Dihedral Codes

by Ian Mc Loughlin

June 2009

A Ph.D. thesis submitted to the
School of Mathematics, Statistics and Applied Mathematics,
National University of Ireland, Galway
under the supervision of
Professor Ted Hurley.

The research contained within was supported by The Irish Research Council for Science, Engineering and Technology under the National Development Plan.

Contents

Abstract

In this thesis we give new constructions of a number of extremal type II codes. Algebraic proofs are provided that the constructions do in fact yield the codes. The codes are constructed using group rings of which the underlying groups are dihedral. Type II codes are not cyclic, but the constructions here are similar to the constructions of cyclic codes from polynomials.

The first code we construct—the extended binary Golay code—is discussed in chapter 2. It is constructed from a zero divisor in the group ring of the finite field with two elements and the dihedral group with twenty-four elements. We create a generator matrix of the code that is in standard form and is a reverse circulant generator matrix. The generator matrix generates the code as quasi cyclic of index two.

Algebraic proofs are given of the code's minimum distance, self-duality and doubly evenness. A list of twenty-three other zero divisors that we have found to generate the code is given. Trivial changes adapt the aforementioned algebraic proofs to any of these zero divisors. We also prove that the twenty-four zero divisors are the only ones of their form that will generate the code.

In chapter 3 we construct the $(48, 24, 12)$ extremal type II code as a dihedral code. The new construction is similar to that of the extended Golay code. Again, proofs of the self-duality and doubly evenness are given. An algebraic proof of the minimum distance is achieved through the use of two different group ring matrices.

A number of different codes are constructed in chapter 4, building on the constructions in previous chapters. Towards the end of the chapter we list some zero divisors that generate type II codes of lengths seventy-two and ninety-six. According to investigations by computer, these codes have minimum distances of twelve and sixteen respectively. No type II codes of each of these lengths are known that have greater respective minimum distances. Some techniques are detailed that vastly reduce the calculations involved in their analysis.

The constructions of the $(72, 36, 12)$ and $(96, 48, 16)$ codes are facilitated at the start of chapter 4 by the construction of extremal type II codes of all lengths a multiple of eight up to length forty. Type II codes only exist at lengths that are multiples of eight. Overall we have shown that extremal type II codes can be constructed in dihedral group rings at every length a multiple of eight up to and including length forty-eight, and at some lengths beyond forty-eight. We also successfully investigate the possibility to construct some type I codes in the same way. □

Thanks

Family

My foremost thanks go to Mum and Dad for their enormous financial and emotional support. Thanks also to my sisters Lisa and Susan for their encouragement, albeit mostly through some form of reverse psychology. My brother from another mother, John deserves much credit for helping to keep me sane, fed and caffeinated during the daytime. Also there's an understanding, wise and stump-wagging family bundle of joy named Shep whose endless barking and occasional stray dog hair on my otherwise ho-hum laptop screen brightened many days.

Ted

As is true of all supervisors, without Ted's help this thesis would never have come to fruition. Not so true of all supervisors is that Ted has always been patient, insightful and helpful. I greatly appreciate your assistance Ted, in getting me so much closer to my future goals.

The School

Thanks to my fellow Ph.D. students in the School of Mathematics, Statistics and Applied Mathematics for the coffee breaks and the laughs. I'm grateful to many of the lecturers for listening and offering ideas, especially Jerome and Claas. Thanks also to Niall for helping a poor defenseless outsider through his undergraduate years.

Friends and More Family

I'm so grateful to Granny K. and Paula for always asking how I was getting on. Finally, thanks to all my friends, lads and ladies—there are too many to list here.

Chapter 1

Introduction

Algebra has played an important role in the study and construction of error correcting codes to date. In this chapter we give some background information concerning this role. Throughout the chapter the algebraic structures relevant to the study are defined. The goal is to facilitate the discussion of codes in subsequent chapters. First we outline here the course that this discussion will take.

All of the codes in this thesis will be constructed using group rings. Ted and Paul Hurley published new methods for constructing codes using group rings in 2007 and 2009 [12, 13]. Different methods are given for two types of group ring elements: zero divisors and units. We use those methods pertaining to zero divisors in this thesis.

The focus of earlier efforts to construct codes in group rings was on ideals [8, p. 829],[11]. All of the codes in this thesis will be ideals in their respective group rings. It should be noted however that in Hurley and Hurley's paper the construction techniques are not limited to ideals. Codes are defined more generally in terms of modules. They are ideals only under the conditions given there.

The first two codes dealt with in this thesis are the extended binary Golay code and the $(48, 24, 12)$ type II code. Both of these have been constructed previously. It has been known that the extended binary Golay code can be constructed as an ideal in a group algebra since 1990 [1]. There the code is constructed as an ideal in a group ring over the symmetric group of order twenty-four. Earlier the construction of the extended binary Golay code was detailed by Florence MacWilliams in her book with Neil Sloane, first published in 1977 [18, p. 634]. In that book a generator matrix for the code is given that is doubly circulant [18, p. 498]. Later in this thesis we will see that the new constructions yield reverse circulant generator matrices.

Doubly circulant codes have received a good deal of coverage in the literature. Richard Jenson publised results in 1980 regarding the construction of quadratic residue codes by doubly circulant generator matrices [15]. He found the construction of such codes to be not always be possible using his methods. Mona Musa published results in 2008 proving that certain extended quadratic residue codes could be constructed from double circulant matrices [21]. T. Aaron Gulliver gave a classification of the double circulant self-dual codes of small lengths in a paper in 1998 [5]. Vera Pless in the Handbook of Coding Theory states that some quasi-cyclic codes are equivalent to double circulant codes [8, p. 60]. Those given in this thesis are quasi-cyclic of index two. Quasi-cyclic codes have received much attention in the literature right up to the present. The emphasis has been on quasi-cyclic low-density parity check codes.

While the codes given in this thesis are not necessarily low-density parity check codes they admit to another composition of interest. They are binary codes that are both self-dual and doubly even. Such codes are termed type II codes [8, p. 96]. The extended binary Golay and Type II $(48, 24, 12)$ codes constructed in this thesis are both *extremal* type II codes. A type II code is called extremal if its minimum distance is $4\lfloor n/24 \rfloor + 4$ where n is the code's length [8, p. 270]. Type II codes are never cyclic [23] and thus can not be constructed as polynomial codes. The constructions given here though, for the type II codes, are very similar to the construction of cyclic codes from polynomials.

There have been numerous calls for further investigation into the existence of longer extremal type II codes. Special interest is given to those of length a multiple of twenty-four as out of all extremal type II codes they achieve the greatest minimum distance compared to their lengths. Their existence has been neither proved nor disproved for lengths as small as seventy-two and ninety-six [16].

We begin now by discussing some of the fundamental concepts on which the rest of the thesis is based. We begin with the definitions pertaining to the subject generally referred to as *abstract algebra*. We are then able to move on to those in the realm of coding theory.

1.1 Groups, Rings and Fields

We assume that the reader is familiar with the definitions of the terms 'group' and 'ring' from abstract algebra. These are defined in any standard textbook on the subject, such as Birkhoff and MacLane's book "Algebra" [17, p. 43]. It is also assumed that the reader is generally acquainted with the basic concepts associated with groups and rings.

Within group theory we will be discussing subgroups, the order of a group, the

order of a group element, commutative and non-commutative groups. We expect the reader knows what a cyclic group is, though other groups that are discussed in the thesis are defined. We use the standard notation $G = \langle \text{generators} \mid \text{relations} \rangle$ to define and denote a group G where 'generators' is a list of generators of the group and 'relations' is a list of combinations of the generators that are equal to the identity of the group. Only finite groups will be discussed.

In the realm of ring theory we also expect that the reader is familiar with the common definitions appropriate to the subject. These are the ideas of multiplicative identities, units, ring commutivity, fields, finite fields, ideals and principal ideals. The smallest field, the finite field with two elements, is denoted in this text by $\mathbb{Z}_2$.

There is one peculiar property a non-zero element in a ring may have that the reader may not be familiar with. A non-zero ring element may multiply with another non-zero ring element to produce zero. These elements are called *zero divisors* and we will use them extensively throughout this text.

We will now move on and define some of the concepts in the subject of *linear algebra*. While the reader is likely knowledgeable of these ideas, the way they are developed here facilitates lesser known definitions later in the chapter. The main structure we want to define is that of a vector space.

1.2 Vector Spaces and Modules

We now define the term 'module' which aids in our later definition of the term 'vector space'. Let $R(+, \times)$ be a ring and let $G(\circ)$ be a commutative group. The group G is called a *left R-module* [17, p.] under an operation $\cdot : R \times G \to G$ when the following axioms are satisfied:

1. For every pair of elements r_1 and r_2 in R and every element g in G: $(r_1 + r_2) \cdot g = (r_1 \cdot g) + (r_2 \cdot g)$.
2. For every pair of elements g_1 and g_2 in G and every element r in R: $r \cdot (g_1 \circ g_2) = (r \cdot g_1) \circ (r \cdot g_2)$.
3. For every pair of elements r_1 and r_2 in R and every element g in G: $(r_1 \times r_2) \cdot g = r_1 \cdot (r_2 \cdot g)$.
4. For every g in G and the multiplicative identity 1 in R: $1 \cdot g = g$.

A module is called a *right R-module* if it satisfies the same axioms except with an operation $\cdot : G \times R \to G$ with the relevant changes to the order of the group and ring elements in the four axioms.

A *vector space* is defined as a module over a field [17, p. 193]. We will later define codes in terms of vector spaces. They will be defined as subspaces of

vector spaces. Subspaces are special subsets of vector spaces and we define them now in the next section.

1.2.1 Subspaces, Basis and Dimension

A *subspace* of a vector space is a submodule of it [20, p. 78]. A non-empty subset W of an R-module is called an R-submodule [20, p. 78], or simply a submodule, when the following two axioms are satisfied:

1. For every pair of subset elements w_1 and w_2 in W: $w_1 + w_2$ is in W.
2. For every ring element r in R and every w in W: $r \times w$ is in W.

Subspaces are not the only interesting subsets of vector spaces. A *basis* (plural: *bases*) of a vector space V is a subset of vectors in V that is linearly independent and spans the vector space. One thing that every basis of a given (finitely generated) vector space has in common is that they all have the same number of elements in them. This number of elements is called the *dimension* of the vector space.

Now that we have discussed some basic algebra we are in a position to discuss linear block codes. The rest of this chapter and indeed the rest of this thesis will be dedicated to their study.

1.3 Linear Block Codes

In this text the only codes we will concern ourselves with are linear block codes. We will simply refer to them as codes. An (n, k) linear block code is a k-dimensional subspace of the vector space $\mathbb{F}^n$ of all n-tuples of and over a finite field $\mathbb{F}$ [10, p. 3]. We denote such a subspace by $\mathcal{C}$ and refer to its elements as *codewords*. The term 'block' refers to the fact that each codeword has the same number of components. The word 'linear' refers to the fact that the code is closed under the operation of taking linear combinations of codewords over the field $\mathbb{F}$. This is a consequence of the code being a subspace. The positive integer n is called the *length* of the code and the positive integer k is called the *dimension* of the code.

Throughout this text we will use the field $\mathbb{F} = \mathbb{F}_2 = \mathbb{Z}_2$, the finite field with two elements. A code whose underlying field is $\mathbb{Z}_2$ is called a *binary code*. The usual way to denote a typical element of $\mathbb{F}^n$ is $(a_1, a_2, \ldots, a_n)$ where a_i is an element of $\mathbb{F}$ for all i and $\mathbb{F}$ is an arbitrary field. When using $\mathbb{Z}_2$ it is more common to omit the brackets and comma separators and to simply write $a_1 a_2 \ldots a_n$. In either notation the elements a_i are referred to as *components* of the codeword. The vector $a_1 a_2 \ldots a_n$ should not be confused with the similarly denoted binary

number of many bits; addition in the code is always done component-wise and there is no carrying. It is quite common to also talk of the components of a code (as opposed to those of a codeword) and denote them using the same symbols. A component of a code is the placeholder in which the components of the codewords lie.

An example of a code is the span of the basis $S = \{1000111, 0100011, 0010101, 0001110\}$ in $\mathbb{Z}_2^7$. It is a code of length seven since each codeword has seven components. There are four elements in its basis and so the dimension of the subspace, and hence the code, is four. Therefore the subspace is a $(7, 4)$ linear block code. It is in fact a well known code known as the Hamming $(7, 4)$ linear block code. This code is interesting because it has the best minimum distance for a binary code of its length and dimension. Minimum distance is a term defined in the next section.

1.3.1 Minimum Distance

The term minimum distance generally refers to a code's minimum Hamming distance. The *Hamming distance* between two codewords in a code is the number of components in which the two differ. We will refer to this as simply the *distance* between two codewords. For example the distance between the codewords 1000111 and 0100011 is three since they differ only in the first, second and fifth components.

The minimum of all of the distances between the distinct codewords of a code is called the *minimum distance* of the code. It is an extremely important parameter of a linear block code, as it is the one that determines the error-correcting capability of the code [10, p. 8]. The minimum distance of a code is notoriously difficult to calculate in general for large codes. This is unfortunate as much of coding theory is concerned with finding codes of large minimum distance for given values of n and k. After determination of its minimum distance d an (n, k) linear block code is called an (n, k, d) linear block code.

Closely related to the concept of distance is that of weight. The *weight* of a codeword is the number of non-zero components it has. For a linear block code the minimum of the weights of all of the non-zero codewords is equal to its minimum distance [10, p. 8]. In general for both binary and non-binary linear block codes the distance between two codewords c_1 and c_2 is equal to the weight of the codeword $c_1 - c_2$. In a binary code the distance is simply equal to the weight of the codeword $c_1 + c_2$ since component-wise addition and subtraction are equivalent.

The fact that the minimum distance equals the weight of one of the codewords reduces the complexity of calculating the minimum distance of a linear block

code. This has helped make linear block codes one of the most studied types of code. Furthermore the ability for linear block codes to be succinctly described by matrices has aided their prevalence. In the next section we look at linear block codes in terms of matrices.

1.3.2 Generator Matrices

The most common way to describe a code is by its generator matrix. A *generator matrix* of an (n, k) linear block code is a k by n matrix whose rows are codewords that form a basis for the code over the scalar field $\mathbb{F}$ of the vector space. We can generate all of the codewords of a code by taking all of the combinations of the generator matrix rows. There may be many generator matrices for the same code but the most common forms of generator matrix are the ones in which the k by k identity matrix appears in the very left hand side. Such a generator matrix is said to be in *standard form*. An example of a standard form generator matrix for the Hamming $(7, 4, 3)$ code is given in figure 1.1. This is simply the

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Fig. 1.1 — A Hamming $(7, 4, 3)$ code generator matrix.

basis vectors given in section 1.3 for the code placed as the rows of a matrix.

In coding theory we are interested in the null space of a generator matrix. The null space of a generator matrix has a special name. It's called the dual code of the code. It is discussed in the next section.

1.4 Dual Codes

The *dual code* of a linear block code $\mathcal{C}$ in $\mathbb{F}^n$ is the set of vectors in $\mathbb{F}^n$ that are orthogonal to all of the codewords in $\mathcal{C}$ [18, p. 26]. Two vectors in $\mathbb{F}^n$ are said to be *orthogonal* if and only if their dot product is zero. The *dot product* of two vectors $\underline{x}$ and $\underline{y}$ in $\mathbb{F}^n$ denoted as $\underline{x} \cdot \underline{y}$ is the scalar:

$$\underline{x} \cdot \underline{y} = \sum_{i=1}^{n} x_i y_i$$

where x_i is the i^{th} component of $\underline{x}$ and y_i that of $\underline{y}$. The dual code of a code is therefore the null space of any generator matrix of the code.

A code's dual code is closely related to its check matrix. A *check matrix* for a linear block code $\mathcal{C}$ of length n and dimension k over a field $\mathbb{F}$ is an $(n-k)$ by n matrix H such that $\mathcal{C} = \{\underline{x} \in \mathbb{F}^n \mid H\underline{x}^{\mathrm{T}}\} = \underline{0}$ whose rank is equal to $n-k$. The rows of H generate the null space of any generator matrix of a code and its rank is $n-k$.

Interestingly the dual code of a code can contain the code itself. Such codes are called *self-orthogonal* codes [10, p. 6]. If the dual is exactly the code itself then the code is called *self-dual* [10, p. 6]. Codes that are self-dual are of even length and their dimension is half that length [10, p. 6]. Their generator matrix serves also as their check matrix. The codes we construct in later chapters will all be self-dual.

Now that we have discussed how codes are usually defined we move on to discussing when two codes are considered to be the same.

1.5 Equivalent Codes

Two linear block codes are said to be *equivalent* if they differ only in the order of their components [18, p. 24]. In other words there is some permutation of components that maps one of the codes to the other. Equivalent codes have the same length, dimension and minimum distance [10, p. 20]. They are generally regarded as being the same code, though they do not necessarily contain the same codewords. Of course permuting the components of the code can be achieved by permuting the columns of its generator matrix. Hence two codes generated by two matrices that are merely column permutations of each other are equivalent, though codes can still be equivalent if their given generator matrices are not column permutations of each other. Interestingly some permutations of code components leave the code exactly the same. These permutations are discussed in the next section.

