_n \text{ and } \sigma(v_1)(\sigma(v_2)+A)^T = (\sigma(v_2)+A)\sigma(v_1)^T.$$

Now,

$$\begin{aligned}(\sigma(v_1)+\sigma(v_2)+A)(\sigma(v_1)+\sigma(v_2)+A)^T &= (\sigma(v_1+v_2)+A)(\sigma((v_1+v_2)^*)+A)\\ &= \sigma(v_1+v_2)\sigma((v_1+v_2)^*) + [\sigma(v_1+v_2)A + A\sigma((v_1+v_2)^*)] + A^2\\ &= \sigma((v_1+v_2)(v_1+v_2)^*) + A^2 = I_n\end{aligned}$$

and

$$\begin{aligned}\sigma(v_1)(\sigma(v_2)+A)^T+(\sigma(v_2)+A)\sigma(v_1)^T &= \sigma(v_1)\sigma(v_2^*)+[\sigma(v_1)A+A\sigma(v_1^*)]+\sigma(v_2)\sigma(v_1^*)\\ &= \sigma(v_1v_2^*)+\sigma(v_2v_1^*)\\ &= \sigma(v_1v_2^*+v_2v_1^*).\end{aligned}$$

Finally, $\sigma(v_1v_2^*+v_2v_1^*)=0$ iff $v_1v_2^*=v_2v_1^*$. ■

Lemma 6.1.8 *Let R be a finite commutative Frobenius ring of characteristic 2 and let G be a finite abelian group of order n. Let C_σ be self-dual. If $A=0$, then v_1+v_2 is unitary.*

Proof. If C_σ is self-dual and $A=0$, then $\sigma((v_1+v_2)(v_1+v_2)^*)=I_n$ and $(v_1+v_2)(v_1+v_2)^*=1$. ■

6.2 Numerical Results

In this section, we construct 32 new self-dual codes of length 68. We begin with the construction of self-dual codes of length 64 from groups of order 4 and 8. Using Theorem 1.2.27, we construct new self-dual codes of length 68. Next, we construct codes of length 68 from groups of order 17. We then find new self-dual codes of length 68 by finding neighbours of these codes, followed by finding neighbours of these neighbours. Magma ([5]) was used to construct all of the codes throughout this section.

The possible weight enumerators for a self-dual Type I $[64,32,12]$-code are given in [20, 28] as:

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

Extremal singly even self-dual codes with weight enumerators $W_{64,1}$ are known ([1, 39, 100]):

$$\beta\in\left\{\begin{array}{c}14,16,18,19,20,22,24,25,26,28,29,30,32,34,\\ 35,36,38,39,44,46,49,53,54,58,59,60,64,74\end{array}\right\}$$

and extremal singly even self-dual codes with weight enumerator $W_{64,2}$ are known for:

$$\beta\in\left\{\begin{array}{c}0,...,40,41,42,44,45,46,47,48,49,50,51,52,54,55,56,57,\\ 58,60,62,64,69,72,80,88,96,104,108,112,114,118,120,184\end{array}\right\}\setminus\{31,39\}.$$

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

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

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

The existence of codes in $W_{68,1}$ are known for ([27]) β =104, 105, 112, 115, 117, 119, 120, 122, 123, 125,..., 284, 287, 289,291, 294, 301, 302, 308, 313, 315, 322, 324, 328,..., 336, 338, 339, 345, 347, 350, 355, 379 and 401.

The first examples of codes with a $\gamma = 7$ in $W_{68,2}$ are constructed in [102]. Together with these, the existence of the codes in $W_{68,2}$ are known for the following parameters (see [39, 102]):
$\gamma = 0,\ \beta \in \{2m | m = 0, 7, 11, 14, 17, 21, \ldots, 99, 102, 105, 110, 119, 136, 165\};$ or
$\beta \in \{2m + 1 | m = 3, 5, 8, 10, 15, 16, 17, 20, \ldots, 82, 87, 93, 94, 101, 104, 110, 115\};$
$\gamma = 1,\ \beta \in \{2m | m = 19, 22, \ldots, 99\};$ or $\beta \in \{2m + 1 | m = 24, \ldots, 85\};$
$\gamma = 2,\ \beta \in \{2m | m = 29, \ldots, 100, 103, 104\};$ or$\beta \in \{2m + 1 | m = 32, \ldots, 81, 84, 85, 86\};$
$\gamma = 6$ with $\beta \in \{2m | m = 69, 77, 78, 79, 81, 88\}$
$\gamma = 7$ with $\beta \in \{7m | m = 14, \ldots, 39, 42\}$.

Firstly, we construct self-dual codes of length 64 from C_4 (over $\mathbb{F}_4 + u\mathbb{F}_4$), $C_{4,2}$ (over $\mathbb{F}_2 + u\mathbb{F}_2$) and C_8 (over $\mathbb{F}_2 + u\mathbb{F}_2$). We then construct three self-dual codes of length 68 (Table 6.1) by applying theorem 1.2.27 to the codes constructed in Tables 6.1,6.2 and 6.3. We replace $1 + u \in \mathbb{F}_2 + u\mathbb{F}_2$ with 3 to save space. The calculation on Magma is shown in Appendix A.4, in order to construct a code of length 32 using the groups C_8 and C_8. Lifting these codes over R_1 produces the code of length 64 in Table 6.2.

Table 6.1: Self-dual code over $\mathbb{F}_4 + u\mathbb{F}_4$ of length 32 from C_4 and C_4.

A_i	$v \in C_4$	$v \in C_4$	r_A	$\lvert Aut(A_i)\rvert$	β
1	(8966)	(0000)	(A617)	2^4	0

Table 6.2: Self-dual code over R_1 of length 64 from C_8 and C_8.

B_i	$v \in C_8$	$v \in C_8$	r_A	$\lvert Aut(B_i)\rvert$	β
1	(uuu10311)	(uu011uu0)	(u0300013)	2^3	0

Table 6.3: Self-dual code over R_1 of length 64 from C_{42} and C_{42}.

C_i	$v \in C_{42}$	$v \in C_{42}$	r_A	$\lvert Aut(C_i)\rvert$	β
1	(uu01u0u1)	(u0u11u31)	(u3u3u3u0)	2^4	48

We now construct two self-dual codes of length 68 using C_{17} (Table 6.5). We let $v_2 = 0 \in RC_{17}$. We note that in this case, the construction is equivalent to the usual four circulant construction.

Table 6.4: Self-dual code of length 68 from extensions of C_1, C_2 and C_3.

D_i	Code	c	X	γ	β	$\lvert Aut(E_i)\rvert$
1	A_1	1	$(0133010303011u1001333u01031uuu1u)$	4	113	2
2	B_1	$u+1$	$(013011030003013301111030uuu13u10)$	**2**	**61**	2
3	C_1	$u+1$	$(0u10303u110333001103u00130103303)$	**1**	**179**	2

Table 6.5: Self-dual codes over $\mathbb{F}_2$ of length 68 ($W_{68,2}$) from C_{17} and C_{17}.

E_i	$v_1 \in C_{17}$	$v_2 \in C_{17}$	r_A	$\lvert Aut(D_i)\rvert$	γ	β
1	(00000000000011011)	(00000000000000000)	(00100110010110111)	$2^2 \cdot 17$	0	238
2	(00000000110001111)	(00000000000000000)	(00100100101010101)	$2^2 \cdot 17$	0	272

We now construct neighbours of these codes, and neighbours of these neighbours.

Tables 6.6 to 6.12 show the repeated process of finding neighbours from neighbours in order to construct numerous interesting results.

Table 6.6: New codes of length 68 from neighbours of E_1 and E_2

F_i	E_i	$(x_{35}, x_{36}, ..., x_{68})$	$\lvert Aut(F_i)\rvert$	γ	β	Type
1	2	(01110111001000110000001001000100110)	2	**0**	**208**	$W_{68,2}$
2	2	(11100000111110000110000111110011000)	1	**0**	**214**	$W_{68,2}$
3	2	(00010001000011101111000010100110 10)	2	**1**	**191**	$W_{68,2}$
4	2	(00101111111111100011110010101110 01)	2	**1**	**202**	$W_{68,2}$
5	1	(10011011110111001100010100001011 0)	1	**1**	**210**	$W_{68,2}$
6	2	(01010010001110011000111100110001 01)	1	**1**	**211**	$W_{68,2}$
7	2	(00101011010101001111000000010100 01)	1	**1**	**229**	$W_{68,2}$
8	2	(11111111111111111111011101111111 1)	1		**317**	$W_{68,1}$

Table 6.7: New codes of length 68 from neighbours of F_7 and F_8

G_i	F_i	$(x_{35}, x_{36}, ..., x_{68})$	$\lvert Aut(G_i)\rvert$	γ	β	Type
1	8	(00010011011100000000000101011001100)	1	**0**	**218**	$W_{68,2}$
2	7	(01100000100010001110001110001000 10)	1	**1**	**193**	$W_{68,2}$
3	7	(10001001010110000110111100110000 00)	1	**1**	**195**	$W_{68,2}$
4	7	(01010010100100100001001001010010 01)	1	1	233	$W_{68,2}$
5	7	(01110100100010010010000000100101 010)	1	**2**	**193**	$W_{68,2}$
6	7	(11000100110000101101110111011011 11)	1	**2**	**195**	$W_{68,2}$

Table 6.8: New codes of length 68 from neighbours of G_5

H_i	G_i	$(x_{35}, x_{36}, ..., x_{68})$	$\lvert Aut(H_i)\rvert$	γ	β	Type
1	5	(00100101100110000000101110011111 10)	1	**1**	**197**	$W_{68,2}$
2	5	(01000010110010111010101101110111 11)	1	**1**	**199**	$W_{68,2}$
3	5	(11010010111011010111111101111001 11)	1	**2**	**199**	$W_{68,2}$
4	5	(00110000110011100110000011000000 01)	1	**2**	**191**	$W_{68,2}$
5	5	(00011001001100100101010001111001 00)	1	**2**	**204**	$W_{68,2}$
6	5	(10111010010000011010010101110111 01)	1	**2**	**218**	$W_{68,2}$

Table 6.9: Code of length 68 from the neighbours of D_1

I_i	D_i	$(x_{35}, x_{36}, ..., x_{68})$	$\lvert Aut(I_i)\rvert$	γ	β	Type
1	1	(11110001101100111101110010101111 01)	1	5	133	$W_{68,2}$

Table 6.10: Code of length 68 from the neighbours of I_1

J_i	I_i	$(x_{35}, x_{36}, ..., x_{68})$	$\lvert Aut(J_i)\rvert$	γ	β	Type
1	1	(00001000010110001110010101000011 00	1	6	141	$W_{68,2}$