1.5.1 Automorphism Groups

The set of all possible permutations of a code's components forms a group under the usual operation of permutation composition. This group is called the symmetric group on n points denoted S_n. The elements of this group that preserve the codewords contained in the code are of particular interest. Together they form a subgroup. This subgroup is called the *permutation automorphism group* or simply the *automorphism group* of the code [10, p. 22]. The elements of the automorphism group are called automorphisms of the code. Thus an

automorphism is not just a permutation of the components of the code but a component permutation that preserves which vectors are codewords.

While all of the properties of a code are preserved by an automorphism, many properties are not preserved by general equivalence of codes. An important property that is not preserved is the cyclic property which is discussed in the following section.

1.6 Cyclic Codes

A *cyclic code* is a linear block code for which every cyclic shift of a codeword is also a codeword. The j^{th} *cyclic shift* of a codeword of length n is the word obtained by replacing each i^{th} component of the codeword with its $(i+j)^{\text{th}}$ component modulo n for j an integer. Thus the first cyclic shift of the codeword 0001110 is 0000111, and the second is 1000011. The Hamming $(7, 4, 3)$ code as generated by the matrix in figure 1.1 is not a cyclic code. An equivalent code generated by the matrix in figure 1.2 is cyclic.

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Fig. 1.2 — A Hamming $(7, 4, 3)$ cyclic-code generator matrix.

A generalisation of the cyclic property of a code is the quasi cyclic property. A *quasi-l cyclic code*, for l a positive integer, is a code for which the l^{th} cyclic shift of a codeword is also a codeword, and l is the least such integer. Obviously l divides the length of a quasi-l cyclic code. Sometimes we say a quasi-l cyclic code is a quasi cyclic code of *index* n/l.

Both cyclic and quasi-cyclic codes have received much attention in the literature. We will now focus on the former, highlighting their fruitful algebraic structure. They are precisely the ideals of certain rings discussed in the following two sections.

1.6.1 Polynomial Rings

Cyclic codes are ideals in certain residue class rings of polynomial rings. We now explain what this means. The *polynomial ring* $\mathbb{F}[x]$ of the indeterminate x over the field $\mathbb{F}(+, \times)$ is the set of all elements of the form $\sum_i a_i x^i$ where a_i is an element of $\mathbb{F}$, x^i is the i^{th} power of x and where all but a finite number of

the a_i are non-zero. The elements of a polynomial ring are called polynomials. The field element a_i is called the coefficient of the i^{th} power of x, x^i. Together the coefficient and the power of x, $a_i x^i$ are called a term of the polynomial. The *degree* of a non-zero polynomial $g(x)$ is the exponent of the highest power of x with non-zero coefficient and we denote it as $\deg(g(x))$ or simply $\deg(g)$

We extend the addition and multiplication of $\mathbb{F}(+,\times)$ to the polynomial ring in following ways:

$$\textbf{Addition:} \qquad \sum_i a_i x^i + \sum_i b_i x^i = \sum_i (a_i + b_i) x^i$$

$$\textbf{Multiplication:} \qquad \sum_i a_i x^i \times \sum_i b_j x^j = \sum_{i,j} (a_i \times b_j) x^{i+j}$$

where a_i, b_i and b_j are elements of $\mathbb{F}$. Under these two operations the polynomial ring, as its name suggests, is a ring [17, p. 109]. As an example of a polynomial in a polynomial ring we can take the element $g(x) = 1 + x + x^3$ in the ring $\mathbb{Z}_2[x]$. This polynomial is of degree three as the highest power of x with non-zero coefficient is three. Now that we have defined the term 'polynomial ring' we can explain what we mean by a residue class ring.

1.6.2 Residue Class Rings

Let us now define a new kind of ring, one that is useful and interesting with respect to cyclic codes. We start with a polynomial ring $\mathbb{F}[x]$ over a field $\mathbb{F}$. We then form the set of *residue classes* $\mathbb{F}[x]/\langle x^n - 1\rangle = \{q + \langle x^n - 1\rangle | q \in \mathbb{F}[x]\}$, for some positive integer n, where $\langle x^n - 1\rangle$ denotes the principal ideal generated by $x^n - 1$ in $\mathbb{F}[x]$. This set forms a ring under the operations $(q_1 + \langle x^n - 1\rangle) + (q_2 + \langle x^n - 1\rangle) = (q_1 + q_2) + \langle x^n - 1\rangle$ for addition and $(q_1 + \langle x^n - 1\rangle) \times (q_2 + \langle x^n - 1\rangle) = (q_1 \times q_2) + \langle x^n - 1\rangle$ for multiplication [17, p. 96][1]. This new ring is called the *residue class ring* of the polynomial ring $\mathbb{F}[x]$ and the principal ideal $\langle x^n - 1\rangle$.

A cyclic code of length n is an ideal of this residue class ring [10, p. 126]. This ideal is a principal ideal generated by the unique monic polynomial expression $g(x)$ of least degree contained in the ring [10, p. 125]. A monic polynomial is one in which the highest power of x with non-zero coefficient has one as its coefficient. It can be shown that in fact the generator polynomial $g(x)$ is a factor of $x^n - 1$ [10, p. 126]. This fact is useful in classifying the cyclic codes of a given length over a given field.

As an example we will again take the cyclic Hamming (7,4,3) binary code. The code is an ideal in the residue class ring $\mathbb{Z}_2[x]/\langle x^7 - 1\rangle$. It is generated by the element $g(x) = 1 + x + x^3$. Thus the code is the set $\mathcal{C}_x = (1 + x + x^3)(\mathbb{Z}_2[x]/\langle x^7 - 1\rangle)$.

[1] In this reference the synonymous term 'quotient ring' is used instead of 'residue class ring'.

Obviously the codewords in this form are polynomials. There is a bijective correspondence between the polynomials of degree less than n over a field $\mathbb{F}$ and the vector space $\mathbb{F}^n$ of n-tuples over a field $\mathbb{F}$. Take the polynomial codeword $1+x+x^3$ of $\mathcal{C}_x$. It corresponds to the vector codeword given by the combination of the first, second and fourth rows from the generator matrix given in section 1.6. This vector codeword is 1101000, which is simply the coefficients of the codeword polynomial $1 + x + x^3$ written in order from x^0 to x^6. Thus the codeword polynomial $a_0(1) + a_1(x) + a_2(x^2) + a_3(x^3) + a_4(x^4) + a_5(x^5) + a_6(x^6)$ becomes $a_0a_1a_2a_3a_4a_5a_6$ in vector codeword form. We can create a generator matrix for a code from a generator polynomial of degree $\deg(g(x))$ by taking the first $n - \deg(g(x))$ cycles of the generator polynomial in vector form and using these as the rows of the generator matrix.

Unfortunately linear block codes that are not cyclic are not ideals in such residue class rings. Some may be equivalent to cyclic codes but others are certainly not[2]. In subsequent chapters we construct codes that are not cyclic but are ideals in group rings over dihedral groups. We will first explain the construction of cyclic codes in terms of group rings. The codes are constructed as ideals in group rings over cyclic groups and the product of the construction bares striking resemblance to that just given. We start by defining the term 'group ring'.

1.7 Group Rings

The main point of reference for the theory of group rings given here is the book "An Introduction to Group Rings" by Milies and Sehgal [20]. Let R be a ring and G be a group. The set of all formal linear combinations over R of the elements in G is a ring under the following operations:

$$\textbf{Addition:} \qquad u+v = \sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g)g$$

$$\textbf{Multiplication:} \qquad u\times v = \sum_{g\in G} a_g g \times \sum_{h\in G} b_h h = \sum_{g,h\in G} (a_g \times b_h)gh$$

where α_g, β_g and β_h are elements of R. It is stipulated that the "support" of each group ring element is a finite set. The *support* of an element $\sum \alpha_g g$ is the set of its non-zero coefficients $\{\alpha_g | \alpha_g \neq 0\}$.

This ring is denoted as RG and it is called the group ring of the group G over the ring R [20, p. 131]. The ring element α_g in a group ring element $u = \sum_g \alpha_g g$ is called the coefficient of g. When the ring R contains a multiplicative identity

[2]See section 1.11.2

a copy of G exists in the group ring. This is the set of group ring elements $1g$ for $g \in G$. The elements in this copy of G form a basis for the group ring over R since all of the elements are by definition formal linear combinations of the group elements. The group $RG(+)$ is in fact an R-module with basis G. When R is a field the group ring is a vector space over R, again with basis G.

As an example we form the group ring $\mathbb{Z}_2\mathbf{C}_7$ of the cyclic group with seven elements over the finite field with two elements. It consists of elements such as $u = 1g^0 + 0g^1 + 0g^2 + 1g^3 + 1g^4 + 0g^5 + 0g^6$, usually written as $1 + g^3 + g^4$. The addition and multiplication of group ring elements is governed by the group elements. Adding the elements $1 + g^3 + g^4$ and $1 + g^2$ produces the element $g^2 + g^3 + g^4$. Furthermore multiplying those same elements gives $1+g^2+g^3+g^5+g^4+g^6$. Group rings involving finite cyclic groups are discussed in more detail in the next section.

1.7.1 Cyclic Group Rings

Group rings in which the group is a finite cyclic group have already been discussed but under a different guise. A group ring in which the ring is a field $\mathbb{F}$ and the group is the infinite cyclic group is actually the ring of polynomials over the field $\mathbb{F}$. In this case the group ring addition and multiplication are exactly the usual addition and multiplication defined for polynomials. In the group ring it is the elements of the group that determine the multiplication just as the powers of x do in a polynomial.

In the case of finite cyclic groups the group ring $\mathbb{F}\mathbf{C}_n$ of the finite cyclic group $\mathbf{C}_n$ over the field $\mathbb{F}$ is isomorphic to the residue class ring of the principal ideal generated by the polynomial $x^n - 1$ in the polynomial ring over $\mathbb{F}$. In the residue class ring the class of $x^n - 1$ is the zero of the ring thus giving $x^n - 1 = 0$, or $x^n = 1$. This is analogous to the finite cyclic group relation $g^n = 1$.

For example the group ring of the finite field with two elements $\mathbb{Z}_2$ and the cyclic group $\mathbf{C}_7 = \langle g \mid g^7 \rangle$ of order seven is isomorphic to the residue class ring $\mathbb{Z}_2[x]/\langle x^7-1\rangle$. The element $a_0+a_1x+a_2x^2+a_3x^3+a_4x^4+a_5x^5+a_6x^6$ in the latter corresponds to the group ring element $a_0+a_1g+a_2g^2+a_3g^3+a_4g^4+a_5g^5+a_6g^6$.

Now that we have defined what a group ring is we can move on and define codes in terms of group rings. We start by defining, for any given group ring, a certain ring of matrices that is isomorphic to the group ring itself.

1.8 Matrices from Group Rings

In the following sections we define two types of matrix. The first type of matrix is called a group matrix. A group matrix has entries that are group elements.

Group matrices facilitate the creation of the second type of matrix. Matrices of the second type have ring elements as entries and are called group ring matrices. Later we will use group ring matrices to create generator matrices for codes we construct.

1.8.1 Group Matrices

Group matrices are given relative to listings of group elements. A *listing* of a group is an ordering of the group elements. Thus $\{1, g, g^2, g^3, g^4, g^5, g^6\}$ and $\{g, 1, g^3, g^2, g^5, g^4, g^6\}$ are two distinct listings of the cyclic group of order seven. The idea of a listing is implied in the case of cyclic codes where a polynomial codeword $a_0 + a_1x + a_2x^2 + a_3x^3 + a_4 + x^4 + a_5x^5 + a_6x^6$ is associated with the vector codeword $a_0a_1a_2a_3a_4a_5a_6$. In associating the codeword polynomial with the codeword vector we have effectively defined a listing of the powers of x and taken the coefficients of those elements in that order. Fixing a listing of the group elements in the underlying group of a group ring allows us to associate component vectors with group ring elements in a similar manner.

Listings play an important role in group matrices. The *group matrix* or *G-matrix* of a group G under the listing $\{g_1, g_2, \ldots, g_n\}$ is the n by n matrix in which the entry in the i^{th} row and j^{th} column is $g_i^{-1}g_j$. The group matrix of the above listing is displayed in figure 1.3. The G-matrix of a listing can thus

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

Fig. 1.3 — A group matrix.

be viewed as a matrix with columns labelled by the elements in the listing and rows labelled by the inverses of the elements in the listing. Each matrix entry is the product of its row label and its column label.

For example the group matrix of the listing $\{1, g, g^2, g^3, g^4, g^5, g^6\}$ of $\mathbf{C}_7$ is that in square brackets in figure 1.4. The column labels appear above the horizontal black line at the top and the row labels appear to the left of the black line on the left. Changing the listing of the group changes the group matrix. Another example, of a group matrix of the same group under a different listing $\{g, 1, g^3, g^2, g^5, g^4, g^6\}$ is given in figure 1.5. This second group matrix is a different matrix from the first.

Notice that the first example is a circulant matrix but the second is not. Certain group matrices admit to properties that others of the same group do

	1	g	g^2	g^3	g^4	g^5	g^6
1	1	g	g^2	g^3	g^4	g^5	g^6
g^6	g^6	1	g	g^2	g^3	g^4	g^5
g^5	g^5	g^6	1	g	g^2	g^3	g^4
g^4	g^4	g^5	g^6	1	g	g^2	g^3
g^3	g^3	g^4	g^5	g^6	1	g	g^2
g^2	g^2	g^3	g^4	g^5	g^6	1	g
g	g	g^2	g^3	g^4	g^5	g^6	1

Fig. 1.4 — A group matrix of $\mathbf{C}_7$.

	g	1	g^3	g^2	g^5	g^4	g^6
g^6	1	g^6	g^2	g	g^4	g^3	g^5
1	g	1	g^3	g^2	g^5	g^4	g^6
g^4	g^5	g^4	1	g^6	g^2	g	g^3
g^5	g^6	g^5	g	1	g^3	g^2	g^4
g^2	g^3	g^2	g^5	g^4	1	g^6	g
g^3	g^4	g^3	g^6	g^5	g	1	g^2
g	g^2	g	g^4	g^3	g^6	g^5	1

Fig. 1.5 — Another group matrix of $\mathbf{C}_7$.

not. We now define the group ring matrix of a group ring element according to a listing.

1.8.2 Group Ring Matrices

The *group ring matrix* of an element u in a group ring RG, according to the listing $\{g_1, g_2, \ldots, g_n\}$ of the group G, is the $|G|$ by $|G|$ matrix with entries over the ring R where the entry in the i^{th} row and j^{th} column is the coefficient of the group element $g_i^{-1}g_j$ in u [12, 13]. The group ring matrix of such an element u is display in figure 1.6 where α_g denotes the coefficient of the group element g in the group ring element u. Thus an element's group ring matrix is the matrix

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

Fig. 1.6 — A Group Ring Matrix.

constructed by replacing the entries in the group matrix with their coefficients in the element. Throughout this text we will use the convention that group ring elements are denoted by lowercase letters and their respective group ring matrices are denoted by those letters in uppercase.

As an example take the element $1 + g + g^3$ in the group ring $\mathbb{Z}_2\mathbf{C}_7$ using the listing $\{1, g, g^2, g^3, g^4, g^5, g^6\}$ from above. The coefficients of the elements in the listing are then $1, 1, 0, 1, 0, 0$ and 0 respectfully. The group ring matrix is given in figure 1.7. Notice that since the group matrix is circulant so too is the group

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Fig. 1.7 — A group ring matrix.

ring matrix. The group ring matrices of all of the group ring elements will be circulant according to this listing.

The set of all group ring matrices of the elements of a group ring under a given listing is a ring itself under matrix addition and multiplication. This ring is isomorphic to the group ring [14]. Should we change the listing of the group in question, and thus change the group matrix, we will also change the group ring matrices of the group ring elements. Thus there is one group ring matrix per element in a group ring, per listing of the group. In the next section we define two important properties of group ring elements that are defined in terms of properties of their group ring matrices.

1.8.3 Rank and Transpose

In the following sections we assume that the underlying ring of each group ring is a field. We now define two terms regarding group ring elements: rank and transpose. We start with the latter. The *transpose* of a group ring element $u = \sum_i \alpha_i g_i$ is the group ring element $u^{\mathrm{T}} = \sum_i \alpha_i g_i^{-1}$, in which the coefficient of each group element in u is the coefficient of its inverse [12, 13]. This definition ensures that the transpose of a group ring matrix of an element is the group ring matrix of the transpose of the element, no matter what the listing. For example the transpose of the group ring element $u = 1 + g + g^3$ in $\mathbb{Z}_2\mathbf{C}_7$ is $u^{\mathrm{T}} = 1^{-1} + g^{-1} + g^{-3} = 1 + g^6 + g^4 = 1 + g^4 + g^6$. Figure 1.8 shows the group ring matrix of u^{T} according to the listing $\{1, g, g^2, g^3, g^4, g^5, g^6\}$. The matrix is

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Fig. 1.8 — The group ring matrix of u^T.

the transpose of the group ring matrix of u given in figure 1.7.