Table 6.11: New codes of length 68 from the neighbours of J_1

K_i	J_i	$(x_{35}, x_{36}, ..., x_{68})$	$\lvert Aut(K_i)\rvert$	γ	β	Type
1	1	(11111111010011000101000001000010100)	1	**6**	**131**	$W_{68,2}$
2	1	(00000011100101111011100111111001111)	1	**7**	**158**	$W_{68,2}$

Table 6.12: New codes of length 68 from the neighbours of K_2

L_i	K_i	$(x_{35}, x_{36}, ..., x_{68})$	$\lvert Aut(L_i)\rvert$	γ	β	Type
1	2	(01101111110101000111010100111010101)	1	**7**	**155**	$W_{68,2}$
2	2	(01010101010100010010100111011100 10)	1	**7**	**156**	$W_{68,2}$
3	2	(00100111010101010101110111110110110)	1	**7**	**157**	$W_{68,2}$
4	2	(11011111101101110011111101011011 00)	1	**7**	**159**	$W_{68,2}$
5	2	(10010111110001100011111101100101110)	1	**7**	**160**	$W_{68,2}$
6	2	(11000001001000000101001011000110 10)	1	**7**	**162**	$W_{68,2}$
7	2	(10000100000101100001111100100111 11)	1	**7**	**164**	$W_{68,2}$
8	2	(01000010011011111111010000101010001)	1	**7**	**165**	$W_{68,2}$
9	2	(00111010001000110111010011111011 11)	1	**7**	**167**	$W_{68,2}$

Chapter 7

New Extremal Binary Self-dual Codes from block circulant matrices and block quadratic residue circulant matrices

A special type of cyclic code is a quadratic-residue code. While quadratic-residue code have been studied extensively since the early 1970's ([2,77,98]), the theory is lacking when it comes to extremal self-dual codes.

If we consider the double circulant construction $(I \mid A)$ where A is an $n \times n$ circulant matrix over a ring R, clearly the search field in this cases is $|R|^n$. In [33], Gaborit introduced this notion of a quadratic residue circulant matrix where by the search field is considerably reduced. We define the quadratic residue circulant matrix as follows:

Let $\mathbb{F}_{p^k}$ be the Galois field of p^k elements. Let $\gamma_i \in \mathbb{F}_p^k$, A be a $p \times p$ circulant matrix, $Q_r(a,b,c)$ be the $p \times p$ quadratic residue circulant matrix with three free variables, obtained through the quadratic residues and non-residues modulo p. Thus, the first row of $\overline{r} = (r_0, r_1, \ldots, r_{p-1})$ of $Q_p(a,b,c)$ is determined by the following rule:

$$r_i = \begin{cases} a & \text{if } i = 0 \\ b & \text{if } i \text{ is a quadratic residue modulo } p \\ c & \text{if } i \text{ is a quadratic non-residue modulo } p. \end{cases}$$

In [33], many self-dual and extremal self-dual codes were produced by replacing A with $Q_p(a,b,c)$ in the usual double circulant construction. Additionally, self-dual codes from generator matrices of the form

$$\left(\begin{array}{c|ccc|c|ccc} \gamma_1 & \gamma_2 & \cdots & \gamma_2 & \gamma_3 & \gamma_4 & \cdots & \gamma_4 \\ \hline \gamma_2 & & & & \gamma_4 & & & \\ \vdots & & I & & \vdots & & Q_p(a,b,c) & \\ \gamma_2 & & & & \gamma_4 & & & \end{array}\right)$$

were considered where $\gamma_i \in \mathbb{F}_{p^k}$. In [75], this technique is extended to consider constructing self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ (where $u^3 = u$) from the generator matrix:

$$\left(\begin{array}{c|c|ccc} & \lambda & \beta & \cdots & \beta \\ \hline & \gamma & & & \\ I_{p+1} & \vdots & & Q_p(a,b,c) & \\ & \gamma & & & \end{array}\right)$$

where $Q_p(a, b, c)$ is the quadratic residue circulant matrix defined above over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ and over $\lambda, \beta, \gamma \in \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. In [37], these techniques were extended to constructing self-dual codes from generator matrices of the form $(Q_p(a, b, c)|A)$ and

$$\left(\begin{array}{c|ccc|c|ccc} \gamma_1 & \gamma_2 & \cdots & \gamma_2 & \gamma_3 & \gamma_4 & \cdots & \gamma_4 \\ \hline \gamma_2 & & & & \gamma_4 & & & \\ \vdots & & Q_p(a,b,c) & & \vdots & & A & \\ \gamma_2 & & & & \gamma_4 & & & \end{array}\right),$$

where A is a $p \times p$ circulant matrix. In this chapter we consider constructing self-dual codes from generator matrices of the form

$$\left(\begin{array}{ccc|ccc} Q_0 & Q_1 & Q_2 & A_0 & A_1 & A_2 \\ Q_2 & Q_0 & Q_1 & A_2 & A_0 & A_1 \\ Q_1 & Q_2 & Q_0 & A_1 & A_2 & A_0 \end{array}\right)$$

where Q_i are quadratic residue circulant matrices and A_i are $p \times p$ circulant matrices.

We begin with discussing some important properties of quadratic residue circulant matrices. Following the fundamental theory, we describe the construction itself. We provide theoretical results that establish certain conditions when this construction yields self-dual codes. This chapter concludes with applying the construction to find many known and unknown self-dual codes that had not been previously constructed.

7.1 Quadratic Residue Circulant Matrices

Let $Q_p(a_i, b_i, c_i)$ be the i^{th}-$p \times p$ quadratic circulant matrix, where $a_i, b_i, c_i \in R$ and p is a prime number and $0 \leq i \leq 2$. For the purpose of this chapter, we need to evaluate $Q_p(a_i, b_i, c_i)Q_p(a_j, b_j, c_j)^T$. From [33], we can clearly see that $Q_p(a_i, b_i, c_i)Q_p(a_i, b_i, c_i)^T$

$$= \begin{cases} Q_p(a_i^2, b_i^2 + k(b_i^2 + c_i^2), c_i^2 + k(b_i^2 + c_i^2)) & \text{if } p = 4k+1 \\ Q_p(a_i^2 + b_i^2 + c_i^2, a_ib_i + a_ic_i + b_ic_i + (b_i^2 + c_i^2)k, a_ib_i + a_ic_i + b_ic_i + (b_i^2 + c_i^2)k) & \text{if } p = 4k+3 \end{cases}.$$

$k \in \mathbb{Z}$. We will now calculate $Q_p(a_i, b_i, c_i)Q_p(a_j, b_j, c_j)^T$. First we will consider the case when $p = 4k + 1$, followed by the case when $p = 4k + 3$.

Theorem 7.1.1 *If $p = 4k + 1$ then* $Q_p(a_i, b_i, c_i)Q_p(a_j, b_j, c_j)^T$

$= Q_p(a_ia_j, a_ib_j+b_ia_j+(k+1)b_ib_j+k(b_ic_j+c_ib_j)+kc_ic_j, a_ic_j+c_ia_j+kb_ib_j+k(b_ic_j+c_ib_j+(k+1)c_ic_j).$

Proof. Assume that $p = 4k + 1$. Let $Q = Q_p(0, 1, 0)$ and $N = Q_p(0, 0, 1)$, then

$$\begin{aligned} Q_p(a_i, b_i, c_i)Q_p(a_j, b_j, c_j)^T &= (a_iI + b_iQ + c_iN)(a_jI + b_jQ + c_jN)^T \\ &= (a_iI + b_iQ + c_iN)(a_jI + b_jQ^T + c_jN^T) \\ &= a_ia_jI + a_ib_jQ^T + a_ic_jN^T + b_ia_jQ + b_ib_jQQ^T \\ &\quad + b_ic_jQN^T + c_ia_jN + c_ib_jNQ^T + c_ic_jNN^T. \end{aligned}$$

Recall ([34]) that $Q = Q^T$, $N = N^T$, $QQ^T = (k + 1)Q + kN$, $QN^T = NQ^T = k(Q + N)$ and $NN^T = kQ + (k + 1)N$. Therefore,

$$\begin{aligned} Q_p(a_i, b_i, c_i)Q_p(a_j, b_j, c_j)^T =& a_ia_jI + (a_ib_j + b_ia_j)Q + (a_ic_j + c_ia_j)N + b_ib_j((k + 1)Q + kN) \\ &+ (b_ic_i + c_ib_j)(k(Q + N)) + c_ic_j(kQ + (k + 1)N) \\ =& a_ia_jI + (a_ib_j + b_ia_j)Q + (a_ic_j + c_ia_j)N + b_ib_j(k + 1)Q + b_ib_jkN \\ &+ (b_ic_i + c_ib_j)kQ + (b_ic_i + c_ib_j)kN + c_ic_jkQ + c_ic_j(k + 1)N \\ =& I[a_ia_j] + Q[a_ib_j + b_ia_j + (k + 1)b_ib_j + k(b_ic_j + c_ib_j) + kc_ic_j] \\ &+ N[a_ic_j + c_ia_j + kb_ib_j + k(b_ic_j + c_ib_j) + (k + 1)c_ic_j] \end{aligned}$$

$= Q_p(a_ia_j, a_ib_j+b_ia_j+(k+1)b_ib_j+k(b_ic_j+c_ib_j)+kc_ic_j, a_ic_j+c_ia_j+kb_ib_j+k(b_ic_j+c_ib_j)+(k+1)c_ic_j).$ ■

Theorem 7.1.2 *If $p = 4k + 3$ then* $Q_p(a_i, b_i, c_i)Q_p(a_j, b_j, c_j)^T$

$$= Q_p(a_ia_j + b_ib_j + c_ic_j, (a_ic_j + b_ia_j) + k(b_ib_j + c_ic_j) + kb_ic_j + (k + 1)c_ib_j, \\ (a_ib_j + c_ia_j) + k(b_ib_j + c_ic_j) + (k + 1)b_ic_j + kc_ib_j).$$

Proof. Assume that $p = 4k + 3$. Then

$$\begin{aligned} Q_p(a_i, b_i, c_i)Q_p(a_j, b_j, c_j)^T = a_ia_jI + a_ib_jQ^T + a_ic_jN^T + b_ia_jQ + b_ib_jQQ^T \\ + b_ic_jQN^T + c_ia_jN + c_ib_jNQ^T + c_ic_jNN^T. \end{aligned}$$

Recall ([34]) that $Q = N^T$, $QQ^T = NN^T = I + kQ + kN$, $QN^T = kQ + (k + 1)N$ and $NQ^T = (k + 1)Q + kN$. Therefore,

$$
\begin{aligned}
Q_p(a_i,b_i,c_i)Q_p(a_j,b_j,c_j)^T =& a_ia_jI + (a_ic_j + b_ia_j)Q + (a_ib_j + c_ia_j)N + (b_ib_j + c_ic_j)QQ^T \\
&+ b_ic_jQN^T + c_ib_jNQ^T \\
=& a_ia_jI + (a_ic_j + b_ia_j)Q + (a_ib_j + c_ia_j)N + (b_ib_j + c_ic_j)(I + kQ + kN) \\
&+ b_ic_j(kQ + (k+1)N) + c_ib_j((k+1)Q + kN) \\
=& a_ia_jI + (a_ic_j + b_ia_j)Q + (a_ib_j + c_ia_j)N + (b_ib_j + c_ic_j)I + k(b_ib_j + c_ic_j)Q \\
&+ k(b_ib_j + c_ic_j)N + kb_ic_jQ + (k+1)b_ic_jN + (k+1)c_ib_jQ + kc_ib_jN \\
=& I[a_ia_j + b_ib_j + c_ic_j] + Q[(a_ic_j + b_ia_j) + k(b_ib_j + c_ic_j) + kb_ic_j \\
&+ (k+1)c_ib_j] + N[(a_ib_j + c_ia_j) + k(b_ib_j + c_ic_j) + (k+1)b_ic_j + kc_ib_j] \\
=& Q_p(a_ia_j + b_ib_j + c_ic_j, (a_ic_j + b_ia_j) + k(b_ib_j + c_ic_j) + kb_ic_j + (k+1)c_ib_j, \\
&(a_ib_j + c_ia_j) + k(b_ib_j + c_ic_j) + (k+1)b_ic_j + kc_ib_j)
\end{aligned}
$$

■

7.2 The Construction

We shall now describe the main construction itself and provide conditions when this technique produces self-dual codes. Let $Q_l = Q_p(a_l, b_l, c_l)$. Define the matrix

$$
M = \left(\begin{array}{ccc|ccc} Q_0 & Q_1 & Q_2 & A_0 & A_1 & A_2 \\ Q_2 & Q_0 & Q_1 & A_2 & A_0 & A_1 \\ Q_1 & Q_2 & Q_0 & A_1 & A_2 & A_0 \end{array} \right)
$$

and let $\mathcal{C}$ be the linear code of length $6p$ generated by the matrix M, where A_i are $p \times p$ circulant matrices over R. Let $CIRC(A_1, \ldots, A_n)$ be the block circulant matrix where the first row of block matrices are $A_1, \ldots, A_n$ and $a_{[l]_3} = a_{(l \mod 3)}$, then

$$
MM^T = CIRC\left(\sum_{i=0}^{2} (Q_iQ_i^T + A_iA_i^T), \sum_{i=0}^{2} Q_iQ_{[(i+2)]_3}^T + A_iA_{[(i+2)]_3}^T, \left(\sum_{i=0}^{2} Q_iQ_{[(i+2)]_3}^T + A_iA_{[(i+2)]_3}^T \right)^T \right).
$$

Clearly, C is self-orthogonal if and only $\sum_{i=0}^{2} A_iA_i^T = \sum_{i=0}^{2} Q_iQ_i^T$ and $\sum_{i=1}^{3} A_iA_{[(i+2)]_3}^T = \sum_{i=1}^{3} Q_iQ_{[(i+2)]_3}^T$.

Using Theorem 7.1.1, we can see that $\sum_{i=0}^{2} Q_i Q_i^T =$

$$\begin{cases} Q_p\left(\sum_{i=0}^{2} a_i^2, \sum_{i=0}^{2}(b_i^2 + k(b_i^2+c_i^2)), \sum_{i=0}^{2}(c_i^2 + k(b_i^2+c_i^2))\right) & \text{if } p = 4k+1 \\ Q_p\left(\sum_{i=0}^{2}(a_i^2+b_i^2+c_i^2), \sum_{i=0}^{2}(a_ib_i + a_ic_i + b_ic_i + k(b_i^2+c_i^2)),\right. & \\ \left.\sum_{i=0}^{2}(a_ib_i + a_ic_i + b_ic_i + k(b_i^2+c_i^2))\right) & \text{if } p = 4k+3 \end{cases}.$$

Additionally (by Theorem 7.1.2), if $p = 4k+1$ then

$$\sum_{i=1}^{3} Q_i Q_{[(i+2)]_3}^T = Q_p\left(\sum_{i=0}^{2} a_i a_{[(i+2)]_3}, \sum_{i=0}^{2}(a_i b_{[(i+2)]_3} + b_i a_{[(i+2)]_3} + (k+1)b_i b_{[(i+2)]_3} + k(b_i c_{[(i+2)]_3} + c_i b_{[(i+2)]_3} + kc_i c_{[(i+2)]_3}), \sum_{i=0}^{2}(a_i c_{[(i+2)]_3} + c_i a_{[(i+2)]_3} + kb_i b_{[(i+2)]_3} + k(b_i c_{[(i+2)]_3} + c_i b_{[(i+2)]_3} + (k+1)c_i c_{[(i+2)]_3})\right)$$

and if $p = 4k+3$ then

$$\sum_{i=1}^{3} Q_i Q_{[(i+2)]_3}^T = Q_p\left(\sum_{i=0}^{2}(a_i a_{[(i+2)]_3} + b_i b_{[(i+2)]_3} + c_i c_{[(i+2)]_3}, \sum_{i=0}^{2}[(a_i c_{[(i+2)]_3} + b_i a_{[(i+2)]_3}) + k(b_i b_{[(i+2)]_3} + c_i c_{[(i+2)]_3}) + kb_i c_{[(i+2)]_3} + (k+1)c_i b_{[(i+2)]_3}], \sum_{i=0}^{2}[(a_i b_{[(i+2)]_3} + c_i a_{[(i+2)]_3}) + k(b_i b_{[(i+2)]_3} + c_i c_{[(i+2)]_3}) + (k+1)b_i c_{[(i+2)]_3} + kc_i b_{[(i+2)]_3})]\right)$$

Combining these results, we reach the following:

Theorem 7.2.1 *If $p = 4k+1$, then C is a self-orthogonal code if and only if the following conditions hold:*

1. $\sum_{i=0}^{2} A_i A_i^T = Q_p\left(\sum_{i=0}^{2} a_i^2, \sum_{i=0}^{2}(b_i^2 + k(b_i^2+c_i^2)), \sum_{i=0}^{2}(c_i^2 + k(b_i^2+c_i^2))\right)$,
2. $$\sum_{i=1}^{3} A_i A_{[(i+2)]_3}^T = Q_p\left(\sum_{i=0}^{2} a_i a_{[(i+2)]_3}, \sum_{i=0}^{2}(a_i b_{[(i+2)]_3} + b_i a_{[(i+2)]_3} + (k+1)b_i b_{[(i+2)]_3} + k(b_i c_{[(i+2)]_3} + c_i b_{[(i+2)]_3} + kc_i c_{[(i+2)]_3}), \sum_{i=0}^{2}(a_i c_{[(i+2)]_3} + c_i a_{[(i+2)]_3} + kb_i b_{[(i+2)]_3} + k(b_i c_{[(i+2)]_3} + c_i b_{[(i+2)]_3} + (k+1)c_i c_{[(i+2)]_3})\right).$$

Theorem 7.2.2 *If $p = 4k+3$, then C is a self-orthogonal code if and only if the following conditions hold:*

1. $\sum_{i=0}^{2} A_i A_i^T = Q_p\left(\sum_{i=0}^{2}(a_i^2 + b_i^2 + c_i^2), \sum_{i=0}^{2}(a_i b_i + a_i c_i + b_i c_i + k(b_i^2 + c_i^2), \sum_{i=0}^{2}(a_i b_i + a_i c_i + b_i c_i + k(b_i^2 + c_i^2) \right)$,

2. $$\sum_{i=1}^{3} A_i A_{[(i+2)]_3}^T = Q_p \left(\sum_{i=0}^{2} (a_i a_{[(i+2)]_3} + b_i b_{[(i+2)]_3} + c_i c_{[(i+2)]_3}, \sum_{i=0}^{2}[(a_i c_{[(i+2)]_3} + b_i a_{[(i+2)]_3}) + k b_i b_{[(i+2)]_3} + k c_i c_{[(i+2)]_3} + k b_i c_{[(i+2)]_3} + (k+1) c_i b_{[(i+2)]_3}], \sum_{i=0}^{2}[(a_i b_{[(i+2)]_3} + c_i a_{[(i+2)]_3}) + k b_i b_{[(i+2)]_3} + k c_i c_{[(i+2)]_3} + (k+1) b_i c_{[(i+2)]_3} + k c_i b_{[(i+2)]_3})] \right).$$

Theorem 7.2.3 *The matrix M has full rank if and only if the following conditions hold:*

1. $\sum_{i=0}^{2}(A_i C_i + A_i D_i) = I_p$,

2. $\sum_{i=0}^{2}(A_i C_{[i+2]_3} + A_i D_{[i+2]_3}) = 0_p$ *and*

3. $\sum_{i=0}^{2}(A_i C_{[i+1]_3} + A_i D_{[i+1]_3}) = 0_p$

for some $p \times p$ circulant matrices C_k and D_l over R.

Proof. Clearly,

$$M = \left(\; CIRC(Q_0, Q_1, Q_2) \;\middle|\; CIRC(A_0, A_1, A_2) \; \right)$$

has full rank iff $MN = I_{3p}$ for some $6p \times 3p$ matrix N over R. Let $N' = (n_1, \ldots, n_{6p})^T$ be the first column of N, clearly $M(circ(n_1, \ldots, n_p)^T, \ldots, circ(n_{5p+1}, \ldots, n_{6p})^T)^T = (I_p, 0_p, 0_p, 0_p, 0_p, 0_p)^T$. If $N'' = (C_0, C_1, C_2, D_0, D_1, D_2)^T$ is the matrix that satisfies $MN'' = (I_p, 0_p, 0_p, 0_p, 0_p, 0_p)^T$, then N can take the form

$$N = \begin{pmatrix} CIRC(C_0, C_2, C_1) \\ CIRC(D_0, D_2, D_1) \end{pmatrix}$$

where C_k and D_l are $p \times p$ circulant matrices over R. Now,

$$MN = CIRC\left(\sum_{i=0}^{2}(A_i C_i + A_i D_i), \sum_{i=0}^{2}(A_i C_{[i+2]_3} + A_i D_{[i+2]_3}), \sum_{i=0}^{2}(A_i C_{[i+1]_3} + A_i D_{[i+1]_3}) \right)$$

and M has full rank if and only if:

1. $\sum_{i=0}^{2}(A_iC_i + A_iD_i) = I_p$,
2. $\sum_{i=0}^{2}(A_iC_{[i+2]_3} + A_iD_{[i+2]_3}) = 0_p$ and
3. $\sum_{i=0}^{2}(A_iC_{[i+1]_3} + A_iD_{[i+1]_3}) = 0_p$

■

Theorem 7.2.4 *Let $\mathcal{C}$ be self-dual. Then,*

$$\left(\sum_{i=0}^{2} Q_i\right) B + \left(\sum_{i=0}^{2} Q_i\right)^T B' = I_p$$

for some $p \times p$ matrices B and B' over R.