The second term we define is rank. The *rank* of a group ring element u is the rank of the group ring matrix of u according to any listing [12, 13]. For example the reduced row echelon form of the group ring matrix of u according to the listing $\{1, g, g^2, g^3, g^4, g^5, g^6\}$ is displayed in figure 1.9. Evidently the group ring matrix is of rank four and hence the rank of u is four. The linear independence of the rows of the group ring matrix is closely related to the linear independence of the set Gu, which we discuss in section 1.9.2.

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Fig. 1.9 — The reduced row echelon form of u.

1.9 Group Ring Codes

In the following section we discuss group ring codes as defined in Hurley and Hurley's papers on the subject [12, 13]. Again we assume that the underlying ring of each group ring is a field. Two different types of group ring code are defined in that paper: zero divisor codes and unit derived codes. In this thesis we only discuss zero divisor codes.

Let u be a left zero divisor in a group ring RG and let W be a submodule of RG with basis $S \subseteq G$. The set of group ring elements Wu is called the (left) *zero divisor code* of the zero divisor u and the submodule W. In the case where RG is non-commutative we may also define a (right) group ring code uW. We will always use the former definition in this thesis however. The element u is called the generator of the zero divisor code. The code is a submodule of RG itself and has basis Su [12, 13]. The elements of a zero divisor code are called group ring codewords.

As an example we use the group ring $\mathbb{Z}_2\mathbf{C}_7$. Let W be the submodule generated by the set of group elements $S = \{1, g, g^2, g^3\}$ in $\mathbf{C}_7$ and let u be the zero divisor $1 + g + g^3$ in the group ring. The group ring code of u and W is then $\mathcal{C} = Wu = \{(a_0 1 + a_1 g + a_2 g^2 + a_3 g^3)u \mid a_0, a_1, a_2, a_3 \in \mathbb{Z}_2\}$.

Earlier we stated that the only codes we construct in this thesis are linear block codes. Group ring codes are linear block codes when R is a field. We only consider the case in which R is the finite field with two elements in this thesis. Irrespective of R being a field, group ring codes have length and dimension. We discuss these terms now in that regard.

1.9.1 Length and Dimension

We use the same notation from the previous section, where W is a submodule of the group ring RG with basis S and u is a zero divisor in RG. The *length* of a zero divisor code is the order of the group G. The *dimension* of a zero divisor

code Wu is the maximum number of linearly independent elements in Su over R. Since S is a subset of the group G we have that the maximum number of linearly independent elements in Su over R is less than or equal to that in Gu.

Where the maximum number of linearly independent elements in Su is equal to that in Gu the code is a left ideal in the group ring [12, 13]. In fact it is the principal left ideal of u: $Wu = (RG)u$ [12, 13]. In subsequent chapters we will deal only with codes that are principal left ideals. In the next section we discuss a method for constructing a generator matrix for a group ring code.

1.9.2 Generator Matrices

For a fixed listing of the group G we get a fixed group matrix. The columns of the group matrix are labelled by the elements of the listing. The rows are labelled by the inverses of the elements of the listing. The group ring matrices of the elements of the group ring are constructed according to this group matrix. The ring of all group ring matrices according to the given group matrix is isomorphic to the group ring [13]. Thus the product of two group ring matrices is still a group ring matrix according to the group matrix.

Let the i^{th} element of the listing be that which is the identity of the group. Then the i^{th} row of the group matrix is exactly the listing itself, albeit in matrix row form. Thus the i^{th} row of each of the group ring matrices is a vector containing the coefficients of the matrix's corresponding group ring element in order according to the listing.

Now consider the group ring element $g_j u$ where g_j is the j^{th} element of the group listing.[3] The group ring matrix of $g_j u$ is equal to the product of the group ring matrix G_j of g_j with the group ring matrix U of u. Consider the i^{th} row of the matrix in question $G_j U$. Its entries are the dot products of row i of G_j with each of the columns of U in order. The i^{th} row of G_j contains a one in the j^{th} position and zeros everywhere else. Thus the j^{th} row of U must consist of the coefficients of $g_j u$ written in a vector according to the listing of the group. We can use this fact to create a component vector form of the code.

Vector Forms of Codes

The code Wu is an R-module generated by the basis Su [12, 13]. The code is the set of all linear combinations of the elements of Su over R. Consider the positions of the elements of S in the group listing. In light of the argument in the previous section the set of all linear combinations over R of the rows of U

[3] Here we are ignoring the distinction between the group element g_j and the group ring element g_j for the purposes of clarity. The distinction is obvious from the context in which each appears.

corresponding to these positions is another form of the same code. The only difference between the code that is comprised of linear combinations of the group ring elements and the code comprised of those of the rows of U is the notation used. We will call the former the *group ring form* of the code and the latter the *vector form* of the code.

The rows of U corresponding to the elements of S form a basis for the vector form of the code and thus can be used to form a generator matrix for the code. When the ring R is a field the group ring is a vector space over that field and the code is a subspace. Thus the code is a linear block code. In the case of the code being the principal left ideal of u in the group ring, the vector form of the code is the span of all of the rows of U. Conversely we can construct a code that is a principal ideal in a group ring by taking the group ring form of the row space of the group ring matrix of a zero divisor. This is exactly how we will construct the codes in this thesis.

Equivalent Vector Forms

Note that the group ring form of a code does not necessarily conform to a listing of the underlying group. The addition defined on the group ring enables us to add group ring codewords without the terms of the codewords following any particular listing. The different vector forms of a group ring code pertaining to the different group listings are thus all equivalent. In the next section we discuss the fact that we can also construct check matrices for the vector forms of group ring codes.

Check Matrices

Let $\mathcal{C}$ be a zero divisor code generated by an element u in RG. An element x in RG with the property $cx = 0$ if and only if $c \in RG$ is in $\mathcal{C}$ is called a *check element* for $\mathcal{C}$. Since u is a zero divisor there exists another element v in RG such that $uv = 0$. The code is the set Wu and thus v has the property that $cv = 0$ for all c in $\mathcal{C}$. Thus v is a check element if yv is not equal to zero when $y \notin \mathcal{C}$. That is the case when the rank of u plus the rank of v is equal to the order of G [12, 13]. This is obvious from the fact that a matrix's rank plus the dimension of its null-space is equal to the number of columns it has [17, p. 245].

We are now in a position to consider codes that are ideals in group rings other than those involving cyclic groups. We will consider the ideals in group rings over dihedral groups. First we define what a dihedral group is.

1.10 Dihedral Groups

One of the first areas of study in which groups arose was that of the symmetries of geometrical shapes. A *dihedral group* $\mathbf{D}_n$ of order $n = 2k$ is the set of symmetries of the regular k-gon together with the operation of the composition of symmetries [17, p. 60]. Regular k-gons have two types of symmetries: rotational and reflectional. The rotation of a regular k-gon through $2\pi/k$ radians is the first rotational symmetry. In the dihedral group of order $2k$ we represent this rotational symmetry by the letter b and it is of order k. Pivoting the regular k-gon through a line joining two opposing vertices in the case where k is even or through the midpoint of a side and the opposing vertex when k is odd is a symmetry of the shape. We represent this symmetry by the letter a and it is of order two. The regular k-gon has thus $n = 2k$ symmetries in total and these can all be described as different compositions of the symmetries a and b.

Dihedral groups are non-commutative, as witnessed by the fact that applying the symmetry a to the regular k-gon and then applying b is not equivalent to first applying b and then a. The dihedral group is generally denoted/defined as $\mathbf{D}_{2k} = \langle a, b \mid a^2, b^k, (ab)^2 \rangle$. The group matrices pertaining to listings of the dihedral group are very interesting and are discussed in the next section.

1.10.1 Dihedral RG-Matrices

The most common way to list the elements of a dihedral group $\mathbf{D}_{2k} = \langle a, b \rangle$ is $\{1, b, b^2, \ldots, b^{k-1}, a, ab, ab^2, \ldots, ab^{k-1}\}$. This is one of the main listings we will use throughout this thesis as it will lead to the illustration of some nice properties of the zero divisor codes we construct. In figure 1.10 we have as an example constructed the group matrix of the dihedral group of order eight under this listing. According to this group matrix the element $1 + a + ab + ab^2$ in $\mathbb{Z}_2\mathbf{D}_8$ has the group ring matrix given in figure 1.11. Notice that this matrix is of the form:

$$\left[\begin{array}{c|c} I & A \\ \hline A & I \end{array}\right]$$

where I is the four by four identity matrix and A is a reverse circulant matrix. A *reverse circulant* matrix is one in which the i^{th} row is the first right cyclic shift of the $(i+1)^{\text{st}}$ row [10, p. 377]. Elements with group ring matrices of this form lead to interesting codes and we will concentrate on such codes in this thesis.

The code $\mathcal{C} = (\mathbb{Z}_2\mathbf{D}_8)u$ where u is the element $1 + a + ab + ab^2$ is the group ring form of the code that is the row space of the above matrix. The element u has the property that u^2 is equal to zero and thus it is a (both left and right) zero divisor. The reduced row echelon form of the group ring matrix turns out

	1	b	b^2	b^3	a	ab	ab^2	ab^3
1	1	b	b^2	b^3	a	ab	ab^2	ab^3
b^3	b^3	1	b	b^2	ab	ab^2	ab^3	a
b^2	b^2	b^3	1	b	ab^2	ab^3	a	ab
b	b	b^2	b^3	1	ab^3	a	ab	ab^2
a	a	ab	ab^2	ab^3	1	b	b^2	b^3
ab	ab	ab^2	ab^3	a	b^3	1	b	b^2
ab^2	ab^2	ab^3	a	ab	b^2	b^3	1	b
ab^3	ab^3	a	ab	ab^2	b	b^2	b^3	1

Fig. 1.10 — A group matrix of $\mathbf{D}_8$.

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Fig. 1.11 — The group ring matrix of u.

to be that given in figure 1.12. The code is of length eight. Its rank, as is evident

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Fig. 1.12 — In reduced row echelon form.

from the above matrix, is four and thus the dimension of the code $\mathcal{C}$ is four. The first four rows of the matrix form a generator matrix for the code. The code is self-dual, a property we will further explore in the next section in terms of group rings.

1.10.2 Self-Dual Zero Divisor Codes

A zero divisor code generated by an element u is self-dual if and only if uu^{T} is equal to zero and the rank of u is half the order of the group [12, 13]. The generator u in the example from the previous section is equal to its own transpose since the identity of $\mathbf{D}_8$ and all of the elements of the form ab^i for i from zero to three are equal to their own inverses. Also u^2 is equal to zero and its rank is four, half the order of $\mathbf{D}_8$. Hence the code $\mathcal{C}$ generated by u is self-dual. It turns out that the code is actually a well known code called the extended Hamming $(8, 4, 4)$ code.

1.11 The Extended Hamming Code

In earlier sections we discussed the Hamming $(7, 4, 3)$ linear block code. This code can be extended by appending an even parity bit to each of its codewords which increases the code's length by one. An *even parity bit* is an extra component appended to a codeword in order to ensure that the codeword is of even weight. Thus a 0 is appended to the codewords in the original code that are of even weight and a 1 is appended to the codewords of odd weight. A new code formed from the appendage of a parity bit to all of a code's codewords is called an *extended* code.

Adding an even parity bit to the Hamming $(7, 4, 3)$ code creates the code known as the extended Hamming $(8, 4, 4)$ code. The dimension of the code

remains unchanged. The minimum distance of the Hamming $(7, 4, 3)$ code is odd and the minimum distance of a linear block code is equal to the least of the weights of its codewords. All of the codewords of weight three in the original code are converted into codewords of weight four. So the minimum distance of the extended Hamming $(8, 4, 4)$ code is four.

1.11.1 Generator Matrix

Consider the generator matrix given in figure 1.2 for the Hamming $(7, 4, 3)$. To create a generator matrix for the extended Hamming $(8, 4, 4)$ code we append a column to the right hand side of this matrix with entries that are the even parity bits for the corresponding rows. Thus a generator matrix for the extended Hamming $(8, 4, 4)$ code is that given in figure 1.13. The new entries added to

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & \mathbf{1} \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & \mathbf{1} \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & \mathbf{0} \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & \mathbf{1} \end{bmatrix}$$

Fig. 1.13 — An extended Hamming code generator matrix.

the matrix are in bold type.

It is straight-forward to show that this matrix generates a code equivalent to the code generated by the zero divisor in section 1.10.1. We re-order the rows of the matrix so that the new matrix consists of rows three, one, four and two of the above matrix in that order. The new matrix is shown if figure 1.14. The new matrix generates the same code as that in figure 1.13, since the basis

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 & \mathbf{0} \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & \mathbf{1} \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & \mathbf{1} \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & \mathbf{1} \end{bmatrix}$$

Fig. 1.14 — A new extended Hamming code generator matrix.

elements of the row space remain unchanged. Then re-ordering the first four columns to create the four by four identity matrix in those columns of the new matrix gives a matrix that generates an equivalent code. The new matrix is of the form $G = [I|A]$ where I is the four by four identity matrix and A is a

four by four reverse circulant matrix. In fact the new matrix is the exact same generator matrix constructed for the code given in section 1.10.1. Thus the zero divisor code constructed there is equivalent to the extended Hamming $(8, 4, 4)$ code. The Hamming $(8, 4, 4)$ code is thus the principal left ideal of the group ring element u given in that section. This is significant since the code cannot be constructed as a cyclic code, a fact shown in the next section.

1.11.2 Not Cyclic

The binary cyclic codes of length n are precisely the principal ideals of the factors of $x^n + 1$ in the residue class ring $\mathbb{Z}_2[x]/\langle x^n + 1\rangle$ [2, p. 101]. Thus the binary cyclic codes of length eight are generated by the factors of $x^8 + 1$. Now $x^8 + 1 = (x^4 + 1)^2 = (x^2 + 1)^4 = (x + 1)^8$ and the dimension of a cyclic code is its length minus the degree of its generator polynomial. The Hamming code is of dimension four so its generator polynomial would have to have degree eight minus four which is four. The only cyclic code of length eight and dimension four is generated by the polynomial $g(x) = (x + 1)^4 = x^4 + 1$. The generator polynomial is a polynomial codeword itself however and is only of weight two. Thus it cannot generate a code of minimum distance four and thus does not generate the extended Hamming $(8, 4, 4)$ code.

1.11.3 Using the Dihedral Group

In light of the fact that the extended Hamming code cannot be generated by a polynomial, the group ring construction of it is quite interesting. It is a construction of the code that closely resembles a polynomial construction. The only real difference is that instead of using the cyclic group the dihedral group was used. In the following chapters we will construct other non-cyclic codes using dihedral group rings.

Chapter 2

The $(24, 12, 8)$ Extended Binary Golay Code

In this chapter we give a new construction of the $(24, 12, 8)$ extended binary Golay code. It is constructed from a zero divisor in a group ring over a dihedral group. The construction resembles that of a cyclic code using a polynomial.

The $(24, 12, 8)$ code is the extension of the $(23, 12, 7)$ binary Golay code by a single even parity bit. The $(23, 12, 7)$ code is a well known code appearing extensively in coding theory literature. It has a number of properties that are of importance in both mathematics and coding theory. These are demonstrated and proven in most introductory books on coding theory [10]. We will only examine the extended code here. While it does not share many of the $(23, 12, 7)$ code's properties, it does exhibit other significant traits. These have been previously explored in other efforts. However, they are readily exposed by the new construction given here.

In the first part of this chapter we show that twenty-four different zero divisors in a given dihedral group ring can be used to construct the code. These zero divisors were originally found by computer search. We prove that we have in fact constructed the code, showing that it is self-dual, doubly even, of dimension twelve and of minimum distance eight. We further show that the code is in a fact an ideal in the group ring and that it is quasi cyclic. These results have already been published in the Institute of Electrical and Electronic Engineer's journal "Transactions on Information Theory" [19]. In the second part of the chapter we prove that these zero divisors are the only ones of their kind in their group ring capable of generating the code. We start with a brief history of the binary Golay codes.

2.1 History of the Code

The extended binary Golay code is the unique $(24, 12, 8)$ linear block code up to equivalence [10, p. 401]. The code is interesting from both a coding theory and a mathematical perspective as it is an extremal type II code. A type II code is a binary linear block code that is both self-dual and doubly even[1] [10, p. 339]. An *extremal* type II code is a type II code with minimum distance $(4\lfloor n/24 \rfloor + 4)$ where n is the code's length [10, p. 346]. This is the best possible minimum distance for a binary type II code of length n [10, p. 344].

Thus eight is the best minimum distance a binary type II code of length twenty-four can achieve. It is in fact the best possible minimum distance a binary code of length twenty-four and dimension twelve can have, as evidenced by the Griesmer bound [10, p. 81]:

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil$$

where n is the length of the code, k the dimension and d the minimum distance.

The (non-extended) $(23, 12, 7)$ binary Golay code is interesting for many reasons. It was originally constructed by Marcel J. E. Golay using Pascal's triangle. He published this result in 1949 [4]. The code turned out to be cyclic and can be generated by the polynomial $1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}$ [10, p. 401]. It is also a perfect binary linear block code, meaning it exactly meets the sphere packing bound:

$$\sum_{i=0}^{\lfloor d-1/2 \rfloor} \binom{n}{i} \leq 2^{n-k}$$

where n is the length of the code, k the dimension and d the minimum distance [10, p. 48]. Thus:

$$\sum_{i=0}^{3} \binom{23}{i} = 2^{11}.$$

In essence the code has the maximum number of codewords that a binary linear code of length twenty-three and distance seven can have [10, p. 49]. In fact it is the only non-trivial, multiple-error correcting binary code that is perfect other than the Hamming codes [10, p. 49]. Furthermore it is the unique binary code of its length, dimension and minimum distance up to equivalence [10, p. 49].

The properties discussed above for each of the two codes are not shared by the other. The extended $(24, 12, 8)$ code is not perfect. Nor is it cyclic since a

[1] A doubly even code is one in which the weight of each codeword is congruent to zero modulo four.

doubly even self-dual code cannot be cyclic [23]. On the other hand the $(23, 12, 7)$ code is not self-dual. It is of dimension twelve but its null space is of dimension (twenty-three minus twelve equals) eleven. Moreover the $(23, 12, 7)$ code is not singly even—let alone doubly even—since its minimum distance is odd.

Thus both codes are of interest in their own right. Much is known about the $(23, 12, 7)$ code due to its cyclic nature. It can be constructed from a single polynomial, it is an ideal in a residue class ring and its minimum distance can be calculated relatively quickly.

In the following chapter we prove that the extended code is also constructible using a single polynomial-like generating element, that it is an ideal in a group ring and that its minimum distance is readily calculated. We'll start now by discussing some elements of interest in a given dihedral group ring.

2.2 A Group Ring Code

The first part of this chapter is dedicated to showing that the $(24, 12, 8)$ extended binary Golay code can be generated by a zero divisor in the group ring $\mathbb{Z}_2\mathbf{D}_{24}$. The group ring $\mathbb{Z}_2\mathbf{D}_{24}$ is formed by the finite field with two elements $\mathbb{Z}_2$ and the dihedral group of order twenty-four $\mathbf{D}_{24}$. In accordance with the previous chapter we denote the generators of the group by a and b. The generator a is that of order two and b is the generator of order twelve.

Our motivation for using this group ring may not be obvious. Our reason for using the finite field with two elements is straightforward. The components of the codewords in a group ring code come from the underlying ring. The code is binary, and hence its components are elements of $\mathbb{Z}_2$.

The dihedral group is a less obvious choice. The length of the $(24, 12, 8)$ extended binary Golay code is twenty-four. The length of a group ring code is the order of the underlying group. Thus for the code to be a group ring code the group involved would be of order twenty-four. There are many groups of order twenty-four however.

In the previous chapter we saw that the dihedral group of order eight generated the extended Hamming $(8, 4, 4)$ code. This code shares many of the extended binary Golay code's properties. Both are self-dual and doubly even. They are also extensions of perfect cyclic codes. This led to our investigation of the dihedral group of order twenty-four. We were successful in our attempts to find generating elements for the code using it.

In total we found twenty-four zero divisors of the form $1 + a\mathbf{f}$ in $\mathbb{Z}_2\mathbf{D}_{24}$ that generate the code where $\mathbf{f}$ is a sum of powers of the group element b. The GUAVA package in GAP was used[3]. The occurrence of the powers of b with non-zero coefficients in $\mathbf{f}$ is the only difference between the zero divisors. We

chose elements of this form because their group ring matrices have some useful properties, as we will see later in the chapter.

Throughout this chapter we will use one of the zero divisors, $u = 1 + a\mathbf{f} = 1 + a(b + b^2 + b^4 + b^5 + b^6 + b^7 + b^9)$, as an example. The other twenty-three zero divisors are of the form $1 + ab^i\mathbf{f}$ for i from one to eleven and $1 + ab^j\mathbf{f}^{\mathrm{T}}$ for j from zero to eleven. Trivial changes to the arguments in this chapter will adapt them to work for any of the other twenty-three zero divisors. In any case we will see later that the generator matrices derived from any of these other twenty-three elements are permutation equivalent to that derived here for u.

The code, as we will see, is the principal left ideal of u in $\mathbb{Z}_2\mathbf{D}_{24}$. Thus the code is constructed in group ring form as $\mathbb{Z}_2\mathbf{D}_{24}u$. The row space of the group ring matrix of u, as described in the previous chapter, is the vector form of the code. In the following sections we rely on the interplay between the vector and group ring forms of the code to prove the results. We describe the group ring matrix of u next.

2.3 The Group Ring Matrix

Let us now construct the group ring matrix of the element $u = 1 + a(b + b^2 + b^4 + b^5 + b^6 + b^7 + b^9)$ in $\mathbb{Z}_2\mathbf{D}_{24}$. We use the listing $\{1, b, b^2, \ldots, b^{11}, a, ab, ab^2, \ldots, ab^{11}\}$ of $\mathbf{D}_{24}$. The reason for choosing this listing is that the group ring matrices of the elements of the form $1 + a\mathbf{f}$ have some useful properties under its influence. According to the listing the group ring matrix U of u is of the form:

$$\left[\begin{array}{c|c} I & A \\ \hline A & I \end{array}\right]$$

where I is the twelve by twelve identity matrix and A is the twelve by twelve matrix in figure 2.1. Note that this is the same form of matrix given in section 1.10.1, albeit with larger submatrices. Due to the form of element and the listing chosen, the twelve by twelve identity matrix thus occupies the upper left-most and lower right-most blocks of the group ring matrix. The matrix A is reverse circulant and sits in the lower left-most and upper-right most blocks of the group ring matrix. All reverse circulant matrices are symmetric, equal to their own transposes. The fact that A is symmetric leads directly to U being symmetric. Thus elements of the form $1 + a\mathbf{f}$ in the group ring $\mathbb{Z}_2\mathbf{D}_{24}$ under the listing $\{1, b, b^2, \ldots, b^{11}, a, ab, ab^2, \ldots, ab^{11}\}$ have symmetric group ring matrices comprised of the twelve by twelve identity matrix and a twelve by twelve reverse circulant matrix.

The matrix U is a matrix with entries in the field $\mathbb{Z}_2$. Thus the row space

$$\begin{bmatrix}
0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0
\end{bmatrix}$$

Fig. 2.1 — The A submatrix of U.

of U is a binary linear block code. We will call this code $\mathcal{C}$. Over the next few sections we will show that $\mathcal{C}$ is a $(24, 12, 8)$ linear block code and hence is the unique extended binary Golay code. Along the way we will show that the code is self-dual, doubly even, quasi-12 cyclic and also that it is an ideal in the group ring. We'll start by showing that the code is of dimension twelve.

2.4 Dimension Twelve

We prove here that the dimension of the code is twelve using a principle from linear algebra. The principle states that the dimension of the row space of a matrix plus the dimension of its null space is equal to the number of columns that it has [17, p. 245]. The proof centres on the fact that the element u when squared is equal to zero, a fact we now discuss.

2.4.1 The Zero Divisor u

We have stated without proof that the element u is a zero divisor. Hence another element of the group ring must multiply with it to produce zero. In fact it multiplies with itself to give zero; the element u when squared is zero. In the group ring it does not take long to multiply the terms of u^2 out in order to prove this. The calculation is marginally hastened by the following argument: $u^2 = (1 + a\mathbf{f})^2 = 1^2 + 2a\mathbf{f} + (a\mathbf{f})^2 = 1 + a^2(\mathbf{f}^{\mathrm{T}}\mathbf{f}) = 1 + (\mathbf{f}^{\mathrm{T}}\mathbf{f})$. Thus u squared is equal to zero if and only if $(\mathbf{f}^{\mathrm{T}}\mathbf{f})$ is equal to one. There is an even quicker way to verify that u squared equals zero however, using its group ring matrix and a little algebra.

Thanks to the ring isomorphism between the group ring $\mathbb{Z}_2\mathbf{D}_{24}$ and every ring of group ring matrices [12, 13], the product u^2 equals 0 if and only if the group ring matrix U when squared equals the zero matrix. Working block-wise with the matrix U we can see that:

$$\begin{aligned}
& U^2 = \underline{0}_{24} \\
\Leftrightarrow & \begin{bmatrix} I & A \\ A & I \end{bmatrix} \begin{bmatrix} I & A \\ A & I \end{bmatrix} = \underline{0}_{24} \\
\Leftrightarrow & \begin{bmatrix} I + A^2 & A + A \\ A + A & I + A^2 \end{bmatrix} = \begin{bmatrix} \underline{0}_{12} & \underline{0}_{12} \\ \underline{0}_{12} & \underline{0}_{12} \end{bmatrix} \\
\Leftrightarrow & \begin{bmatrix} I + A^2 & \underline{0}_{12} \\ \underline{0}_{12} & I + A^2 \end{bmatrix} = \begin{bmatrix} \underline{0}_{12} & \underline{0}_{12} \\ \underline{0}_{12} & \underline{0}_{12} \end{bmatrix}
\end{aligned}$$

Here we have denoted the m by m zero matrix as $\underline{0}_m$ for m a positive integer. Thus the matrix U when squared is equal to zero if and only if the matrix A squared is equal to the identity matrix.

In multiplying A by A we take the dot products of each of the rows of A with each of the columns of A, giving the entries of the product. The matrix A when squared is equal to the identity matrix if the dot product of row i with column j is one when i is equal to j and zero otherwise, for i and j from one to twelve.

Since A is symmetric, its rows are equal to its columns in the same order. Hence we only need show that the dot product of distinct rows of A is zero and the dot product of each row with itself is one. The latter is easy. The first row is of odd weight and hence its dot product with itself is one. All the other rows are cyclic shifts of the first row and so are of odd weight. The dot product of each row with itself is thus one.

In order to show that the dot product of distinct rows of A is zero we will use a property of A that we will re-use at other times later in the chapter. Thus we will give it its own section.

2.4.2 Pairs of Rows of A

In this section we will prove that the dot product of each pair of distinct rows of A is equal to the dot product of row one with one of the rows two to seven of A. Consider two arbitrary rows of A: rows i and j where $1 \leq i < j \leq 12$. All the rows of A are cycles of each other since A is reverse circulant. Thus rows i and j are both cycles of the first row.

The dot product of two vectors is unaffected by cycling the two vectors by the same amount. Hence we can cycle rows i and j by the same amount and their dot product will remain unchanged. We can cycle row i to become the

Row	Components
5	1 1 1 1 0 1 0 0 0 1 1 0
10	1 0 0 0 1 1 0 1 1 1 1 0
+	0 1 1 1 1 0 0 1 1 0 0 0
1	0 1 1 0 1 1 1 1 0 1 0 0
6	1 1 1 0 1 0 0 0 1 1 0 1
+	1 0 0 0 0 1 1 1 1 0 0 1
1	0 1 1 0 1 1 1 1 0 1 0 0
8	1 0 1 0 0 0 1 1 0 1 1 1
+	1 1 0 0 1 1 0 0 0 0 1 1

Fig. 2.2 — Three Combinations of Equal Weight

first row and cycle row j by the same amount. The two cycled rows have the same dot product as the two rows before the cycling. We can also cycle row j until it becomes the first row and cycle row i by the same amount, leaving their dot product unchanged. Rows i and j have thus the same dot product as two potentially distinct pairs of rows where one of the rows in the pair is the first row of A.

The only case in which these two pairs of rows are not distinct is when the two rows are six cycles apart. Six is half the number of rows in A. Otherwise the two pairs of rows are distinct. The first pair of rows is row one with row $j + (13 - i)$ modulo twelve since it takes $13 - i$ modulo twelve cycles to turn the i^{th} row into the first. The second is row one with row $i + (13 - j)$ modulo twelve since row one and row j are $(13 - j)$ modulo twelve cycles apart. Figure 2.2 illustrates this connection for rows five and ten of A.

The dot product of row one and row $i + (13 - j)$ is therefore equal to that of row one with row $j + (13 - i)$. This implies that the dot product of row one with row k is equal to that of row one with row $14 - k$ for k from two to seven. Letting $k = i + (13 - j)$ we can manipulate the equality (modulo twelve) to show that $j + (13 - i) = 14 - k$. In other words the dot product of the first row with any of the rows further down the matrix than the seventh row is equal to the dot product of the first row with one of the rows further up the matrix than the seventh row.

So the dot product of row one with row two is equal to that of row one with row twelve, that of row one with row three is equal to that of row one with row eleven, and so on. Therefore we can check that the dot product of every pair of distinct rows of A is zero by checking that the dot product of row one with each of the rows two to seven is zero. A quick investigation of the matrix A above shows this to be true. Thus the matrix U^2 and the group ring element u^2 are both equal to zero in their respective rings.

The dot product is not the only operation to which the above argument can be applied. For instance, the weight of each two row combination of A is also equal to the weight of some combination of row one and one of the rows two to seven. This observation will be used in later sections. Furthermore we will use the fact that row one paired with row seven is the only combination involving row one that is not necessarily equal in weight to any of the others. Right now we will determine the rank of U and hence the dimension of the code $\mathcal{C}$.

2.4.3 The Rank of U

We will show that the rank of U is exactly twelve by first showing that is at least twelve and then showing that it is at most twelve. The rank of a matrix is the dimension of its row space which is equal to the maximum number of rows that are linearly independent. Every identity matrix is of full rank since all of its rows are linearly independent. The twelve by twelve identity matrix forms the top left block of the matrix U. Hence the rank of U is at least twelve.

The fact that the matrix U squared is equal to zero limits its rank. From linear algebra the rank of a matrix plus the dimension of its null space is equal to the number of columns it has [17, p. 245]. The matrix U has twenty-four columns and we've just seen that its rank is at least twelve. All of the columns of U are contained in its null space since squaring it gives zero. The matrix is equal to its own transpose and so its columns are equal to its rows and therefore the rows of U are contained in its null space. Hence the null space of U is of dimension at least twelve and its rank is therefore at most twenty-four minus twelve which is twelve. Combined with the previous argument therefore the rank of U must be exactly twelve.

Obviously then the code $\mathcal{C}$ which is the span of the rows of U is a $(24, 12)$ linear block code. Moreover the first twelve rows of U are linearly independent and so form a basis for the code. A generator matrix for the code $\mathcal{C}$ is thus the matrix $G = [I|A]$. This matrix is of an interesting form a fact discussed in the next section.

2.4.4 Reverse Circulant Generator Matrices

Having created the generator matrix for our code we will make a quick aside to note a property of the construction that has been of interest in the literature. The generator matrix that has been constructed consists entirely of two square k by k submatrices, one on the left that is circulant (the identity matrix) and another on the right that is reverse circulant (the matrix A). Code generator matrices of this form are called reverse circulant generator matrices [10, p. 377]. A closely related type of generator matrix that has received a good deal of

coverage in the literature are those of the form $G' = [B|C]$ where B and C are circulant matrices. Generator matrices of that form are called double circulant generator matrices [5]. Switching the i^{th} column of the submatrix A in our generator matrix with its $(13 - i)^{\text{th}}$, for i from one to six, will result in a double circulant matrix that generates the same code (up to equivalence).

Now we will return to the main points points of interest in our construction. We have constructed a code $\mathcal{C}$ of length twenty-four and dimension twelve. Should this code have minimum distance eight then it is the extended binary Golay code. Before proving that this is in fact the minimum distance of $\mathcal{C}$ we will show that the code is self-dual and doubly even. We start with the code's self-duality.

2.5 Self-Duality

As defined in section 1.4 a code is self-dual if it is exactly its own dual code. The code $\mathcal{C}$ in vector form is the row space of the group ring matrix U. We saw in section 2.4.3 that the rows of U are contained in its dual code. Hence the code $\mathcal{C}$ is self-orthogonal.

Of course we also saw also that the row space of U is of dimension twelve and the null space of U is of dimension twenty-four minus twelve, which is also twelve. Since the code is a subspace, the row space and null space of U are exactly the same. Hence the code $\mathcal{C}$ is self-dual.

As stated in section 1.10.2 a zero divisor code generated by a zero divisor x is self-dual if and only if $xx^{\mathrm{T}} = 0$ and the rank of x is half the order of the group [13]. These two conditions hold true for u, since the group ring matrix U is symmetric and of rank twelve. Thus we can see that the code is self-dual from both the vector code perspective and the group ring perspective. In the next section we use the self-duality of the code to observe that it is doubly even.

2.6 Doubly Evenness

A *doubly even code* is a code in which the weight of every non-zero codeword is divisible by four. Any binary and self-orthogonal linear block code generated by a matrix whose rows are all of weight divisible by four is doubly even [10, p. 10]. Since $\mathcal{C}$ is self-dual, it is self-orthogonal. Also the first row of G is of weight eight and all the other rows are permutations of this row. Hence all of the rows are of weight eight. Therefore $\mathcal{C}$ is a doubly even code.

The fact that the code is doubly even greatly aids the calculation of its minimum distance. Another facet of the code that aids the calculation of its minimum distance is its quasi cyclic nature.