Proof. By the previous result,

1. $\sum_{i=0}^{2}(A_iC_i + A_iD_i) = I_p$,
2. $\sum_{i=0}^{2}(A_iC_{[i+2]_3} + A_iD_{[i+2]_3}) = 0_p$ and
3. $\sum_{i=0}^{2}(A_iC_{[i+1]_3} + A_iD_{[i+1]_3}) = 0_p$.

Adding these equations, we obtain that

$$\left(\sum_{i=0}^{2} Q_i\right)\left(\sum_{i=0}^{2} C_i\right) + \left(\sum_{i=0}^{2} A_i\right)\left(\sum_{i=0}^{2} D_i\right) = I_p.$$

Let $Q_3 = \sum_{i=0}^{2} Q_i$, $A_3 = \sum_{i=0}^{2} A_i$, $C_3 = \sum_{i=0}^{2} C_i$ and $D_3 = \sum_{i=0}^{2} D_i$. Thus,

$$Q_3C_3 + A_3D_3 = I_p$$

and

$$(Q_3C_3 + A_3D_3)^T = C_3^TQ_3^T + D_3^TA_3^T = Q_3^TC_3^T + A_3^TD_3^T = I_p$$

since circulant matrices commute. Therfore,

$$\begin{aligned} Q_3C_3 + A_3D_3 &= Q_3C_3 + A_3(Q_3^TC_3^T + A_3^TD_3^T)D_3 \\ &= Q_3C_3 + A_3Q_3^TC_3^TD_3 + A_3A_3^TD_3^TD_3 \\ &= I_p. \end{aligned}$$

If $\mathcal{C}$ is self-dual, then $MM^T = 0_{3p}$ and

$$\begin{pmatrix} I_p & I_p & I_p \end{pmatrix} MM^T \begin{pmatrix} I_p & I_p & I_p \end{pmatrix}^T = 0_p.$$

Consequently,

$$\begin{pmatrix} Q_3 & Q_3 & Q_3 & A_3 & A_3 & A_3 \end{pmatrix} \begin{pmatrix} Q_3 & Q_3 & Q_3 & A_3 & A_3 & A_3 \end{pmatrix}^T = 0_p \text{ and } Q_3Q_3^T = A_3A_3^T.$$

Finally,

$$\begin{aligned} I_p &= Q_3C_3 + A_3Q_3^TC_3^TD_3 + A_3A_3^TD_3^TD_3 \\ &= Q_3C_3 + A_3Q_3^TC_3^TD_3 + Q_3Q_3^TD_3^TD_3 \\ &= Q_3C_3 + Q_3Q_3^TD_3^TD_3 + A_3Q_3^TC_3^TD_3 \\ &= Q_3(C_3 + Q_3^TD_3^TD_3) + Q_3^T(A_3C_3^TD_3) \\ &= Q_3B + Q_3^TB' \end{aligned}$$

where $B = C_3 + Q_3^TD_3^TD_3$ and $B' = A_3C_3^TD_3$. ■

Theorem 7.2.5 *Assume that $p = 4k + 1$ and let $\mathcal{C}$ be self-dual. Then $\sum_{i=0}^{2} Q_i$ is invertible.*

Proof. By the previous result,

$$\left(\sum_{i=0}^{2} Q_i\right) B + \left(\sum_{i=0}^{2} Q_i\right)^T B' = I_p$$

for some $p \times p$ matrices B and B' over R. Clearly, $Q_i = a_iI_p + b_iQ + c_iN$ where $Q = Q_p(0, 1, 0)$, $N = Q_p(0, 0, 1)$. Now,

$$\begin{aligned} Q_i^T &= (a_iI_p + b_iQ + c_iN)^T \\ &= a_iI_p + b_iQ^T + c_iN^T \\ &= a_iI_p + b_iQ + c_iN \\ &= Q_i \end{aligned}$$

since $Q = Q^T$, $N = N^T$. Therefore,

$$\left(\sum_{i=0}^{2} Q_i\right) B + \left(\sum_{i=0}^{2} Q_i\right)^T B' = \left(\sum_{i=0}^{2} Q_i\right) B + \left(\sum_{i=0}^{2} Q_i\right) B' = \left(\sum_{i=0}^{2} Q_i\right) (B + B') = I_p$$

and $\sum_{i=0}^{2} Q_i$ is invertible. ■

In the next result, we consider a specific example of a commutative Frobenius ring of characteristic 2. For the purpose of the next result, we assume that R is a local ring with a residue class field that contains 2 elements.

Theorem 7.2.6 *Assume that $p = 4k+3$, let R be a local ring with a residue class field that contains 2 elements and assume that k is even. Let $\mathcal{C}$ be a self-dual code over R. Then $\sum_{i=0}^{2} Q_i$ is invertible.*

Proof. Let $Q_3 = \sum_{i=0}^{2} Q_i$, $a_3 = \sum_{i=0}^{2} a_i$, $b_3 = \sum_{i=0}^{2} b_i$ and $c_3 = \sum_{i=0}^{2} c_i$. Clearly, $Q_3 = a_3 I_p + b_3 Q + c_3 N$ (where $Q = Q_p(0, 1, 0)$, $N = Q_p(0, 0, 1)$) and $Q_3 B + Q_3^T B' = I_p$ for some matrices B and B'. Let J be the unique maximal ideal in R. It remains to show that $Q_3 \pmod J$ is invertible. If $b_3 \equiv c_3 \pmod J$ then

$$Q_3^T \equiv (a_3 I_p + b_3 Q + b_3 N)^T \equiv a_3 I_p + b_3 Q^T + b_3 N^T \equiv a_3 I_p + b_3 N + b_3 Q \equiv Q_3 \pmod J$$

since $Q = N^T$. Therefore,

$$Q_3(B + B') \equiv Q_3 B + Q_3^T B' \equiv I_p \pmod J.$$

and $Q_3 \pmod J$ is invertible.

If $b_3 \not\equiv c_3 \pmod J$ then $b_3 + c_3 \equiv 1 \pmod J$ and

$$(\underbrace{1, \ldots, 1}_{p}) Q_3^T = (\underbrace{1, \ldots, 1}_{p}) Q_3 \equiv (\underbrace{a_3 + b_3 + c_3, \ldots, a_3 + b_3 + c_3}_{p}) \equiv (a_3 + 1)(\underbrace{1, \ldots, 1}_{p}) \pmod J.$$

Thus

$$(\underbrace{1, \ldots, 1}_{p}) Q_3 B + (\underbrace{1, \ldots, 1}_{p}) Q_3^T B' = (\underbrace{1, \ldots, 1}_{p}) I_p,$$

$$(a_3 + 1)(\underbrace{1, \ldots, 1}_{p})(B + B') \equiv (a_3 + 1)(\underbrace{1, \ldots, 1}_{p}) B + (a_3 + 1)(\underbrace{1, \ldots, 1}_{p}) B' \equiv (\underbrace{1, \ldots, 1}_{p}) \pmod J$$

and

$$(a_3 + 1)(\underbrace{1, \ldots, 1}_{p})(B + B')(\underbrace{1, \ldots, 1}_{p})^T \equiv (\underbrace{1, \ldots, 1}_{p})(\underbrace{1, \ldots, 1}_{p})^T \equiv 1 \pmod J.$$

So $a_3 + 1$ is invertible by modulo ideal J and $a_3 \equiv 0 \pmod{J}$. Thus $Q_3 \equiv Q \pmod{J}$ or $Q_3 \equiv N \pmod{J}$ and $Q^2 = N^2 = I_p$ since k is even and $Q^2 = N^2 = I_p + kQ + kN$. Thus $Q_3 \pmod{J}$ is invertible. ■

7.3 Numerical results

In this section, we construct new self-dual codes of length 66 and 68 via certain extensions, neighbours and sequences of neighbours. Initially, we consider the above construction when $p = 5$ over $\mathbb{F}_2 + u\mathbb{F}_2$. We construct an extremal self-dual code (Type I) of length 60 (described in Table 7.1). From this code, we construct an extremal self-dual code (Type I) of length 64 via an $\mathbb{F}_2 + u\mathbb{F}_2$ extension (Table 7.2). Next, we find a new self-dual code of length 66 by a $\mathbb{F}_2$ extension of the previously constructed self-dual code of length 64 (Table 7.3). Finally, we find new self-dual codes of length 68 from a $\mathbb{F}_2 + u\mathbb{F}_2$ extension of the previously constructed self-dual code of length 64 and sequences of neighbours of this code (Tables 7.4, 7.5, 7.6, 7.7 and 7.8). Magma ([5]) was used to construct all of the codes throughout this section.

The possible weight enumerators for a self-dual Type I $[60, 30, 12]$-code is given in [20, 28] as:

$$\begin{aligned} W_{60,1} &= 1 + 3451y^{12} + 24128y^{14} + 336081y^{16} + \cdots, \\ W_{60,2} &= 1 + (2555 + 64\beta)\, y^{12} + (33600 - 384\beta)\, y^{14} + \cdots, 0 \leq \beta \leq 10. \end{aligned}$$

Extremal singly even self-dual codes with weight enumerator $W_{60,1}$ and $W_{60,2}$ are known ([57]) for $\beta \in \{0, 1, \ldots, 8, 10\}$.