G	I	A
1	1 0 0 0 0 0 0 0 0 0 0 0	0 1 1 0 1 1 1 1 0 1 0 0
5	0 0 0 0 1 0 0 0 0 0 0 0	1 1 1 1 0 1 0 0 0 1 1 0
10	0 0 0 0 0 0 0 0 0 0 1 0	1 0 0 0 1 1 0 1 1 1 1 0
+	1 0 0 0 1 0 0 0 0 1 0 0	0 0 0 1 0 1 1 0 1 1 0 0

G'	A	I
1	0 1 1 0 1 1 1 1 0 1 0 0	1 0 0 0 0 0 0 0 0 0 0 0
5	1 1 1 1 0 1 0 0 0 1 1 0	0 0 0 0 1 0 0 0 0 0 0 0
10	1 0 0 0 1 1 0 1 1 1 1 0	0 0 0 0 0 0 0 0 0 0 1 0
+	0 0 0 1 0 1 1 0 1 1 0 0	1 0 0 0 1 0 0 0 0 1 0 0

G	I	A
4	0 0 0 1 0 0 0 0 0 0 0 0	0 1 1 1 1 0 1 0 0 0 1 1
6	0 0 0 0 0 1 0 0 0 0 0 0	1 1 1 0 1 0 0 0 1 1 0 1
7	0 0 0 0 0 0 1 0 0 0 0 0	1 1 0 1 0 0 0 1 1 0 1 1
9	0 0 0 0 0 0 0 0 1 0 0 0	0 1 0 0 0 1 1 0 1 1 1 1
10	0 0 0 0 0 0 0 0 0 1 0 0	1 0 0 0 1 1 0 1 1 1 1 0
+	0 0 0 1 0 1 1 0 1 1 0 0	1 0 0 0 1 0 0 0 0 1 0 0

Fig. 2.3 — The Quasi-12 Cyclic Nature of $\mathcal{C}$

2.7 Quasi Cyclicity

Inspection of the matrix U in section 2.3 will convince the reader that the code $\mathcal{C}$ is in fact quasi-12 cyclic. The first twelve rows of U are of the form $G = [I|A]$ and the last twelve rows are of the form $G' = [A|I]$. The first twelve rows generate the code.

For two vectors $\underline{x}_1$ and $\underline{x}_2$ we call the vector resulting from appendage of the components of $\underline{x}_2$ to the end of those in $\underline{x}_1$ the *concatenation* $\underline{x}_1\underline{x}_2$ of $\underline{x}_2$ to $\underline{x}_1$. Let $\underline{c}$ be a combination of rows of G and let $\underline{a}$ and $\underline{b}$ be the vectors consisting first and last twelve components respectively of $\underline{c}$, in the same order that the components appear in $\underline{c}$. Then the same rows from G' combine to give the concatenation $\underline{ba}$ of the vector $\underline{a}$ to the vector $\underline{b}$. The 1's in the first twelve components of a codeword indicate which combination of rows of G is the codeword.

For example in figure 2.3 we can see that the combination $\underline{x} = \underline{ab}$ of rows one, five and ten of G is equal to the twelfth right cyclic shift of the combination of rows one, five and ten of G'. This latter combination is equal to the combination of rows four, six, seven, nine and ten of G.

The row space of G' is contained in the row space of U, and so it is contained in the code $\mathcal{C}$. Thus $\underline{ba}$ is a codeword in $\mathcal{C}$ whenever $\underline{ab}$ is. Therefore the code $\mathcal{C}$ is quasi-12 cyclic, or in other words is quasi cyclic of index two.

Row	$\underline{a}$	$\underline{b}$
1	1 0 0 0 0 0 0 0 0 0 0 0	0 1 1 0 1 1 1 1 0 1 0 0
5	0 0 0 0 1 0 0 0 0 0 0 0	1 1 1 1 0 1 0 0 0 1 1 0
10	0 0 0 0 0 0 0 0 0 0 1 0	1 0 0 0 1 1 0 1 1 1 1 0
+	1 0 0 0 1 0 0 0 0 1 0 0	0 0 0 1 0 1 1 0 1 1 0 0
	weight 3	weight 5

Fig. 2.4 — Rows of the Identity Matrix

2.8 Minimum Distance

As we know, the extended binary Golay code is the only linear block code of length twenty-four, dimension twelve and minimum distance eight [10, p. 401]. Our code $\mathcal{C}$ has so far been shown to be of length twenty-four and dimension twelve. We will now see that $\mathcal{C}$ is of minimum distance eight and therefore it is the extended binary Golay code. In the following arguments we will use many of the properties of the construction that we have already highlighted. First we will consider how the matrix A is related to the minimum distance of the code.

2.8.1 The Matrix A and the Code

The generator matrix G of the code $\mathcal{C}$ is of the form $G = [I|A]$. Every codeword is a combination of rows of G and every combination of rows of G is a codeword. Remember that the minimum distance of a linear block code is equal to the minimum of the weights of its codewords. To show the minimum distance of the code $\mathcal{C}$ is eight, we will show that the weight of every non-zero combination of the rows of G is of weight at least eight.

Now note that the combination of any i rows of a k by k identity matrix is of weight exactly i for i from zero to k. Like in the previous section, let $\underline{a}$ be the vector consisting of the first twelve components of a combination of i rows of G in order and let $\underline{b}$ be the last twelve in order where i is an integer between zero and twelve inclusive. The vector $\underline{a}$ is then a combination of i rows of the identity matrix and so is of weight exactly i. Thus the weight of the combination of the rows of G is i plus the weight of the combination of those rows from A. That is, the weight of the vector $\underline{b}$. This is illustrated with an example in figure 2.4. The weight of the combination of the three rows in the figure is equal to three from the first twelve components plus the weight from the last twelve.

The weight of a combination of rows from G is thus the weight of the combination of those rows from A plus the number of rows involved in the combination. In the next section we use this fact to show that many of the codewords in $\mathcal{C}$ cannot be of weight less than eight.

2.8.2 Four Rows or More

Using the relationship between the weights of the combinations of the rows of G and those of A we can see that there are a large number of combinations of rows of G that are obviously of weight at least eight. Every combination of i rows of G must be of weight at least i for i from zero to twelve. Thus every combination of five or more rows of G is of weight at least five. Now, the code $\mathcal{C}$ is doubly even and so every combination of five or more rows of G must in fact combine to give a codeword of at least weight eight. Hence the only non-zero codewords of $\mathcal{C}$ that could possibly be of weight less than eight are those that are combinations of four or less rows of G.

A four row combination of G being of weight four would imply that those four rows of A are linearly dependent, combining to give the zero vector of length twelve. Earlier in the matrix calculation in section 2.4.1, showing that U^2 was equal to zero, we saw that A^2 was equal to the identity matrix. This implies that A is its own inverse and any matrix that has an inverse is of full rank [17, p. 246]. Hence the rows of A are linearly independent over $\mathbb{Z}_2$ and so no non-zero combination of them is the zero vector. Thus every non-zero combination of four rows of A has non-zero weight. Hence every four row combination of the rows of G is of weight at least eight. We therefore are only left to prove that no three-, two- or one-row combinations of G have weight less than eight. These cases are straightforward to prove.

2.8.3 One and Two Row Combinations

The first row of G is of weight eight and all other rows are permutations of this row. Hence no single row is of weight less than eight. Furthermore we saw in section 2.4.2 that the weight of each two row combination of A is equal to the weight of one of the combinations of row one with rows two to seven. The weight of these combinations is easy to check: rows two to six combine with row one to give combinations of weight six, and the row one and row seven combination is of weight ten. Combining those weights with the weight of two rows from the identity matrix, we see that all of the two row combinations of G are of weight eight or more. Thus the only non-zero combinations of rows of G that could lead to codewords of weight less than eight are those of three rows. We will now prove that none of these three row combinations have weight less than eight.

2.8.4 Three Row Combinations

We use the quasi-12 cyclic property to show that no three row combination of G is of weigh less than eight. The code $\mathcal{C}$ is doubly even. Thus the only possible

weight that a non-zero combination of rows of G can have that is less than eight is four.

Suppose $\underline{c}$ is a weight four combination of three rows of G. Let $\underline{a}$ be the first twelve components of $\underline{c}$ and let $\underline{b}$ be the last twelve. Then $\underline{a}$ is of weight three and $\underline{b}$ is of weight one.

Since $\underline{c} = \underline{ab}$ is a codeword, then so too is the vector $\underline{c}' = \underline{ba}$. The generator matrix G is in standard form and is of rank twelve so the first twelve components of a codeword in the code $\mathcal{C}$ indicate exactly the rows of G that combine to generate that codeword. When the i^{th} component of such a codeword is 1 for i from one to twelve the i^{th} row of G is involved in the combination. The number of non-zero components in these first twelve components is the number of rows of G that combined to generate the codeword. Therefore in the case of $\underline{c}'$ a single row of G forms the codeword. But all of the rows of G are of weight eight, not weight four. Thus we have a contradiction and our original supposition that three rows of G combine to give a codeword of weight four must be incorrect.

So every three row combination of G is at least of weight eight. This concludes the proof that the minimum distance of $\mathcal{C}$ is at least eight. Since the rows of G are all of weight eight and are codewords in themselves the minimum distance of G is exactly eight. We will now discuss the fact that the code is actually an ideal in group ring.

2.9 The Code as an Ideal

We have used the full row space of the group ring matrix U in constructing the code $\mathcal{C}$. In section 1.9.2 we saw that this means that the code is the principal left ideal of u in the group ring. Thus the $(24, 12, 8)$ extended binary Golay code is the principal left ideal of the element $u = 1 + a(b + b^2 + b^4 + b^5 + b^6 + b^7 + b^9)$ in the group ring $\mathbb{Z}_2\mathbf{D}_{24}$.

This concludes the first part of this chapter in which we show that u generates the code. In the second part of this chapter we will show that twenty-three other elements in the group ring also generate the code. We then prove that these are the only elements of their form that generate the code. We start by discussing the twenty-three zero divisors.

2.10 The Other Generators

In the next few sections we will see first that the other twenty-three zero divisors listed in section 2.2 also generate the $(24, 12, 8)$ extended binary Golay code. We do this by showing that they generate equivalent codes to that generated by

$u = 1 + a\mathbf{f} = 1 + a\mathbf{f} = a(b + b^2 + b^4 + b^5 + b^6 + b^7 + b^9)$, which we have just dealt with. The other generators are $1 + ab^i\mathbf{f}$ for i from one to eleven and $1 + ab^j\mathbf{f}^{\mathrm{T}}$ for j from zero to eleven. We first deal with the former type in the next section, followed by the latter type in the section after that.

2.10.1 Those without the Transpose

We deal now with the generating elements of the form $1 + ab^i\mathbf{f}$ for i from one to eleven. The fact that $u^2 = (1 + a\mathbf{f})^2$ is equal to zero implies that $u_i = (1 + ab^i\mathbf{f})^2$ is also equal to zero for all i. Working through the multiplication:

$$\begin{aligned}(1 + ab^i\mathbf{f})^2 &= 1 + 2(ab^i\mathbf{f}) + (ab^i\mathbf{f})^2 \\ &= 1 + 0 + (ab^i\mathbf{f})^2 \\ &= 1 + ab^i\mathbf{f}ab^i\mathbf{f} \\ &= 1 + ab^ia\mathbf{f}^{\mathrm{T}}b^i\mathbf{f} \\ &= 1 + ab^iab^i\mathbf{f}^{\mathrm{T}}\mathbf{f} \\ &= 1 + \mathbf{f}^{\mathrm{T}}\mathbf{f}.\end{aligned}$$

In section 2.4.1 we proved that $\mathbf{f}^{\mathrm{T}}\mathbf{f}$ is equal to 1 and so $(1 + ab^i\mathbf{f})^2$ is zero for i from one to eleven. Thus the maximum rank of the group ring matrix U_i of u_i is twelve.

Notice that, just like in u's case, the group ring matrix U_i is of the form:

$$\left[\begin{array}{c|c} I & A_i \\ \hline A_i & I \end{array}\right]$$

where I is the twelve by twelve identity matrix and A_i is a twelve by twelve reverse circulant matrix. Thus the rank of U_i is exactly twelve and the first twelve rows of it generate its row space. Here we are still using the listing $\{1, b, b^2, \ldots, b^{11}, a, ab, ab^2, \ldots, ab^{11}\}$ of $\mathbf{D}_{24}$.

The components of the first row of A_i are the coefficients in u_i of the elements ab^j for j from zero to eleven written in order. The other rows of A_i are determined by this first row since A_i is reverse circulant. Multiplying $\mathbf{f}$ by a power of b simply cycles the first row of A. This has the effect of cycling A's columns. Thus A_i is the matrix resulting from cycling the columns of A i times. Hence the row space of the group ring matrix U_i is generated by a matrix $G_i = [I|A_i]$ that is a column permutation of the generator matrix $G = [I|A]$ of the group ring code $\mathcal{C}$ from section 2.3.

Thus the code that is the row space of the group ring matrix of any element $u_i = 1 + ab^i\mathbf{f}$ for i from one to eleven is equivalent to the code $\mathcal{C}$. Therefore it

is the extended binary Golay code. Notice that we can easily adapt the above proof to prove that any element of the form $1 + ab^k\mathbf{h}$ generates an equivalent code to that of $1 + a\mathbf{h}$ where $\mathbf{h}$ is an arbitrary sum of powers of b for k from one to eleven, so long as $\mathbf{h}^2$ is equal to one. We will use such an adaptation of the proof in section 2.13. We now move on to those elements of the form $1 + ab^j\mathbf{f}^{\mathrm{T}}$ for j from zero to eleven.

2.10.2 Those with the Transpose

In this section we turn our attention to the elements of the form $1 + ab^j\mathbf{f}^{\mathrm{T}}$ for j from zero to twelve. Suppose $1 + a\mathbf{f}^{\mathrm{T}}$ does generate the extended binary Golay code. The argument in the previous section showing that $1 + ab^i\mathbf{f}$ generates an equivalent code to $1 + a\mathbf{f}$ will also show that elements of the form $1 + ab^j\mathbf{f}^{\mathrm{T}}$ generate an equivalent code to $1 + ab^j\mathbf{f}^{\mathrm{T}}$. The only necessary change to the argument is to substitute $\mathbf{f}^{\mathrm{T}}$ for every $\mathbf{f}$. Thus we only need show that $1 + a\mathbf{f}^{\mathrm{T}}$ generates an equivalent code to $u = 1 + a\mathbf{f}$.

The fact that u^2 equals zero again implies that $(1 + a\mathbf{f}^{\mathrm{T}})^2$ is also equal to zero:

$$\begin{aligned}(1 + a\mathbf{f}^{\mathrm{T}})^2 &= 1 + 2(a\mathbf{f}^{\mathrm{T}}) + (a\mathbf{f}^{\mathrm{T}})^2\\ &= 1 + (a\mathbf{f}^{\mathrm{T}})^2\\ &= 1 + a\mathbf{f}^{\mathrm{T}}a\mathbf{f}^{\mathrm{T}}\\ &= 1 + aa\mathbf{f}\mathbf{f}^{\mathrm{T}}\\ &= 1 + \mathbf{f}\mathbf{f}^{\mathrm{T}}\\ &= 1 + \mathbf{f}^{\mathrm{T}}\mathbf{f}.\end{aligned}$$

Thus $1 + a\mathbf{f}^{\mathrm{T}}$ generates a code of dimension twelve and the first twelve rows of its group ring matrix generate the code.

This generator matrix is of the form $[I|B]$ where B is the twelve by twelve matrix on the right-hand side of figure 2.5. The matrix on the left-hand side of the figure is the matrix A in the generator matrix $G = [I|A]$ of the code $\mathcal{C}$ generated by u. They have been placed side by side for comparison.

In the following we will show that the codes generated by $[I|A]$ and $[I|B]$ are equivalent. We do this by showing that A can be constructed from B by row and column permutations. Any matrix formed by a permutation of the rows of G generates the same code. A matrix formed by a column permutation of A will, on being appended to the identity matrix, generate an equivalent code to $\mathcal{C}$. Thus the result will show that $1 + a\mathbf{f}^{\mathrm{T}}$ generates the extended binary Golay code.

We start with the matrix B. The first permutation we apply is a row

$$\begin{bmatrix}
0&1&1&0&1&1&1&1&0&1&0&0\\
1&1&0&1&1&1&1&0&1&0&0&0\\
1&0&1&1&1&1&0&1&0&0&0&1\\
0&1&1&1&1&0&1&0&0&0&1&1\\
1&1&1&1&0&1&0&0&0&1&1&0\\
1&1&1&0&1&0&0&0&1&1&0&1\\
1&1&0&1&0&0&0&1&1&0&1&1\\
1&0&1&0&0&0&1&1&0&1&1&1\\
0&1&0&0&0&1&1&0&1&1&1&1\\
1&0&0&0&1&1&0&1&1&1&1&0\\
0&0&0&1&1&0&1&1&1&1&0&1\\
0&0&1&1&0&1&1&1&1&0&1&0
\end{bmatrix}
\qquad
\begin{bmatrix}
0&0&0&1&0&1&1&1&1&0&1&1\\
0&0&1&0&1&1&1&1&0&1&1&0\\
0&1&0&1&1&1&1&0&1&1&0&0\\
1&0&1&1&1&1&0&1&1&0&0&0\\
0&1&1&1&1&0&1&1&0&0&0&1\\
1&1&1&1&0&1&1&0&0&0&1&0\\
1&1&1&0&1&1&0&0&0&1&0&1\\
1&1&0&1&1&0&0&0&1&0&1&1\\
1&0&1&1&0&0&0&1&0&1&1&1\\
0&1&1&0&0&0&1&0&1&1&1&1\\
1&1&0&0&0&1&0&1&1&1&1&0\\
1&0&0&0&1&0&1&1&1&1&0&1
\end{bmatrix}$$

Fig. 2.5 — The Matrix A on the left and the matrix B on the right.

$$\begin{bmatrix}
1&0&0&0&1&0&1&1&1&1&0&1\\
1&1&0&0&0&1&0&1&1&1&1&0\\
0&1&1&0&0&0&1&0&1&1&1&1\\
1&0&1&1&0&0&0&1&0&1&1&1\\
1&1&0&1&1&0&0&0&1&0&1&1\\
1&1&1&0&1&1&0&0&0&1&0&1\\
1&1&1&1&0&1&1&0&0&0&1&0\\
0&1&1&1&1&0&1&1&0&0&0&1\\
1&0&1&1&1&1&0&1&1&0&0&0\\
0&1&0&1&1&1&1&0&1&1&0&0\\
0&0&1&0&1&1&1&1&0&1&1&0\\
0&0&0&1&0&1&1&1&1&0&1&1
\end{bmatrix}
\qquad
\begin{bmatrix}
1&0&1&1&1&1&0&1&0&0&0&1\\
0&1&1&1&1&0&1&0&0&0&1&1\\
1&1&1&1&0&1&0&0&0&1&1&0\\
1&1&1&0&1&0&0&0&1&1&0&1\\
1&1&0&1&0&0&0&1&1&0&1&1\\
1&0&1&0&0&0&1&1&0&1&1&1\\
0&1&0&0&0&1&1&0&1&1&1&1\\
1&0&0&0&1&1&0&1&1&1&1&0\\
0&0&0&1&1&0&1&1&1&1&0&1\\
0&0&1&1&0&1&1&1&1&0&1&0\\
0&1&1&0&1&1&1&1&0&1&0&0\\
1&1&0&1&1&1&1&0&1&0&0&0
\end{bmatrix}$$

Fig. 2.6 — Column and row permutations of B showing code equivalence.

permutation where the first and last, the second and second-last, the third and third-last, and so on, rows are interchanged. The result is the matrix on the left-hand side of figure 2.6. The second permutation we apply is the similar column permutation where the first and last, the second and second-last, the third and third-last, and so on, columns are interchanged. The resulting matrix is that on the right-hand side of the figure. The final permutation is a column permutation in which the columns are cycled two steps to the right. The result is the matrix A on the left-hand side of the previous figure 2.5.

The matrix B is thus a combination of row and column permutations of the matrix A. The group ring element $1 + a\mathbf{f}^{\mathrm{T}}$ therefore generates the extended binary Golay code. As a consequence so do the elements $1 + ab^j\mathbf{f}^{\mathrm{T}}$ for j from one to eleven.

This concludes the proof the elements $1 + ab^i\mathbf{f}$ for i from one to eleven and $1 + ab^j\mathbf{f}^{\mathrm{T}}$ for j from zero to eleven generate the extended binary Golay code

Components	1	2	3	4	5	6	7	8	9	10	11	12
Row 1	0	1	1	0	1	1	1	1	0	1	0	0
Row 7	1	1	0	1	0	0	0	1	1	0	1	1

Fig. 2.7 — Rows one and seven share components two and eight.

along with u. We will now discuss why these twenty-four group ring elements are capable of generating the code, while the others of the form $1 + a\mathbf{f}'$ are not.

2.11 The Only Zero Divisors

The computer search we conducted in our initial analysis of the extend binary Golay code as a group ring code found only the twenty-four zero divisors in the last section to generate the code. The computer only searched for zero divisors of the form $1 + a\mathbf{h}$ where $\mathbf{h}$ is a sum of powers of b. Having algebraically proven that these elements did in fact generate the code, we turned our attention to the investigation of why they generate the code. The hope was that this would offer insight allowing the construction of longer type II codes. The result was the following proof that the twenty-four elements from the last section are the only ones of the form $1 + a\mathbf{h}$ that do generate the code. In the next section we highlight two properties that together are unique to the twenty-four elements.

2.11.1 Combinations of Two Rows

Consider the matrix A in figure 2.1. In section 2.8.3 we listed the weights of the combinations of row one and each of rows two to seven of A. The combinations of row one with each of rows two to six are of weight six. This implies that the combinations of row one with each of rows eight to twelve are also of weight six, as was shown in section 2.4.2. The combination of rows one and seven is of weight ten. In total for the eleven two-row combinations of A involving row one, ten are of weight six and one is of weight ten.

Each row of A is of weight seven. In combining two rows we lose one from each of the two weights of seven every time both rows contain a 1 in the same component. We say that two rows 'share' a 1-component whenever they both contain a 1 in that component. This is illustrated in the example in figure 2.7. Rows one and seven of A share 1-components in components two and eight. We say the 1 from one row 'cancels' the 1 in the same component in their combination since the sum of two 1's is 0. This terminology helps in the following argument that $\mathbf{h}$ in the generator $1 + a\mathbf{h}$ must be of weight seven to lead to the generation of the extended binary Golay code.

Only Weight Seven

Let $\mathbf{h}$ be a sum of powers of the generator b of $\mathbf{D}_{24}$. The extended binary Golay code is doubly even. The rows of any generator matrix of the code must thus have weights divisible by four. For an element of the form $1 + a\mathbf{h}$ to generate the code, $\mathbf{h}$ must thus be of weight congruent to three modulo four. The possible weights of $\mathbf{h}$ are thus three, seven and eleven. There are only twelve group elements involved in $\mathbf{h}$ and thus it cannot have any higher weight.

The minimum distance of the extended binary Golay code is eight. The minimum distance of any code generated by an element in which $\mathbf{h}$ is of weight three is at most four. The generator of the code is a codeword itself and it has weight four. Were $\mathbf{h}$ to have weight eleven then the combination of row one and two of the group ring matrix of $1 + a\mathbf{h}$ would have weight four. So again the minimum distance of the code would be at most four.

The only possible weight of $\mathbf{h}$ is therefore seven. When $\mathbf{h}$ is of weight seven, the group ring element $1 + a\mathbf{h}$ is of weight eight. All of the twenty-four generators in section 2.10 are of weight eight. This property along with another elucidated in the next section are together unique in the group ring to the twenty-four zero divisors listed in section 2.2.

Shared 1-Components

Since the combinations of row one of A with each of the rows two to six and eight to twelve are of weight six, those rows each share four 1-components with row one. Row seven shares only two with row one. This is the second property that makes the twenty-four weight eight zero divisors unique in the group ring. They all have ten of the other rows sharing four 1-components with row one and one row sharing two with row one.

We saw in section 2.4.1 that u^2 is only equal to zero if the rows of A are orthogonal. They are only orthogonal if each pair of rows of A shares an even number of 1-components. This argument can be extended to any element of the form $1 + a\mathbf{h}$ in $\mathbb{Z}_2\mathbf{D}_{24}$. Such an element, according to the listing $\mathbf{D}_{24} = \{1, b, \ldots, b^{11}, a, ab, \ldots, ab^{11}\}$ has a group ring matrix of the form:

$$\left[\begin{array}{c|c} I & B \\ \hline B & I \end{array}\right]$$

where I and B are twelve by twelve matrices. The matrix B is reverse circulant, just like in the case of u in section 2.3. The element is only a zero divisor with itself when each of B's rows shares an even number of components with row one of B.

Thus row one of such a B must share either zero, two, four, six, eight or ten 1-components with each of the other rows. Two rows of B must share at least one 1-component as B has only twelve columns and each row is of weight seven. Two rows of weight seven can share a maximum of seven components. Should two rows share six 1's then the weight of the combination of those two rows would be four. Thus the code that is the row space of the group ring matrix of $1 + a\mathbf{h}$ is only of minimum distance eight if each of the rows two to twelve of B shares either two or four 1-components with the first row.

The total number of 1-components the other rows of B share with row one is forty-two. This is exactly the product of seven, the weight of $\mathbf{h}$, and six. The correspondence is due to B's reverse circulant nature. Each of the 1's in the first row cancels each of the other 1's in the row exactly once as we move down through the rows of the matrix.

Thus the only way for eleven rows to provide forty two cancellations is if one of them provides two cancellations and the other provide four each. The one that provides two must be the seventh row. If one of the rows two to six provided only two then so would one of the rows eight to twelve. Since only one row can provide exactly two, it must be row seven. So only generators of the form $1 + a\mathbf{h}$ where $\mathbf{h}$ is of weight seven and all of the rows two to six of B share four 1-components and row seven shares two, can generate the extended binary Golay code. We will see in a moment that only the twenty-four zero divisors we have listed in section 2.10 have these properties. First we will discuss the shared 1-components from the group ring perspective.

2.12 The Multiset of Differences

In this section we look from the group ring perspective at the 1-components shared between the first row of B and the other rows. The correspondence between these sharings and the elements of b with non-zero coefficient in $\mathbf{h}$ is interesting. We show that their 'multiset of differences', as defined below, has an interesting structure. The notation used here is the same as in the last few sections—we are looking at the situations in which an element $1 + a\mathbf{h}$ can generate the extended binary Golay code. The B matrix is as defined in section 2.11.1: it is the reverse circulant submatrix in the top-right of the group ring matrix of $1 + a\mathbf{h}$. As always in this chapter, we are using the listing $\{1, b, \ldots, b^{11}, a, ab, \ldots, ab^{11}\}$ of $\mathbf{D}_{24}$.

Row $i + 1$ of the group ring matrix is the vector form of the group ring codeword $g_{i+1}(1 + a\mathbf{h})$ where g_{i+1} is the $(i+1)^{\text{th}}$ element of the listing. This was discussed in section 1.9.2. Thus row $i + 1$ of the group ring matrix corresponds to the group ring element $b^i u = b^i(1 + a\mathbf{h}) = b^i + a(b^{-i}\mathbf{h})$ for i an integer from

zero to eleven. Row $i+1$ of the matrix B has a 1 in the $(j+1)^{\text{th}}$ component when $b^{-i}b^k = b^j$ where b^k has a non-zero coefficient in $\mathbf{h}$. The 1's in rows two to twelve are in the same components that row one has 1's when $b^j = b^l$ where b^l is some power of b in $\mathbf{h}$ with non-zero coefficient. As we saw in the last section, $\mathbf{h}$ must be of weight seven in order for $1 + a\mathbf{h}$ to generate the extended binary Golay code. Thus rows two to twelve of B have a total of eleven times seven 1's, forty-two of which are shared with row one's 1-components. Row one and row $(i+1)$ therefore share a 1-component whenever $b^{-i}b^k = b^l$, or $b^i = b^{k-l}$, where b^k and b^l are powers of b with non-zero coefficients in $\mathbf{h}$.

The integer k never equals l as the same 1-component passes through all the of the columns while moving down through the matrix B and thus never cancels with itself. Therefore the set $\{b^{k-l} \mid b^k, b^l \in \mathbf{f}, k \neq l\}$, where by "$\in$" we mean 'has non-zero coefficient in', is a set of powers of b that describes exactly when the 1's from row one cancel with the 1's from the other rows. We will call this set *the multiset of differences* and denote it $\mathcal{D}$. The number of times this set contains b^i is the number of 1-components that the $(i+1)^{\text{th}}$ row cancels from the first row.

As an example of a multiset of differences, we'll calculate that pertaining to the extended binary Golay code generator element $\mathbf{f}$ in $u = 1 + a\mathbf{f}$ from section 2.2. The element $\mathbf{f}$ is thus $\mathbf{f} = b + b^2 + b^4 + b^5 + b^6 + b^7 + b^9$. The multiset of differences is given in figure 2.8. These calculations support our earlier assertion that rows two to six and rows eight to twelve share four 1-components in common with row one and row seven shares two with it. We say the multiset of differences $\mathcal{D}$ has the form $(\mathbf{10} \times 4) + (\mathbf{1} \times 2)$ meaning ten elements appear in it four times and one element appears twice.

The element b^{l-k} is a member of $\mathcal{D}$ whenever b^{k-l} is. The elements b^{k-l} and b^{l-k} are inverses of each other and so the appearance of an element implies its inverse. Suppose we calculate the elements of the set $\mathcal{D}' = \{b^{k-l} \mid b^k, b^l \in \mathbf{f}, k > l\}$ where k is greater than l. Then we can calculate the number of times each element appears in $\mathcal{D}$ by simply adding the number of times it appears in $\mathcal{D}'$ to the number of times its inverse appears in $\mathcal{D}'$.

In the remainder of this chapter we will show that the only elements of the form $1 + a\mathbf{h}$ that can generate the extended binary Golay code are those in which $\mathbf{h}$ is of weight seven and has a multiset of differences of the form $(\mathbf{10} \times 4) + (\mathbf{1} \times 2)$.

2.13 Possible Sets of Differences

In section 2.11.1 we proved that a zero divisor of the form $1 + a\mathbf{h}$ where $\mathbf{h}$ is a sum of powers of b can generate the extended binary Golay code only if $\mathbf{h}$ is of weight seven. Furthermore in section 2.11.1 we showed that row

$$\begin{array}{lllllll}
\mathcal{D} = \{ & b^{1-2}, & b^{1-4}, & b^{1-5}, & b^{1-6}, & b^{1-7}, & b^{1-9}, \\
& b^{2-1}, & b^{2-4}, & b^{2-5}, & b^{2-6}, & b^{2-7}, & b^{2-9}, \\
& b^{4-1}, & b^{4-2}, & b^{4-5}, & b^{4-6}, & b^{4-7}, & b^{4-9}, \\
& b^{5-1}, & b^{5-2}, & b^{5-4}, & b^{5-6}, & b^{5-7}, & b^{5-9}, \\
& b^{6-1}, & b^{6-2}, & b^{6-4}, & b^{6-5}, & b^{6-7}, & b^{6-9}, \\
& b^{7-1}, & b^{7-2}, & b^{7-4}, & b^{7-5}, & b^{7-6}, & b^{7-9}, \\
& b^{9-1}, & b^{9-2}, & b^{9-4}, & b^{9-5}, & b^{9-6}, & b^{9-7} \quad \}
\end{array}$$

$$\begin{array}{lllllll}
\Rightarrow \mathcal{D} = \{ & b^{11}, & b^{9}, & b^{8}, & b^{7}, & b^{6}, & b^{4}, \\
& b^{1}, & b^{10}, & b^{9}, & b^{8}, & b^{7}, & b^{5}, \\
& b^{3}, & b^{2}, & b^{11}, & b^{10}, & b^{9}, & b^{7}, \\
& b^{4}, & b^{3}, & b^{1}, & b^{11}, & b^{10}, & b^{8}, \\
& b^{5}, & b^{4}, & b^{2}, & b^{1}, & b^{11}, & b^{9}, \\
& b^{6}, & b^{5}, & b^{3}, & b^{2}, & b^{1}, & b^{10}, \\
& b^{8}, & b^{7}, & b^{5}, & b^{4}, & b^{3}, & b^{2} \quad \}
\end{array}$$

$$\begin{array}{llllll}
\Rightarrow \mathcal{D} = \{ & b^{1}, & b^{1}, & b^{1}, & b^{1}, & \\
& b^{2}, & b^{2}, & b^{2}, & b^{2}, & \\
& b^{3}, & b^{3}, & b^{3}, & b^{3}, & \\
& b^{4}, & b^{4}, & b^{4}, & b^{4}, & \\
& b^{5}, & b^{5}, & b^{5}, & b^{5}, & \\
& b^{6}, & b^{6}, & & & \\
& b^{7}, & b^{7}, & b^{7}, & b^{7}, & \\
& b^{8}, & b^{8}, & b^{8}, & b^{8}, & \\
& b^{9}, & b^{9}, & b^{9}, & b^{9}, & \\
& b^{10}, & b^{10}, & b^{10}, & b^{10}, & \\
& b^{11}, & b^{11}, & b^{11}, & b^{11} \quad \}
\end{array}$$

Fig. 2.8 — The multiset of differences of $\mathbf{f}$.

Row One:	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}
Row Five:	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	x_1	x_2	x_3	x_4
Row Nine:	x_9	x_{10}	x_{11}	x_{12}	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8

Fig. 2.9 — The combination of rows one, five and nine.

seven in the B submatrix of the group ring matrix of $1 + a\mathbf{h}$ must share two 1-components with row one, and each of the other rows must share four. We now prove that the twenty-four zero divisors listed in section 2.10 are the only ones of the form $1 + a\mathbf{h}$ with these properties. The zero divisors listed there are $u = 1 + a\mathbf{f} = a(b + b^2 + b^4 + b^5 + b^6 + b^7 + b^9)$, $1 + ab^i\mathbf{f}$ for i an integer from one to eleven and $1 + ab^j\mathbf{f}^{\mathrm{T}}$ for an integer j from zero to eleven. We start by discussing the combination of rows one, five and nine of such a B. This combination is interesting because row one is four cycles from row five, which is four cycles from row nine, which is four cycles from row one. The matrix B only contains twelve rows.