Firstly, we construct the $[30, 15, 6]$ code when $p = 5$. The calculation on Magma is given in Appendix A.5. These binary codes are lifted over $\mathbb{F}_2 + u\mathbb{F}_2$ and we construct the following code:

Table 7.1: Self-dual codes of length 60 (codes over $\mathbb{F}_2 + u\mathbb{F}_2$ when $p = 5$)

$\mathcal{C}_i$	(a_1, b_1, c_1)	(a_2, b_2, c_2)	(a_3, b_3, c_3)	v_1	v_2	v_3	$Aut(\mathcal{C}_i)$	β
1	(u, u, u)	$(u, u, 1)$	$(1, u, 0)$	$(u, u, u, u, 0)$	$(u, 0, 0, u, 1)$	$(u, u+1, u+1, u, 0)$	$2^3 \cdot 3 \cdot 5$	0

The possible weight enumerators for a self-dual Type I $[64, 32, 12]$-code are given in [20, 28] as:

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

Extremal singly even self-dual codes with weight enumerators $W_{64,1}$ are known ([1, 39, 100]) for the following:

$$\beta \in \left\{ \begin{array}{c} 14, 16, 18, 19, 20, 22, 24, 25, 26, 28, 29, 30, 32, 34, \\ 35, 36, 38, 39, 44, 46, 49, 53, 54, 58, 59, 60, 64, 74 \end{array} \right\}$$

and extremal singly even self-dual codes with weight enumerator $W_{64,2}$ are known for

$$\beta \in \left\{ \begin{array}{c} 0, ..., 40, 41, 42, 44, 45, 46, 47, 48, 49, 50, 51, 52, 54, 55, 56, 57, \\ 58, 60, 62, 64, 69, 72, 80, 88, 96, 104, 108, 112, 114, 118, 120, 184 \end{array} \right\} \setminus \{31, 39\}.$$

The weight enumerators of an extremal self-dual code of length 66 is given in [28] as follows:

$$\begin{aligned} W_{66,1} &= 1 + (858 + 8\beta)y^{12} + (18678 - 24\beta)y^{14} + \cdots \quad \text{where } 0 \leq \beta \leq 778, \\ W_{66,2} &= 1 + 1690y^{12} + 7990y^{14} + \cdots \quad \text{and} \\ W_{66,3} &= 1 + (858 + 8\beta)y^{12} + (18166 - 24\beta)y^{14} + \cdots \quad \text{where } 14 \leq \beta \leq 756. \end{aligned}$$

Together with the codes recently obtained in [1] and the codes from [68], [69] and [37], extremal singly even self-dual codes with weight enumerator $W_{66,1}$ are known for

$$\beta \in \{0, 1, 2, 3, 5, 6, \ldots, 94, 100, 101, 115\}$$

and extremal singly even self-dual codes with weight enumerator $W_{66,3}$ are known for

$$\beta \in \{22, 23, \ldots, 92\} \setminus \{89, 91\}.$$

The known weight enumerators of a self-dual $[68, 34, 12]_I$-code are as follows ([20, 28]):

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

where $0 \leq \gamma \leq 9$. Codes have been obtained for $W_{68,2}$ when ([40])

$\gamma = 2,\ \beta \in \{2m | m = 29, \ldots, 100, 103, 104\};$ or $\beta \in \{2m + 1 | m = 32, \ldots, 81, 84, 85, 86\};$
$\gamma = 3,\ \beta \in \{2m | m = 39, \ldots, 92, 94, 95, 97, 98, 101, 102\};$ or
$\beta \in \{2m + 1 | m = 38, 40, 43, \ldots, 77, 79, 80, 81, 83, 87, 88, 89, 96\};$
$\gamma = 4,\ \beta \in \{2m | m = 43, 46, \ldots, 58, 60, \ldots, 93, 97, 98, 100\};$ or
$\beta \in \{2m + 1 | m = 48, \ldots, 55, 57, 58, 60, 61, 62, 64, 68, \ldots, 72, 74, 78, 79, 80, 83, 84, 85, 89, 95\};$
$\gamma = 5$ with $\beta \in \{101,105,109,111,...,182,187,189,191,192,193,195,198,200,201,202,211,213\}$
$\gamma = 6,\ \beta \in \{131, 133, 137, \ldots, 202, 203, 206, 207, 210\};$
$\gamma = 7,\ \beta \in \{7m\,| m = 14, \ldots 22, 28, \ldots, 39, 42\}$ or $\beta \in \{155, \ldots, 199\};$
$\gamma = 8,\ \beta \in \{180, \ldots, 221\};$
$\gamma = 9,\ \beta \in \{186, \ldots, 226, 228, 230\};$

Applying Theorem 1.2.27 over $\mathbb{F}_2$ and $\mathbb{F}_2 + u\mathbb{F}_2$ (to the code constructed in Table 7.1), we construct self-dual codes of lengths 64, 66 and 68 (Tables 7.2, 7.3 and 7.4). We replace $1 + u$ with 3 to save space.

Let $\mathcal{N}_{(0)} = \mathcal{F}_1$. Applying the k^{th}-range neighbour formula (Definition 1.2.28), we obtain
We shall now separately consider the neighbours of $\mathcal{N}_{(7)}$, $\mathcal{N}_{(8)}$ and $\mathcal{N}_{(9)}$.

Table 7.2: Self-dual codes of length 64 from $\mathbb{F}_2 + u\mathbb{F}_2$ extensions of codes from Table 7.2

$\mathcal{D}_i$	$\mathcal{C}_i$	c	X	$W_{64,i}$	β	$Aut(\mathcal{D}_i)$
1	1	3	$(uu0u3030u330301013u1u1100u1311)$	1	14	2^2

Table 7.3: Self-dual codes of length 66 from $\mathbb{F}_2$ extensions of codes from Table 7.3 where $x_i = 0$ for $1 \leq i \leq 33$.

$\mathcal{E}_i$	$\mathcal{D}_i$	c	X	$W_{66,i}$	β	$Aut(\mathcal{E}_i)$
1	1	1	$(00111100110110011001111001101011)$	3	**21**	1

Table 7.4: Self-dual codes of length 68 ($W_{68,2}$) from $\mathbb{F}_2 + u\mathbb{F}_2$ extensions of codes from Table 7.2

$\mathcal{F}_i$	$\mathcal{D}_i$	c	X	α	β	$Aut(\mathcal{F}_i)$
1	1	$1+u$	$(0uu01u130130000031100u1u331030u0)$	2	67	2

Table 7.5: i^{th} neighbour of $\mathcal{N}_{(0)}$

i	$\mathcal{N}_{(i+1)}$	x_i	γ	β
0	$\mathcal{N}_{(1)}$	(10100010011111001010101001000000001)	3	103
1	$\mathcal{N}_{(2)}$	(10010101000011110011111000111111110)	4	124
2	$\mathcal{N}_{(3)}$	(11111010111111011110100001101101111)	5	134
3	$\mathcal{N}_{(4)}$	(10101000111000011000110001100100010)	6	149
4	$\mathcal{N}_{(5)}$	(00101010001100010110101010110101110)	6	133
5	$\mathcal{N}_{(6)}$	(00000010010001111011110000001011110)	**7**	**145**
6	$\mathcal{N}_{(7)}$	(11011111011111110011111101010111011)	**8**	**161**
7	$\mathcal{N}_{(8)}$	(10010000011000100001111000000110010)	**8**	**153**
8	$\mathcal{N}_{(9)}$	(00101110110100111000011100000101111)	**9**	**177**

Table 7.6: 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		(10011101000010110010000010110001111)	**6**	**135**	7		(01101011100110001101111011101111101)	**7**	**142**
7		(10101011110100000111010110100001)	**7**	**144**	7		(10100000010011001000110011100101110)	**7**	**148**
7		(11000001000001000001111101000011000)	**7**	**150**	7		(00000011011010100111001100000101010)	**7**	**152**
7		(11000010101000000101010001010000011)	**8**	**156**	7		(01110111010111110100011111011111101)	**8**	**157**
7		(10011101110111101111110110100110111)	**8**	**158**	7		(11001111011100010011010111111111010)	**8**	**159**
7		(01111111111111011110110100010011110)	**8**	**160**	7		(00000101000110100000111000000110110)	**8**	**162**
7		(10111001101101111100011110101110001)	**8**	**163**	7		(10000011000111010100010011011100111)	**8**	**164**
7		(01011010101111111000000101100110 10)	**8**	**165**	7		(11001111101111110110001111011011 01)	**8**	**166**
7		(01101100110001011011010100000111011)	**8**	**167**	7		(11100010010110010000101011011011 11)	**8**	**168**
7		(00001100011001111001100101100000100)	**8**	**169**	7		(11011000010101001111110001100100 00)	**8**	**170**
7		(01001111010111010000000011111011110)	**8**	**171**	7		(11010111001010011110000010101011 01)	**8**	**172**
7		(00110111110101111101000100110011 10)	**8**	**173**	7		(10000001111111101100001110011101 00)	**8**	**174**
7		(10001110100011011010000010101001 11)	**8**	**175**	7		(10110110011101001010000110000100 11)	**8**	**176**
7		(11011101000110111000101101010 0001)	**8**	**177**	7		(00000010011110100001011010110001 01)	**8**	**178**
7		(10101101111101110001001010100 00110)	**8**	**179**					

Table 7.7: 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
8		(10111000000001000110010110010 10000)	**6**	**134**	8		(01000110110011100100101100000 110000)	**7**	**146**
8		(10000100011010000001101100010 01100)	**8**	**154**	8		(01000101111010000101111001010 11101)	**8**	**155**

Table 7.8: 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
9		(10110000101110010111111001011111 11)	**9**	**169**	9		(01110110110111001110101010111 01011)	**9**	**171**
9		(10101110011010001111101011111 10011)	**9**	**173**	9		(10001001011111111111011111 01000011)	**9**	**174**
9		(10010101001111100111110001011 00001)	**9**	**175**	9		(11001100010000100110000110000 10100)	**9**	**176**
9		(00001111000101101100000100111 01110)	**9**	**178**	9		(00001111110011101110001111000 10001)	**9**	**179**
9		(00101101100000001011001111001 010110)	**9**	**180**	9		(11011000011010110100001100101 01111)	**9**	**181**
9		(10000100100011011101101001111 00100)	**9**	**182**	9		(11110101011101100011101011100 11011)	**9**	**183**
9		(01010011111000111110100110111 11011)	**9**	**184**	9		(10110000000011001111000011000 11001)	**9**	**185**

Chapter 8

Conclusion

To conclude, we consider future work as an extension of this thesis. We reflect on the work published and review the importance of the theory and numerical results. There are many opportunities throughout this work to extend the theory or consider different paths; here are some of the suggested routes for future research.

In chapter 2, the structure of $\mathcal{U}(\mathbb{F}_{3^t}(C_n \times D_6))$ was established. Going forward, we could try to extend the techniques used in this calculation to establish the structure of $\mathcal{U}(\mathbb{F}_{3^t} D_{2\cdot 3^n})$.

Throughout chapters 3 to 7, codes over $\mathbb{F}_2$, $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$ were mainly considered. In future other alphabets could be considered. For example $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_7$, $\mathbb{Z}_4$ or even non-commutative rings. Additionally, larger groups could be considered as we have mainly dealt with small groups.

Let C is a self-dual $[2n, n, d]$ code over $\mathbb{F}_q$. If $d \leq 3\lfloor \frac{n}{12} \rfloor + 3$, then C is extremal of type III ([59]). If $d \leq 2\lfloor \frac{n}{6} \rfloor + 2$, then C is extremal of type IV ([59]). The techniques described in chapters 3 to 7 inclusively, could be used in order to find unknown extremal type III and type IV codes.

We established a new technique by combining group rings with well established techniques such as the double circulant construction, four circulant construction, four block construction and quadratic residue circulants. Future work could consider combining group rings with other well known techniques, such as:

1. constructing self-dual codes with the assumption that the automorphism group of the codes have a certain size; this technique assumes that the automorphsim group has a certain size and builds the code based on this assumption. It has been extensively used since the early 1970's ([7, 38, 64, 65, 103]).

2. constructing self-dual codes from groups acting on the affine polar graph; in [18], the authors construct an extremely unusual extremal self-dual type I code of length 68 by considering the action of A_8 (the alternating group on 8 elements) on the affine polar graph.

Finally, constructing other classes of codes using group rings could be considered. In [62] and [63], group rings were used to construct MDS codes and LDPC codes. In [83], group rings were used to

construct LCD and LCP codes. However, there was no link to any type of well known elements of group rings. Another possible avenue to explore would be to link certain well known group ring elements to the construction of LCD and LCP codes.

Appendices

Appendix A

Magma Programs

In this section, we include a small selection of the programs implemented by MAGMA to construct the codes in Chapters 3, 4, 5, 6 and 7.

A.1 Chapter 3

Here we present the program used to construct the $[24, 12, 8]$ code using the group algebra $\mathbb{F}_2(C_3 \times D_8)$ (Section 3.2.1).

```
t:=Cputime();
SetLogFile("C3D8.txt");

Rk:=GF(2);
codeF2:=[];
M:=[];

Mtemp1:=RMatrixSpace(Rk,24,24)!0;

function cycgen(gg)
  n:=4;
  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;

function revcycgen(gg)
  n:=4;
  M:=RMatrixSpace(Rk,n,n)!0;
     for k:=1 to n do
       M[k]:=gg;
       temp:=gg;
       for t:=2 to n do
         temp[t-1]:=gg[t];
       end for;
       temp[n]:=gg[1];
       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

v1:=RSpace(Rk,4)![i1,i2,i3,i2];
v2:=RSpace(Rk,4)![i4,i5,i6,i5];
v3:=RSpace(Rk,4)![i4,i5,i6,i5];
v4:=RSpace(Rk,4)![i7,i8,i9,i1+i3+i7+i8+i9];
v5:=RSpace(Rk,4)![i10,i11,i12,i4+i6+i10+i11+i12];
v6:=RSpace(Rk,4)![i10,i11,i12,i4+i6+i10+i11+i12];

M1:=cycgen(v1);
M2:=cycgen(v2);
M3:=cycgen(v3);
M4:=revcycgen(v4);
M5:=revcycgen(v5);
M6:=revcycgen(v6);

CM:=BlockMatrix(6,6,
[
M1,M2,M3,M4,M5,M6,
```

```
M3,M1,M2,M6,M4,M5,
M2,M3,M1,M5,M6,M4,
M4,M5,M6,M1,M2,M3,
M6,M4,M5,M3,M1,M2,
M5,M6,M4,M2,M3,M1
]);

if CM*CM eq Mtemp1 and Rank(CM) eq 12 and MinimumWeight(LinearCode(CM)) eq 8 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;

#M;

r1:=RSpace(Rk,4)![1,0,0,0];
r2:=RSpace(Rk,4)![0,0,0,0];
r3:=RSpace(Rk,4)![0,0,0,0];
r4:=RSpace(Rk,4)![1,1,0,1];
r5:=RSpace(Rk,4)![0,1,1,0];
r6:=RSpace(Rk,4)![0,1,1,0];

T1:=cycgen(r1);
T2:=cycgen(r2);
T3:=cycgen(r3);
T4:=revcycgen(r4);
T5:=revcycgen(r5);
T6:=revcycgen(r6);

L:=BlockMatrix(6,6,
[
T1,T2,T3,T4,T5,T6,
T3,T1,T2,T6,T4,T5,
T2,T3,T1,T5,T6,T4,
T4,T5,T6,T1,T2,T3,
T6,T4,T5,T3,T1,T2,
T5,T6,T4,T2,T3,T1
]);

C:=LinearCode(L);
dm:=MinimumWeight(C);
```

```
AutomorphismGroup(C);
WeightDistribution(C);

print Cputime(t);
```

A.2 Chapter 4

Here we present the program used to construct the $[16, 8, 4]$ code in Example 4.1.2 using the group algebra $\mathbb{F}_2 C_2^3$. The results are shown in Table 4.4

```
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:=4;
  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;

function revcycgen(gg)
  n:=4;
  M:=RMatrixSpace(Rk,n,n)!0;
     for k:=1 to n do
       M[k]:=gg;
       temp:=gg;
       for t:=2 to n do
         temp[t-1]:=gg[t];
```

```
       end for;
       temp[n]:=gg[1];
       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,4)![i1,i2,i3,i4];
v2:=RSpace(Rk,4)![i5,i6,i7,i8];
v3:=RSpace(Rk,4)![i7,i8,i5,i6];

M1:=cycgen(v1);
M2:=revcycgen(v2);
M3:=revcycgen(v3);

CM:=BlockMatrix(2,2,[
M1,M2,
M3,M1]);

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 5

Here we present the program used to construct the $[80, 40, 14]$ code using the group algebra $\mathbb{F}_2 D_{38}$ shown in Table 5.5.

```
Rk:=GF(2);

codeF2:=[];
M:=[];

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;
```

```
function cycgen1(gg)
  n:=19;
  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;

Mtemp1:=RMatrixSpace(Rk,38,38)!0;
            for i:=1 to 38 do
              Mtemp1[i,i]:=1;
            end for;

ConstMat := func< n, r, c |
RMatrixSpace(Rk, r, c) ! [ n : i in [1..r*c]] >;

Mtemp0:=RMatrixSpace(Rk,40,40)!0;

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 for i22:=0 to 1 do
for i23:=0 to 1 do for i24:=0 to 1 do
for i25:=0 to 1 do for i26:=0 to 1 do

v1:=RSpace(Rk,2)![0,1];
```

```
B1:=cycgen(v1);

A1:=ConstMat(0,1,19);
A2:=ConstMat(0,1,19);

B2:=BlockMatrix(2,2,[
A1,A2,
A2,A1]);

v2:=RSpace(Rk,2)![0,0];
B3:=cycgen(v2);

A3:=ConstMat(0,1,19);
A4:=ConstMat(1,1,19);


B4:=BlockMatrix(2,2,[
A3,A4,A4,A3]);

T1:=HorizontalJoin(B1,B2);T2:=HorizontalJoin(T1,B3);T3:=HorizontalJoin(T2,B4);

v3:=RSpace(Rk,19)![0,0,0,0,0,0,i1,i2,i3,i4,i5,i6,i7,i8,i9,i10,i11,1,1];
v4:=RSpace(Rk,19)![0,0,i12,i13,i14,i15,i16,i17,i18,i19,i20,i21,i22,i23,i24,i25,i26,1,1];
v4A:=RSpace(Rk,19)![1,0,0,i12,i13,i14,i15,i16,i17,i18,i19,i20,i21,i22,i23,i24,i25,i26,1];

M3:=cycgen1(v3);
M4:=cycgen1(v4);
M4A:=cycgen1(v4A);

 B5:=BlockMatrix(2,2,
[M3,M4,
M4A,M3]);

H1:=HorizontalJoin(Transpose(B2),Mtemp1); H2:=HorizontalJoin(H1,Transpose(B4)); H3:=Horizo

CM:=VerticalJoin(T3,H3);

if CM*Transpose(CM) eq Mtemp0  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;end for;end for;end for;
end for;end for;

#M;

for i:=1 to #M do

C:=LinearCode(M[i]); dm:=MinimumWeight(C);
if (dm ge 12) and IsSelfDual(C) and not(IsDoublyEven(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;
             M[i];
             AutomorphismGroup(C);
            ddd:=PartialWeightDistribution(C,16); ddd;
             "**********************";
             end if;
  end if;
end for;
print Cputime(t);
```

A.4 Chapter 6

Here we present the program used to construct the $[32, 16, 6-8]$ codes using the the groups C_8 and C_8. These binary codes are then lifted over $\mathbb{F}_2 + u\mathbb{F}_2$ to obtain the codes in Table 6.2

```
Rk:=GF(2);
codeF2:=[];
M:=[];

Mtemp1:=RMatrixSpace(Rk,16,16)!0;
            for i:=1 to 16 do
```

```
              Mtemp1[i,i]:=1;
            end for;

Mt2:=RMatrixSpace(Rk,8,8)!0;

Mt3:=RMatrixSpace(Rk,8,8)!0;
            for i:=1 to 8 do
              Mt3[i,i]:=1;
            end for;

function cycgen(gg)
  n:=8;
  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;

function revcycgen(gg)
  n:=8;
  M:=RMatrixSpace(Rk,n,n)!0;
     for k:=1 to n do
       M[k]:=gg;
       temp:=gg;
       for t:=2 to n do
         temp[t-1]:=gg[t];
       end for;
       temp[n]:=gg[1];
       gg:=temp;
     end for;
     return M;
  end function;



ConstMat := func< n, r, c |
```

```
RMatrixSpace(Rk, r, c) ! [ n : i in [1..r*c]] >;

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 for i22:=0 to 1 do
for i23:=0 to 1 do for i24:=0 to 1 do


e1:=RSpace(Rk,8)![i1,i2,i3,i4,i5,i6,i7,i8];
E1:=cycgen(e1);

f1:=RSpace(Rk,8)![i9,i10,i11,i12,i13,i14,i15,i16];
F1:=cycgen(f1);

g1:=RSpace(Rk,8)![i17,i18,i19,i20,i21,i22,i23,i24];
G1:=revcycgen(g1);


CM:=BlockMatrix(2, 2,
[
E1,F1+G1,
F1+G1,E1
]);


if CM*Transpose(CM) eq Mtemp1 then
M:=Append(M,[E1,F1,G1]);
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;end for;end for;end for;


#M;
for i:=1 to #M do


M1:=BlockMatrix(2, 4,
[
Mt3,Mt2,M[i][1],M[i][2]+M[i][3],
Mt2,Mt3,M[i][2]+M[i][3],M[i][1]
]);

 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;
             M[i];
            AutomorphismGroup(C);
            PartialWeightDistribution(C,12);
             "**********************";
             end if;

  end if;


end for;




print Cputime(t);
```

A.5 Chapter 7

Here we present the program used to construct the $[30, 15, 6]$ codes when $p = 5$. These binary codes are then lifted over $\mathbb{F}_2 + u\mathbb{F}_2$ to obtain the codes in Table 7.1.