The Combination of Rows One, Five and Nine

The combination of rows one, five and nine of B in the group ring matrix of $1 + a\mathbf{h}$ has an interesting property. The rows of the combination are evenly spaced throughout B. Cycling the three rows four times means the first becomes the fifth row, the fifth row becomes the ninth and the ninth becomes the first. The first four components of the combination are thus equal to the second four, which are equal to the last four in the same order. This is illustrated in figure 2.9, where the i^{th} component of row one of B is labelled by x_i. This implies that the weight of the combination is a multiple of three. The possible weights of the combination are thus three, six, nine and twelve.

The combination must also be of weight congruent to one modulo four. This is due to the fact that the extended binary Golay code is doubly even and thus every combination of i rows of B must be of weight congruent to $(4 - i)$ modulo four in order to facilitate the code's generation. The only possibility for the weight of the combination of rows one, five and nine of B is thus nine. The first four components of the combination must then be a subvector of weight three, consisting of three 1-components and a single 0-component. In the next section we show that exactly one of the 1-components must arise from the combination of three 1-components in the three-row combination.

x_1	x_2	x_3	x_4
x_5	x_6	x_7	x_8
x_9	x_{10}	x_{11}	x_{12}

Fig. 2.10 — The array of the first four components.

The First Four Components

The first four components in the combination of rows one, five and nine of B are the column sums of the array in figure 2.10. We've seen that three of these column sums are 1 and one is 0. We will now show that this arises from a single combination of three 1-components, two combinations of a single 1-component with two 0-components and a single combination of two 1-components and a 0-component. Note that the entries in the array are the components of the first row of B in order moving across the rows and from top to bottom.

Every column of three 1-components in the array leads to the sharing of three 1-components between row one and row five of B. Suppose the first column of the array is such a column. Examining figure 2.9, in which the first two rows are rows one and five of B, convinces us that the first, fifth and ninth components of those two rows will then both contain 1-components. This is true since those components of the combination are the sum of two of the components in the first column of the array in figure 2.10. Were column two of the array to contain all 1-components then components two, six and ten of those two rows would both contain 1-components, and so on. In section 2.11.1 we proved that rows one and five must share exactly four 1-components. Thus there is at most one column of the array in figure 2.10 that contains all 1-components.

Now we will show that there must be at least one column of the array containing all 1-components. Three of the column sums of the array must be 1-components. Seven of the twelve components in the first row of B must be 1-components in the first row of B. These twelve components make up the entries of the array. If there is no all 1-component column then three of the columns would have to contain exactly two 1-components and the other would have to contain exactly one. This would mean there were three 0 column sums and a single 1 column sum. Thus the array contains at least one, and so exactly one, column of all 1-components. We can assume without loss of generality that this is the first column of the array, a fact we discuss in the following section.

The First Column

In the previous section we showed that exactly one of the columns in the array in figure 2.10 contains all 1-components. In section 2.10.1 we proved that the

Row One:	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}
Row Seven:	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	x_1	x_2	x_3	x_4	x_5	x_6

Fig. 2.11 — The combination of rows one and seven.

elements of the form $1 + ab^i\mathbf{h}$ for i an integer from one to eleven generate the same code as the element $1 + a\mathbf{h}$ when $\mathbf{h}^{\mathrm{T}}\mathbf{h}$ equals one. Here we are assuming that $(1 + a\mathbf{h})^2$ is zero and so $\mathbf{h}^{\mathrm{T}}\mathbf{h}$ must be one.

The proof relied on the fact that the multiplication of $\mathbf{h}$ by b^i has the effect of cycling the first row and hence the columns of B. Cycling the first row of B has the effect of cycling the columns in the array in figure 2.10. Note that as a column is wrapped from left to right the elements within get permuted, but that will not affect the following arguments. Thus we can assume without loss of generality that the column of the array containing all 1-components is the first column.

In section 2.13 we showed that the other three columns of the array are one that contains exactly two 1-components and two that contain exactly one 1-component. We will now see that, when the first column of the array contains all 1-components, the column containing two 1-components cannot be the third column of the array.

The Third Column

The first column of the array in figure 2.10 contains all 1-components. Every 1-component in the third column thus contributes two 1-component cancellations in the combination of rows one and seven of B. This is evident in figure 2.11. The 1-components in the first column of the array are in components x_1, x_5 and x_9. When x_7 is a 1-component then, in figure 2.11, it cancels in columns one and seven the 1-component denoted x_1. When x_3 is, it cancels in columns three and nine the 1-component denoted x_9 . When x_{11} is, it cancels in columns five and eleven of the 1-component denoted x_5.

Thus every 1-component in column three contributes two to the number of 1-components shared between rows one and seven of B. In section 2.11.1 we showed that rows one and seven must share exactly two 1-components in order for B to lead to the generation of the extended binary Golay code. The third column of the array can therefore harbour only one 1-component. Since the column is either a one or a two 1-component containing column, it must contain exactly one 1-component. Of course we have not stipulated which of the three components in the third column is that 1-component. We will work through each of the three possibilities in a moment. First we discuss the second and

fourth columns of the array.

The Second and Fourth Columns

One of columns two and four of the array in figure 2.10 contains two 1-components and the other contains one. In a moment we will see that in both cases we will find an extended binary Golay code generating element. First we discuss the fact that the positioning of the 1-component in the column containing one 1-component determines the positioning of the 0-component in the two 1-component containing column.

Whether the one 1-component containing column is the second or the fourth column of the array we can assume, again without loss of generality, that the single 1-component in that column is the top-most component in the column. Cycling the elements of the first row of B four times will permute the rows of the array so that the first row becomes the second, the second becomes the third and the third becomes the first. The column sums remain unaffected. The cycling will also permute the components within the columns of B, but as discussed in section 2.13, the matrix after cycling will lead to the generation of the code if and only if the matrix did before the cycling. Once the position of the 1-component in that column has been decided, there is only one positioning of the two 1-components in the other column that can occur.

Some of the components in the second and fourth columns can lead to shared 1-components between the first and seventh rows of B, just as in the situation with the first and third columns of the array. We have already reached our maximum number of such shared components and thus we need to ensure that no such sharings arise from the second and fourth columns. Considering figure 2.11 we can identify the components that lead to such sharings.

The components in the second column of the array are x_2, x_6 and x_{10} and those in column four are x_4, x_8 and x_{12}. First we take the case in which the one 1-component column is the second. The component x_2 of the array is then the 1-component. In that case if the component x_8 is a 1-component then rows one and seven share two extra 1-components in columns two and eight in figure 2.11. Thus x_8 must be a 0-component and x_4 and x_{12} must both be 1-components.

Second we take the case in which the column containing a single 1-component is the fourth. The component x_4 is then the 1-component in that column. In that case if the component x_{10} is a 1-component then rows one and seven share two extra 1-components in columns four and ten of figure 2.11. Thus x_{10} must be a 0-component and x_2 and x_6 must both be 1-components.

We are then only left with six possibilities to analyse, three from each of the two cases just discussed. The three possibilities in each case are: that in

1	1	x_3	1
1	0	x_7	0
1	0	x_{11}	1

Fig. 2.12 — The array in the first case.

$x_3 = 1$	1	1	1	1	1	0	0	0	1	0	0	1
$x_7 = 1$	1	1	0	1	1	0	1	0	1	0	0	1
$x_{11} = 1$	1	1	0	1	1	0	0	0	1	0	1	1

Fig. 2.13 — The first rows of B in the first case.

which the 1-component in column three of the array is x_3, that in which the component is x_7 and that in which it is x_{11}. We take each of the two cases in turn, going quickly through the three possibilities in each.

The First Case

In the first case the array has the form displayed in figure 2.12. One of the components x_3, x_7 and x_{11} is a 1-component. When it is x_3 the first row of B is the first row displayed to the right of the double vertical lines in figure 2.13. In that situation rows one and two (which is the first cycle of row one) would share five 1-components. They are only allowed share exactly four.

When the 1-component is x_7 then the first row of B is the second row in figure 2.13. In that situation rows one and two of B would share only three 1-components. When x_{11} is the 1-component the first row of B is then the third row in figure 2.13. This is the first row of the matrix B corresponding to that of the group ring element $1 + ab^5\mathbf{f}^{\mathrm{T}}$, one of generators listed in section 2.10. Thus only in the situation that x_{11} is the 1-component will B lead to the generation of the extended binary Golay code, and that situation corresponds to on of the twenty-four zero divisors. We now move on to the second case.

The Second Case

In the second case the array has the form given in figure 2.14. Again in this case, exactly one of x_3, x_7 and x_{11} is a 1-component. When it is x_3 the first row of B is the first row displayed to the right of the double vertical lines in figure 2.15. In that situation rows one and two (which is the first cycle of row one) would share five 1-components. Again, they are only allowed share exactly four.

When the 1-component is x_{11} then the first row of B is the third row in

1	1	x_3	1
1	1	x_7	0
1	0	x_{11}	0

Fig. 2.14 — The array in the second case.

$x_3 = 1$	1	1	1	1	1	1	0	0	1	0	0	0
$x_7 = 1$	1	1	0	1	1	1	0	0	1	0	1	0
$x_{11} = 1$	1	1	0	1	1	1	1	0	1	0	0	0

Fig. 2.15 — The first rows of B in the second case.

figure 2.15. In that situation rows one and two of B would share only three 1-components. When x_7 is the 1-component the first row of B is then the second row in figure 2.15. This is the first row of the matrix B corresponding to that of the group ring element $1 + ab^{11}\mathbf{f}$, one of generators listed in section 2.10. Thus in case two, only in the situation that x_7 is the 1-component will B lead to the generation of the extended binary Golay code, and that situation corresponds to on of the twenty-four zero divisors

Interestingly (but perhaps unsurprisingly), case one and case two as above are connected. Consider again the array in figure 2.10. These are the coefficients of the group ring element $a\mathbf{h}$ written according to the last twelve elements of the listing $\{1, b, \ldots, b^{11}, a, ab, \ldots, ab^{11}\}$ of $\mathbf{D}_{24}$. Transposing the group ring element $\mathbf{h}$ has the effect of switching the coefficients of the elements so that they become associated with the inverse of their corresponding group elements.

The component x_i of the array is the coefficient of b^{i-1} in $\mathbf{h}$ for i from one to twelve. Hence after transposing, the component x_i is in the former place of $x_{(12-(i-1)+1)}$, or x_{14-i} where the subscript indices are calculated modulo twelve. Thus the array becomes that in figure 2.16. Columns one and three of the array have stayed put, albeit with their entries permuted. Columns two and four have become interchanged however, again with their entries permuted. The distinction between case one and two was the placement of the column with two 1-components. In case one it was column four and in case two it was column two. Thus the two cases are somewhat related. This concludes the proof that the zero divisors listed in section 2.10 are the only extended binary Golay code generators of their form in $\mathbb{Z}_2\mathbf{D}_{24}$, drawing us to the conclusion of the chapter.

x_1	x_{12}	x_{11}	x_{10}
x_9	x_8	x_7	x_6
x_5	x_4	x_3	x_2

Fig. 2.16 — The transposed array.

Conclusion

In this chapter we have seen that the extended binary Golay code can be constructed as the principal ideal of twenty-four different zero divisors in the group ring $\mathbb{Z}_2\mathbf{D}_{24}$. The zero divisors can be used to construct generator matrices that generate quasi cyclic forms of the code. Furthermore we explored some techniques that will aid us in the analysis of longer codes that are like the extended binary Golay code. In the process it was proven that the twenty-four zero divisors given are the only ones of their specific form that generate the code in the group ring.

In the next chapter we discuss a code that is twice as long, the $(48, 24, 12)$ type II extremal code. We use many similar methods to those used in this chapter in its construction. In particular we exploit a very similar technique to that in the last few sections where we analyse the combination of three rows spaced evenly throughout a submatrix of the group ring matrix. We use this to prove that the code constructed is in fact the $(48, 24, 12)$ type II code.

Chapter 3

The $(48, 24, 12)$ Code

In the previous chapter we constructed the $(24, 12, 8)$ extended binary Golay code. The code is the first in the series of extremal type II codes of length a multiple of twenty-four. As discussed in chapter 1, a type II code is a binary, self-dual and doubly even code. Such a code is called extremal if its minimum distance is $4\lfloor n/24 \rfloor + 4$ where n is the code's length. Of all of the extremal type II codes the ones whose length is a multiple of twenty-four achieve the best minimum distance compared to their length.

For a given length that is a multiple of twenty-four, an extremal type II code may or may not exist. As we've seen in the last chapter an extremal $(24, 12, 8)$ type II code does exist, in the form of the extended binary Golay code. It has been shown to be the unique such code up to equivalence. In this chapter we will see that a $(48, 24, 12)$ type II code also exists. It is also the unique such code up to equivalence [7].

We construct the $(48, 24, 12)$ type II code in this chapter as the principal left ideal of a zero divisor in a dihedral group ring. The construction yields straight-forward algebraic proofs of the code being self-dual, doubly even and of dimension twenty-four. Furthermore the code as constructed is easily seen to be quasi-cyclic of index two, and a generator matrix given is of reverse circulant generator matrix form. The code is constructed in much the same way as the extended binary Golay code in the previous chapter.

The minimum distance of the code is algebraically proven. This shows that the constructed code is the $(48, 24, 12)$ type II code [7]. Evaluating the minimum distance is a difficult task, much more so than the algebraic proof of the minimum distance of the Golay code in the previous chapter. The difficulty arises primarily due to the greater minimum distance of the code.

It is further compounded by the number of codewords in the code. The number of codewords in the extended binary Golay code is two to the power

of twelve, or four thousand and ninety-six. The $(48, 24, 12)$ type II code, on the other hand, contains two to the power of twenty-four, or sixteen million, seven hundred and seventy-seven thousand, two hundred and sixteen codewords. Proving the minimum distance of the code requires showing that each of the non-zero codewords is of weight at least twelve.

We begin the chapter by listing one hundred and ninety-two zero divisors that we found by computer search to generate the code. We then take one of these and algebraically prove that it generates the code. Most of the proofs are readily adapted to the other one-hundred and ninety-one zero divisors. The only exception is the proof that the minimum distance of the code is twelve, which forms the last part of the chapter. It should be noted however that there is no real difficulty in showing that the code is of minimum distance at least eight. Problems only arise in showing that the minimum distance is greater than eight.

3.1 History of the Code

There is only one type II code of length forty-eight, dimension twenty-four and minimum distance twelve. This result, published in 2003, was achieved by computer search [7]. Thus any type II code of length forty-eight, dimension twenty-four and minimum distance twelve is assumed to be the code. The code constructed in this chapter submits to these parameters. It should be noted that the equivalence of the code to the extended quadratic residue code is not proven here. The result of the uniqueness of such a code was the result of an empirical calculation by computer [7]. While we do not doubt the validity of that result, it has not been proved algebraically.

A type II code is a binary code that is both self-dual and doubly even [10, p. 339]. These codes have received a good deal of attention in the literature. The reader is directed to Huffman's paper on the classification and enumeration of self-dual codes, published in 2005, for more information [9]. A type II code of length n is of minimum distance at most $4\lfloor n/24 \rfloor + 4$ [10, p. 344]. Codes achieving this upper bound are called extremal [10, p. 346]. The $(48, 24, 12)$ is thus an extremal type II code. It is in an interesting class of extremal type II codes: those of length a multiple of twenty-four. Out of all extremal type II codes these achieve the best minimum distance relative to their length, as evidenced by above mentioned upper bound. Extremal type II codes of length a multiple of twenty-four have received much attention in their own right. Indeed many have called for further investigations into their existence [16].

The $(48, 24, 12)$ type II code is commonly constructed by the extension of the quadratic residue code of length forty-seven by an even parity bit. Quadratic residue codes and indeed the extensions of quadratic residue codes have received

much attention previously. The reader should see Ward's chapter in "The Handbook of Coding Theory" for more information [8, p. 827].

The $(47, 24, 11)$ quadratic residue code is cyclic and generated by the polynomial $x+x^2+x^3+x^4+x^6+x^7+x^8+x^9+x^{12}+x^{14}+x^{16}+x^{17}+x^{18}+x^{21}+x^{24}+x^{25}+x^{27}+x^{28}+x^{32}+x^{34}+x^{36}+x^{37}+x^{42}$. The extended form of the code is not cyclic however and can not be generated by a polynomial [23]. We will now prove that the code can be generated by a zero divisor in a dihedral group ring. The construction is much like that of the construction of the $(47, 24, 11)$ code from a polynomial. We begin by discussing a certain group ring code in the next section.

3.2 Another Group Ring Code

In the previous chapter we constructed a group ring code using a zero divisor of the form $u = 1 + a\mathbf{f}$. The zero divisor is an element of the group ring $\mathbb{Z}_2\mathbf{D}_{24}$, the dihedral group of order twenty-four over the finite field with two elements. The group $\mathbf{D}_{24}$ is generated by the element a of order two and the element b of order twelve. Regarding the zero divisor $u = 1 + a\mathbf{f}$, the group ring element $\mathbf{f}$ is a sum of powers of b. The group ring code was shown in the chapter to be the extended binary Golay code.

In this chapter we construct another group ring code in a similar way. This time we use the group ring $\mathbb{Z}_2\mathbf{D}_{48}$, the dihedral group of length forty-eight over the finite field with two elements. The group $\mathbf{D}_{48}$ is again generated by two elements a and b but this time, while a is still of order two, b is now of order twenty-four. The group is thus presented $\langle a, b \mid a^2, b^{24}, ab = b^{-1}a\rangle$.