```
Rk:=GF(2);
codeF2:=[];
M:=[];

Mtemp1:=RMatrixSpace(Rk,15,15)!0;

function cycgen(gg)
  n:=5;
  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;

ConstMat := func< n, r, c |
RMatrixSpace(Rk, r, c) ! [ n : i in [1..r*c]] >;

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 for i22:=0 to 1 do
for i23:=0 to 1 do for i24:=0 to 1 do
```

```
b1:=RSpace(Rk,5)![i1,i2,i3,i3,i2];
B1:=cycgen(b1);

b2:=RSpace(Rk,5)![i4,i5,i6,i6,i5];
B2:=cycgen(b2);

b3:=RSpace(Rk,5)![i7,i8,i9,i9,i8];
B3:=cycgen(b3);

m1:=RSpace(Rk,5)![i10,i11,i12,i13,i14];
M1:=cycgen(m1);

m2:=RSpace(Rk,5)![i15,i16,i17,i18,i19];
M2:=cycgen(m2);

m3:=RSpace(Rk,5)![i20,i21,i22,i23,i24];
M3:=cycgen(m3);

CM:=BlockMatrix(3, 6,
[
B1,B2,B3,M1,M2,M3,
B3,B1,B2,M3,M1,M2,
B2,B3,B1,M2,M3,M1
]);

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;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);
            PartialWeightDistribution(C,12);
             "*********************";
             end if;

  end if;
end for;
print Cputime(t);
```

Bibliography

[1] D. Anev, M. Harada, and N. Yankov, *New extremal singly even self-dual codes of lengths 64 and 66*, J. Algebra Comb. Discrete Struct. Appl. **5** (2018), no. 3, 143–151.

[2] E. Assmus and H. Mattson, *On weights in quadratic-residue codes*, Discrete Math. **3** (1972), 1–20.

[3] K. Betsumiya, S. Georgiou, T. Gulliver, M. Harada, and C. Koukouvinos, *On self-dual codes over some prime fields*, Discrete Math. **262** (2003), no. 1-3, 37–58.

[4] M. Borello, *The automorphism group of a self-dual* $[72, 36, 16]$ *code is not an elementary abelian group of order 8*, Finite Fields Appl. **25** (2014), 1–7.

[5] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993).

[6] S. Bouyuklieva, *On the automorphisms of order 2 with fixed points for the extremal self-dual codes of length* $24m$, Des. Codes Cryptogr. **25** (2002), no. 1, 5–13.

[7] S. Buyuklieva, *On the binary self-dual codes with an automorphism of order* 2, Des. Codes Cryptogr. **12** (1997), no. 1, 39–48.

[8] N. Bourbaki, *Algebra. I. Chapters 1–3*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 1989. Translated from the French; Reprint of the 1974 edition.

[9] S. Bouyuklieva and I. Bouyukliev, *An algorithm for classification of binary self-dual codes*, IEEE Trans. Inform. Theory **58** (2012), no. 6, 3933–3940.

[10] S. Bouyuklieva, E. O'Brien, and W. Willems, *The automorphism group of a binary self-dual doubly even* $[72, 36, 16]$ *code is solvable*, IEEE Trans. Inform. Theory **52** (2006), no. 9, 4244–4248.

[11] A. A. Bovdi and C. Polcino Milies, *Normal subgroups of the group of units in group rings of torsion groups*, Publ. Math. Debrecen **59** (2001), no. 1-2, 235–242.

[12] V. Bovdi, *Group rings in which the group of units is hyperbolic*, J. Group Theory **15** (2012), no. 2, 227–235.

[13] S. D. Berman, *On the theory of group codes*, Cybernetics **3** (1969), no. 1, 25–31 (1969).

[14] S. D. Berman and I. I. Grushko, *Parameters of abelian codes in the group algebra* KG *of* $G = (a) \times (b)$, $a^p = b^p = 1$, *p prime, over a finite field* K *with primitive pth root of unity and related MDS-codes*, Representation theory, group rings, and coding theory, Contemp. Math., vol. 93, Amer. Math. Soc., Providence, RI, 1989, pp. 77–83.

[15] F. Bernhardt, P. Landrock, and O. Manz, *The extended Golay codes considered as ideals*, J. Combin. Theory Ser. A **55** (1990), no. 2, 235–246.

[16] G.Hamburg Călugăreanu P., *Semisimple Rings*, Springer Netherlands, 1998.

[17] C. L. Chen, W. W. Peterson, and E. J. Weldon Jr., *Some results on quasi-cyclic codes*, Information and Control **15** (1969), 407–423.

[18] N. Chigira, M. Harada, and M. Kitazume, *Extremal self-dual codes of length 64 through neighbors and covering radii*, Des. Codes Cryptogr. **42** (2007), no. 1, 93–101.

[19] G. H. Cliff, S. K. Sehgal, and A. R. Weiss, *Units of integral group rings of metabelian groups*, J. Algebra **73** (1981), no. 1, 167–185.

[20] J. H. Conway and N. J. A. Sloane, *A new upper bound on the minimal distance of self-dual codes*, IEEE Trans. Inform. Theory **36** (1990), no. 6, 1319–1333.

[21] Leo Creedon and Joe Gildea, *The structure of the unit group of the group algebra* $\mathbb{F}_{3^k}D_6$, Int. J. Pure Appl. Math. **45** (2008), no. 2, 315–320. MR2421868

[22] P. Davis, *Circulant matrices*, John Wiley & Sons, New York-Chichester-Brisbane, 1979. A Wiley-Interscience Publication; Pure and Applied Mathematics.

[23] G. Dorfer and H. Maharaj, *Generalized AG codes and generalized duality*, Finite Fields Appl. **9** (2003), no. 2, 194–210.

[24] S. Dougherty, *Algebraic coding theory over finite commutative rings*, SpringerBriefs in Mathematics, Springer, Cham, 2017.

[25] S. Dougherty, P. Gaborit, M. Harada, and P. Solé, *Type II codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory **45** (1999), no. 1, 32–45.

[26] S. Dougherty, J. Gildea, R. Taylor, and A. Tylyshchak, *Group rings, G-codes and constructions of self-dual and formally self-dual codes*, Des. Codes Cryptogr. **86** (2018), no. 9, 2115–2138.

[27] S. Dougherty, J. Gildea, A. Korban, A. Kaya, A. Tylyshchak, and Bahattin Yildiz, *Bordered constructions of self-dual codes from group rings and new extremal binary self-dual codes*, Finite Fields Appl. **57** (2019), 108–127.

[28] S. Dougherty, T. Gulliver, and M. Harada, *Extremal binary self-dual codes*, IEEE Trans. Inform. Theory **43** (1997), no. 6, 2036–2047.

[29] S. Dougherty, J. L. Kim, H. Kulosman, and H. Liu, *Self-dual codes over commutative Frobenius rings*, Finite Fields Appl. **16** (2010), no. 1, 14–26, DOI 10.1016/j.ffa.2009.11.004. MR2588123

[30] S. Dougherty, B. Yıldız, and S. Karadeniz, *Self-dual codes over* R_k *and binary self-dual codes*, Eur. J. Pure Appl. Math. **6** (2013), no. 1, 89–106.

[31] S. Dougherty, B. Yildiz, and S. Karadeniz, *Codes over* R_k*, Gray maps and their binary images*, Finite Fields Appl. **17** (2011), no. 3, 205–219.

[32] S. Dougherty, S. Karadeniz, and B. Yildiz, *Cyclic codes over* R_k, Des. Codes Cryptogr. **63** (2012), no. 1, 113–126.

[33] P. Gaborit, *Quadratic double circulant codes over fields*, J. Combin. Theory Ser. A **97** (2002), no. 1, 85–107.

[34] P. Gaborit, V. Pless, P. Solé, and O. Atkin, *Type II codes over* $\mathbb{F}_4$, Finite Fields Appl. **8** (2002), no. 2, 171–183.

[35] S. Georgiou and E. Lappas, *Self-dual codes from circulant matrices*, Des. Codes Cryptogr. **64** (2012), no. 1-2, 129–141.

[36] J. Gildea, *The structure of the unit group of the group algebra* $\mathbb{F}_{3^K}(C_3 \times D_6)$, Comm. Algebra **38** (2010), no. 9, 3311–3317.

[37] J. Gildea, H. Hamilton, A. Kaya, and B. Yildiz, *Modified quadratic residue constructions and new extremal binary self-dual codes of lengths 64, 66 and 68*, Inform. Process. Lett. **157** (2020), 105927.

[38] M. Gürel and N. Yankov, *Self-dual codes with an automorphism of order 17*, Math. Commun. **21** (2016), no. 1, 97–107.

[39] J. Gildea, A. Kaya, A. Korban, and B. Yildiz, *Constructing Self-Dual Codes from Group Rings and Reverse Circulant Matrices*, to appear in Adv. Math. Commun.

[40] J. Gildea, A. Kaya, A. Korban, and B. Yildiz, *New Extremal binary self-dual codes of length 68 from a novel approach to neighbors* **https://arxiv.org/abs/2002.10030**.

[41] J. Gildea, A. Kaya, R. Taylor, and A. Tylyshchak, *New Self-dual Codes from 2×2 block circulant matrices, Group Rings and Neighbours of Neighbours, submitted* **https://arxiv.org/abs/2002.09789**.

[42] J. Gildea, A. Kaya, R. Taylor, A. Tylyshchak, and B. Yildiz, *New Extremal Binary Self-dual Codes from block circulant matrices and block quadratic residue circulant matrices* **https://arxiv.org/abs/2003.05296**.

[43] J. Gildea, A. Kaya, and B. Yildiz, *New binary self-dual codes via a generalization of the four circulant construction*, to appear in Math. Commun.

[44] Joe Gildea, Abidin Kaya, Rhian Taylor, and Bahattin Yildiz, *Constructions for self-dual codes induced from group rings*, Finite Fields Appl. **51** (2018), 71–92.

[45] J. Gildea and F. Monaghan, *Units of some group algebras of groups of order 12 over any finite field of characteristic 3*, Algebra Discrete Math. **11** (2011), no. 1, 46–58.

[46] J. Gildea and R. Taylor, *Units of the group algebra of the group $C_n \times D_6$ over any finite field of characteristic 3*, Int. Electron. J. Algebra **24** (2018), 62–67, DOI 10.24330/ieja.440205. MR3828096

[47] J. Gildea, R. Taylor, A. Kaya, and A. Tylyshchak, *Double bordered constructions of self-dual codes from group rings over Frobenius rings.*, Cryptogr. Commun., posted on 2020, 1, DOI https://doi.org/10.1007/s12095-019-00420-3.

[48] T. Gulliver and M. Harada, *Weight enumerators of double circulant codes and new extremal self-dual codes*, Des. Codes Cryptogr. **11** (1997), no. 2, 141–150.

[49] T. Gulliver and M. Harada, *Classification of extremal double circulant formally self-dual even codes*, Des. Codes Cryptogr. **11** (1997), no. 1, 25–35.

[50] T. Gulliver, M. Harada, and J. L. Kim, *Construction of new extremal self-dual codes*, Discrete Math. **263** (2003), no. 1-3, 81–91.

[51] T. Gulliver, M. Harada, and H. Miyabayashi, *Double circulant and quasi-twisted self-dual codes over $\mathbb{F}_5$ and $\mathbb{F}_7$*, Adv. Math. Commun. **1** (2007), no. 2, 223–238.

[52] T. Gulliver and M. Harada, *On double circulant doubly even self-dual $[72, 36, 12]$ codes and their neighbors*, Australas. J. Combin. **40** (2008), 137–144.

[53] T. Gulliver and M. Harada, *On the performance of optimal double circulant even codes*, Adv. Math. Commun. **11** (2017), no. 4, 767–775.

[54] T. Gulliver and M. Harada, *Classification of extremal double circulant self-dual codes of lengths 74–88*, Discrete Math. **306** (2006), no. 17, 2064–2072.

[55] S. Han, J. L. Kim, H. Lee, and Y. Lee, *Construction of quasi-cyclic self-dual codes*, Finite Fields Appl. **18** (2012), no. 3, 613–633.

[56] M. Harada and A. Munemasa, *Some restrictions on weight enumerators of singly even self-dual codes*, IEEE Trans. Inform. Theory **52** (2006), no. 3, 1266–1269.

[57] M. Harada, *Binary extremal self-dual codes of length 60 and related codes*, Des. Codes Cryptogr. **86** (2018), no. 5, 1085–1094.

[58] G. Higman, *The units of group-rings*, Proc. London Math. Soc. (2) **46** (1940), 231–248.

[59] W. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003.

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

[61] T. Hurley, *Self-dual, dual-containing and related quantum codes from group rings*, arXiv:0711.3983 (2007).

[62] B Hurley and T Hurley, *Systems of MDS codes from units and idempotents*, Discrete Math. **335** (2014), 81–91.

[63] Paul Hurley and Ted Hurley, *LDPC and convolutional codes from matrix and group rings*, Selected topics in information and coding theory, Ser. Coding Theory Cryptol., vol. 7, World Sci. Publ., Hackensack, NJ, 2010, pp. 195–237.

[64] V. Ĭorgov and N. Zyapkov, *Doubly even self-dual* $[40, 20, 8]$*-codes with an automorphism of odd order*, Problemy Peredachi Informatsii **32** (1996), no. 3, 41–46 (Russian, with Russian summary); English transl., Problems Inform. Transmission **32** (1996), no. 3, 253–257 (1997).

[65] V. Ĭorgov, *Binary self-dual codes with automorphisms of odd order*, Problemy Peredachi Informatsii **19** (1983), no. 4, 11–24 (Russian); English transl., Problems Inform. Transmission **19** (1983), no. 4, 260–270 (1984).

[66] G. Janssens, E. Jespers, and D. Temmerman, *Free products in the unit group of the integral group ring of a finite group*, Proc. Amer. Math. Soc. **145** (2017), no. 7, 2771–2783.

[67] S. Karadeniz and B. Yildiz, *Double-circulant and bordered-double-circulant constructions for self-dual codes over* R_2, Adv. Math. Commun. **6** (2012), no. 2, 193–202.

[68] S. Karadeniz and B. Yildiz, *New extremal binary self-dual codes of length 66 as extensions of self-dual codes over* R_k, J. Franklin Inst. **350** (2013), no. 8, 1963–1973.

[69] A. Kaya, *New extremal binary self-dual codes of lengths 64 and 66 from* R_2*-lifts*, Finite Fields Appl. **46** (2017), 271–279.

[70] S. Karadeniz, B. Yildiz, and N. Aydin, *Extremal binary self-dual codes of lengths 64 and 66 from four-circulant constructions over* $\mathbb{F}_2 + u\mathbb{F}_2$, Filomat **28** (2014), no. 5, 937–945.

[71] A. Kaya, *New extremal binary self-dual codes of lengths 64 and 66 from* R_2*-lifts*, Finite Fields Appl. **46** (2017), 271–279.

[72] A. Kaya, *New extremal binary self-dual codes of length 68 via the short Kharaghani array over* $\mathbb{F}_2 + u\mathbb{F}_2$, Math. Commun. **22** (2017), no. 1, 121–131.

[73] A. Kaya, B. Yildiz, and A. Pasa, *New extremal binary self-dual codes from a modified four circulant construction*, Discrete Math. **339** (2016), no. 3, 1086–1094.

[74] S. Karadeniz and B. Yildiz, *New extremal binary self-dual codes of length 64 from* R_3*-lifts of the extended binary Hamming code*, Des. Codes Cryptogr. **74** (2015), no. 3, 673–680.

[75] A. Kaya, B. Yildiz, and I. Siap, *New extremal binary self-dual codes of length 68 from quadratic residue codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$, Finite Fields Appl. **29** (2014), 160–177.

[76] M. Karlin, *New binary coding results by circulants*, IEEE Trans. Inform. Theory **IT-15** (1969), 81–92.

[77] M. Karlin and F. MacWilliams, *On finding low weight vectors in quadratic residue codes for* $p = 8m - 1$, SIAM J. Appl. Math. **25** (1973), 95–104.

[78] K. Kaur and M. Khan, *Units in* F_2D_{2p}, J. Algebra Appl. **13** (2014), no. 2, 1350090, 9.

[79] K. Kaur and M. Khan, *Units in modular group algebra*, Comm. Algebra **45** (2017), no. 3, 971–976.

[80] A. V. Kelarev and P. Solé, *Error-correcting codes as ideals in group rings*, Abelian groups, rings and modules (Perth, 2000), Contemp. Math., vol. 273, Amer. Math. Soc., Providence, RI, 2001, pp. 11–18.

[81] M. Khan, R. K. Sharma, and J. B. Srivastava, *The unit group of* FS_4, Acta Math. Hungar. **118** (2008), no. 1-2, 105–113.

[82] S. Ling and P. Solé, *Type II codes over* $\mathbb{F}_4 + u\mathbb{F}_4$, European J. Combin. **22** (2001), no. 7, 983–997.

[83] M. Koroglu, *Systems of MDS codes from units and idempotents*, Sakarya University Journal of Science **23 (3)** (2019), 486–492.

[84] Ian McLoughlin and Ted Hurley, *A group ring construction of the extended binary Golay code*, IEEE Trans. Inform. Theory **54** (2008), no. 9, 4381–4383.

[85] Ian McLoughlin, *A group ring construction of the [48,24,12] type II linear block code*, Des. Codes Cryptogr. **63** (2012), no. 1, 29–41.

[86] Gabriele Nebe, *An extremal* $[72, 36, 16]$ *binary code has no automorphism group containing* $Z_2 \times Z_4$*,* Q_8*, or* Z_{10}, Finite Fields Appl. **18** (2012), no. 3, 563–566.

[87] E. O'Brien and W. Willems, *On the automorphism group of a binary self-dual doubly even* $[72, 36, 16]$ *code*, IEEE Trans. Inform. Theory **57** (2011), no. 7, 4445–4451.

[88] D. S. Passman and P. F. Smith, *Units in integral group rings*, J. Algebra **69** (1981), no. 1, 213–239.

[89] D.S. Passman, *The algebraic structure of group rings*, Pure and Applied Mathematics, Wiley-Interscience [John Wiley & Sons], New York-London-Sydney, 1977.

[90] C. Polcino Milies and S. K. Sehgal, *An introduction to group rings*, Algebras and Applications, vol. 1, Kluwer Academic Publishers, Dordrecht, 2002.

[91] Eric M. Rains, *Shadow bounds for self-dual codes*, IEEE Trans. Inform. Theory **44** (1998), no. 1, 134–139.

[92] R. Sandling, *Units in the modular group algebra of a finite abelian p-group*, J. Pure Appl. Algebra **33** (1984), no. 3, 337–346.

[93] ———, *Presentations for Unit Groups of Modular Group Algebras of Groups of Order 16*, Mathematics of Computation **59** (1992), no. 200, 689–701.

[94] R. K. Sharma, J. B. Srivastava, and M. Khan, *The unit group of FS_3*, Acta Math. Acad. Paedagog. Nyházi. (N.S.) **23** (2007), no. 2, 129–142.

[95] R. K. Sharma, J. B. Srivastava, and M. Khan, *The unit group of FA_4*, Publ. Math. Debrecen **71** (2007), no. 1-2, 21–26.

[96] M. Shi, A. Alahmadi, and P. Solé, *Codes and rings*, Pure and Applied Mathematics (Amsterdam), Academic Press, London, 2017. Theory and practice; With a foreword by S. K. Jain. MR3791823

[97] *The GAP Group: GAP - Groups, Algorithms and Programming*, Version 4.11.0.

[98] H. Ward, *Quadratic residue codes and symplectic groups*, J. Algebra **29** (1974), 150–171.

[99] N. Yankov, *A putative doubly even* $[72, 36, 16]$ *code does not have an automorphism of order 9*, IEEE Trans. Inform. Theory **58** (2012), no. 1, 159–163.

[100] N. Yankov and D. Anev, *On the self-dual codes with an automorphism of order 5*, Appl. Algebra Engrg. Comm. Comput. **https://doi.org/10.1007/s00200-019-00403-0** (2019).

[101] N. Yankov, D. Anev, and Müberra Gürel, *Self-dual codes with an automorphism of order 13*, Adv. Math. Commun. **11** (2017), no. 3, 635–645.

[102] N. Yankov, M. Ivanova, and M.H. Lee, *Self-dual codes with an automorphism of order 7 and s-extremal codes of length 68*, Finite Fields Appl. **51** (2018), 17–30.

[103] N. Yankov, R. Russeva, and E. Karatash, *Classification of binary self-dual* $[76, 38, 14]$ *codes with an automorphism of order 9*, IEEE Trans. Inform. Theory **65** (2019), no. 2, 1101–1105.