Again we use a zero divisor of the form $u = 1 + a\mathbf{f}$ but now the element $\mathbf{f}$ is $b^4+b^5+b^6+b^7+b^9+b^{10}+b^{11}+b^{13}+b^{15}+b^{18}+b^{19}+b^{20}+b^{21}+b^{22}+b^{23}$. We found this generator by computer search using GAP [3]. The search found one hundred and ninety-two zero divisors that generate the code. These are all of the form $1 + a\mathbf{h}$ where $\mathbf{h}$ is a sum of powers of b. The one hundred and ninety-two elements can be partitioned into four sets of forty-eight elements.

A representative of each of these sets are the elements u above and the elements $1 + a\mathbf{h}_1$, $1 + a\mathbf{h}_2$ and $1 + a\mathbf{h}_3$ where h_1, h_2 and h_3 are the following three respective elements:

1. $b^5+b^6+b^7+b^9+b^{10}+b^{12}+b^{13}+b^{15}+b^{17}+b^{18}+b^{19}+b^{20}+b^{21}+b^{22}+b^{23}$.
2. $b^2+b^5+b^7+b^9+b^{10}+b^{12}+b^{13}+b^{14}+b^{15}+b^{17}+b^{19}+b^{20}+b^{21}+b^{22}+b^{23}$.
3. $b+b^4+b^6+b^7+b^8+b^9+b^{12}+b^{13}+b^{14}+b^{16}+b^{18}+b^{20}+b^{21}+b^{22}+b^{23}$.

The other elements in each set are $1 + ab^i\mathbf{h}_k$ for i an integer from one to twenty-three and $1 + ab^j\mathbf{h}_k^{\mathrm{T}}$ for j an integer from zero to twenty-three, for k an element of $\{1, 2, 3, 4\}$ and $1 + a\mathbf{h}_4 = u$. All of the arguments given below for u—bar one—can easily be adapted to any of these other one hundred and ninety-one elements. The only argument for which the adaptation is not easy is the proof that the minimum distance of the code derived from u is in fact twelve and not eight. We are not aware of any obstacles that would hinder such an adaptation however, it is just that proof is tedious in detail.

The code we construct in this chapter is defined to be the principal left ideal $(\mathbb{Z}_2\mathbf{D}_{48})u$ of the zero divisor u in the group ring. We denote the code as $\mathcal{C}$. Since the group $\mathbf{D}_{48}$ is of order forty-eight, the code $\mathcal{C}$ is of length forty-eight. In the following sections we will show that this code is of dimension twenty-four, is self-dual, doubly even, quasi cyclic of index two, generated by a reverse circulant generator matrix and that it is of minimum distance twelve. We start by showing that u is a zero divisor in the group ring, which leads to the fact that $\mathcal{C}$ is self-dual.

3.3 The Zero Divisor

The group ring element u is a zero divisor. Multiplied by itself it yields zero. The element u is of the form $1 + a\mathbf{f}$ where $\mathbf{f}$ is $b^4 + b^5 + b^6 + b^7 + b^9 + b^{10} + b^{11} + b^{13} + b^{15} + b^{18} + b^{19} + b^{20} + b^{21} + b^{22} + b^{23}$. The multiplication is tedious to calculate in the group ring. Fortunately the result can be quickly shown using a given group ring matrix of u.

The group ring matrix that we will use will be that according to the listing $\{1, b, b^2, \ldots, b^{23}, a, ab, ab^2, \ldots, ab^{23}\}$ of $\mathbf{D}_{48}$. Under this listing the group ring matrix of u has the form:

$$\left[\begin{array}{c|c} I & A \\ \hline A & I \end{array}\right]$$

where I is the twenty-four by twenty-four identity matrix and A is the matrix given in figure 3.1. We will denote the full forty-eight by forty-eight matrix as U. Should U squared equal the zero matrix then the group ring element u squared equals zero. This is due to the fact that the ring of group ring matrices under any listing is isomorphic to the group ring.

Of course, just like the matrices of this form discussed in the previous chapter in section 2.4.1, working block-wise we can show that U^2 is zero if and only if

$$\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}$$

Fig. 3.1 — The Matrix A.

A^2 is the identity matrix:

$$\begin{aligned}
& U^2 = \underline{0}_{48} \\
\Leftrightarrow & \begin{bmatrix} I & A \\ A & I \end{bmatrix} \begin{bmatrix} I & A \\ A & I \end{bmatrix} = \underline{0}_{48} \\
\Leftrightarrow & \begin{bmatrix} I + A^2 & A + A \\ A + A & I + A^2 \end{bmatrix} = \begin{bmatrix} \underline{0}_{24} & \underline{0}_{24} \\ \underline{0}_{24} & \underline{0}_{24} \end{bmatrix} \\
\Leftrightarrow & \begin{bmatrix} I + A^2 & \underline{0}_{24} \\ \underline{0}_{24} & I + A^2 \end{bmatrix} = \begin{bmatrix} \underline{0}_{24} & \underline{0}_{24} \\ \underline{0}_{24} & \underline{0}_{24} \end{bmatrix}.
\end{aligned}$$

The submatrix A is reverse circulant and thus its row vectors are equal to its column vectors. Therefore, should the dot product of each row of A with itself be one and the dot product of distinct rows be zero then A^2 is the identity matrix and U^2 is zero. The former property is easy to see. Each row of A is a cycle of the first and the first is of weight fifteen. Thus the dot product of each row with itself is one.

The result regarding the two distinct rows of A is not quite as straight-forward. Since A is reverse circulant the dot product of every pair of its rows is equal to the dot product of row one of A with one of the other rows. This is because two rows of A can be cycled by the same amount until one of them becomes the first row, leaving their dot product intact. If upon cycling the two rows in this way the non-first row is one of the rows fourteen to twenty-four, then cycling the rows again so that that row becomes the first will induce the other row to become one of rows two to twelve. This effect is as described for the extended binary Golay code in section 2.4.2. Therefore, should the dot product of row one with each of rows two to thirteen of A be zero then U^2 is equal to zero. A quick check verifies this to be the case.

Thus the matrix U upon squaring becomes the forty-eight by forty-eight zero matrix and u is a zero divisor with itself in the group ring. We now use this fact to show that the code $\mathcal{C}$ is self-dual and of dimension twenty-four.

3.4 Dimension Twenty-Four and Self-Duality

The vector form of the group ring code $\mathcal{C}$ is the row space of the matrix U. This is due to the fact that $\mathcal{C}$ has been defined to be the principal left ideal of u in the group ring. The vector form of such codes is discussed in section 1.9.2. The row space of U is a subspace of the vector space $\mathbb{Z}_2^{48}$. We will now see that the code is equal to its dual code. At the same time we see that the code is of dimension twenty-four.

The matrix U when squared is equal to the zero matrix. Thus its columns are contained in its null space. The matrix U is equal to its own transpose, as is evident from its description in section 3.3. Thus the rows of U are also contained in its null space. The code $\mathcal{C}$ in vector form is the row space of U, and the null space of U is the dual code of $\mathcal{C}$. The code $\mathcal{C}$ is therefore contained in its own dual code and is thus self-orthogonal.

The null space of U has dimension forty-eight minus the rank of U. The rank of U is at least twenty-four since its first twenty-four rows are linearly independent. Thus the dimension of the null space is at most twenty-four. This is evident from the fact that the twenty-four by twenty-four identity matrix sits as its top-left block. The row space of U, as we've seen, is contained in its null space, and thus both must in fact be the same space. Thus the code $\mathcal{C}$ is not only self-orthogonal, but self-dual. Furthermore the code is of dimension twenty-four. We will now use these facts to prove that $\mathcal{C}$ is doubly-even.

3.5 Doubly Evenness

We've just seen that the code is self-orthogonal, and more specifically that it is self-dual. Every self-orthogonal code generated by a generator matrix with rows each of weight divisible by four is doubly-even [10, p. 10]. It is easy to find a generator matrix of $\mathcal{C}$ with rows of weights divisible by four, as we shall now see.

The code $\mathcal{C}$ is the row space of the matrix U. We saw in the previous section that the first twenty-four rows of U are linearly independent. We also saw that the dimension of $\mathcal{C}$ is twenty-four. Thus $\mathcal{C}$ is generated by the first twenty-four rows of U. These form a submatrix $G = [I|A]$ of U where A is the matrix in figure 3.1. The matrix G is thus a generator matrix for $\mathcal{C}$.

The first row of U is of weight sixteen, which is divisible by four. All of the other rows of G are permutations of the first row and thus are each of weight sixteen. Therefore the self-orthogonal code $\mathcal{C}$ is generated by a generator matrix with rows all of weight divisible by four. The code $\mathcal{C}$ is thus doubly even.

Since $\mathcal{C}$ is a binary code that is self-dual and doubly even, it is a type II code. The code is of length forty-eight and dimension twenty-four. Should its minimum distance be twelve then it is the unique such type II code, and also it is an extremal code. Later in this chapter we will prove this to be the case. First we will show that the code is quasi-cyclic.

3.6 Quasi Cyclicity

The code $\mathcal{C}$ in vector form is generated by the generator matrix G. The matrix G is of the form $[I|A]$ where A is reverse circulant. Such matrices are called reverse circulant generator matrices [10, p. 377]. Reversing the columns of A gives a generator matrix that is double circulant, and this generator matrix generates an equivalent code to $\mathcal{C}$. Sometimes double circulantly generated codes are equivalent to quasi cyclic codes [8, p. 60]. This is the case with $\mathcal{C}$.

The code $\mathcal{C}$ is the row space of the matrix U. The matrix U is of the form:

$$\left[\begin{array}{c|c} I & A \\ \hline A & I \end{array}\right]$$

and the matrix $G = [I|A]$ generates the code. As generated by G the code $\mathcal{C}$ is quasi cyclic of index two. This is due to the fact that the rows of the matrix $[A|I]$ are contained in the code.

Any combination of the rows of $G = [I|A]$ is a codeword and every codeword is a combination of the rows of G. Let $\underline{c}$ be a given combination of rows of G and let $\underline{d}$ be the combination of the same rows of $[A|I]$. Furthermore let $\underline{x}$ be the vector containing the first twenty-four components of $\underline{c}$ in order and $\underline{y}$ be that containing the last twenty-four in order. The codeword $\underline{c}$ is equal to $\underline{xy}$, by which be mean the concatenation of $\underline{y}$ to $\underline{x}$. The codeword $\underline{d}$ is then equal to $\underline{yx}$.

Thus for any codeword $\underline{xy}$ in $\mathcal{C}$, the codeword $\underline{yx}$ is also a codeword. Thus the code $\mathcal{C}$ as generated by G is quasi cyclic of index two. We use this fact in the following section to show that the code is of minimum distance at least eight.

3.7 Minimum Distance at Least Eight

In the following section we will prove that the code $\mathcal{C}$ has minimum distance at least eight. This facilitates our later proof that the minimum distance is in fact twelve. We start by discussing the role that the identity matrix in $G = [I|A]$ plays in determining the weight of a codeword. Remember that the minimum of all the weights of the codewords of $\mathcal{C}$ is equal to the code's minimum distance [10, p. 8]. We start by showing that no combination of more than five rows of G is of weight less than eight.

3.7.1 More than Eight Rows

As in section 3.6 we let $\underline{c} = \underline{xy}$ be a non-zero codeword of $\mathcal{C}$. Then $\underline{c}$ is the combination of some set of i rows of $G = [I|A]$ for i an integer between one and twelve. The subvector $\underline{x}$ is the combination of those i rows of I and $\underline{y}$ is that

of A. The weight of $\underline{x}$ is exactly i. Every codeword of $\mathcal{C}$ is doubly even and therefore when i is greater than four the codeword $\underline{c}$ is of weight at least eight. Thus every combination of five or more rows of G is of weight at least eight. We continue with this notation to now show that no combination of four rows of G is of weight less than eight.

3.7.2 Four-Row Combinations

The subvector $\underline{y}$ is never of weight zero. This is due to $\underline{y}$ being a combination of one or more rows of the matrix A. In section 3.3 we saw that A is its own inverse and so is of full rank. Thus no combination of four rows of A is the zero vector and $\underline{y}$ is of non-zero weight. Furthermore, the subvector $\underline{x}$ is of weight four. Every combination of four rows of G is therefore of weight at least five. Combinations of four rows of G are therefore always of weight at least eight, since $\mathcal{C}$ is doubly even. We are only left to show that no combination of one, two or three rows of G is of weight less than eight.

3.7.3 One and Two Rows

The one and two row combinations of G are easily seen to be of weight eight or more. The first row of G is of weight sixteen and the other rows are all permutations of this row. Thus every row of G is of weight sixteen.

Every combination of two rows of A is of weight either ten or fourteen. This result is due to the fact that each of rows two to thirteen of A combines with row one of A to give a subvector of weight ten or fourteen. Every combination of two rows of A is equal in weight to one of these subvectors due to A's reverse circulant nature. Cycling two rows of A the same number of times leaves the weight of their combination intact. Either of the two rows of the combination can be cycled until it becomes the first row of A. Should cycling the other row by the same amount induce it to become one of rows fourteen to twenty-four, then cycling that row to become the first will induce the first row to become one of those from two to twelve. This is exactly as described in section 3.3 for the dot product of two rows. Thus each combination of two rows of G is of weight twelve or sixteen. The only remaining possibilities for a non-zero codeword of weight less than eight in $\mathcal{C}$ are the three-row combinations of G.

3.7.4 Three Rows

We will use the quasi cyclic nature of $\mathcal{C}$ to show that no three-row combination of G is of weight less than eight. Since $\mathcal{C}$ is doubly even, a non-zero codeword of weight less than eight would have to have weight four. Every combination of

three rows of I is of weight three and thus if a three-row combination of G was of weight four, the combination of those rows of A would be of weight one. Thus in such a codeword $\underline{c} = \underline{x}\underline{y}$, $\underline{x}$ would be of weight three and $\underline{y}$ would be of weight one. In section 3.6 we proved that the code is quasi cyclic of index two and thus $\underline{c}$'s existence would imply that $\underline{y}\underline{x}$ was also a codeword. This codeword $\underline{y}\underline{x}$ would have to be the combination of a single row of G and would have weight four. Every row of G is of weight sixteen however, and thus the codeword $\underline{c}$ cannot exist.

So we see that every non-zero combination of rows of the generator matrix G is of weight at least eight. This proves that the minimum distance of the code $\mathcal{C}$ is at least eight. The code's minimum distance is in fact twelve, as we shall prove in the rest of this chapter. We start by showing that the combinations of three and four rows of G are the key to the proof.

3.8 The Three and Four Row Combinations

In this section we show that so long as all of the three-row and four-row combinations of G are of weight at least twelve then the minimum distance of $\mathcal{C}$ is twelve. In the preceding section we used $\mathcal{C}$'s quasi cyclic nature to prove that no non-zero codeword was of weight less than eight. The code $\mathcal{C}$ is doubly even and so the next greatest weight a codeword can have after eight is twelve. Showing that no codeword is of weight eight will thus show that the code is of minimum distance at least twelve. Note that some of the two-row combinations of G are of weight twelve, as we saw in section 3.7.3. Thus the code is of minimum distance at most twelve. We start now by showing that no combination of eight or more rows of G is of weight eight.

3.8.1 Eight or More Rows

Each combination of eight or more rows of G is of weight at least twelve. Just like earlier, we let the codeword $\underline{c}$ be a combination of i rows of G. We again split $\underline{c}$ into two subvectors $\underline{x}$ and $\underline{y}$ which consist of the first and last twenty-four components of $\underline{c}$ respectively.

The weight of $\underline{x}$ is always i. Thus every combination of nine or more rows of G is of weight at least nine. Since $\mathcal{C}$ is doubly even, every such combination is of weight at least twelve.

When i is eight $\underline{x}$ is of weight eight. The codeword $\underline{c}$ would then only be of weight eight if $\underline{y}$ is a zero vector. Since A is of full rank, $\underline{y}$ is never the zero vector. As a consequence $\underline{y}$ has weight at least one. Thus $\underline{c}$ is of weight at least nine and therefore is of weight at least twelve.

We need only to show then that no non-zero combination of less than eight rows of G is of weight eight.

3.8.2 Less than Eight Rows

The code $\mathcal{C}$ as generated by G is quasi cyclic. Again we let $\underline{c} = \underline{xy}$ be an arbitrary combination of i rows of G. We can see that if $\underline{c}$ is of weight eight for i from one to seven, then some combination of $8 - i$ rows of G is also of weight eight. The weight of $\underline{x}$ is i and that of $\underline{y}$ is $8 - i$. The vector $\underline{c'} = \underline{yx}$ is also a codeword since $\mathcal{C}$ is quasi cyclic. The codeword $\underline{c'}$ must be the result of a combination of $8 - i$ rows of G.

This result is extremely useful. It proves that a combination of seven rows of G is only of weight eight if one row is, that of six rows of G is only of weight if a combination of two rows is and that a combination of five rows of G is only of weight eight if a combination of three rows is. We have thus reduced the proof of $\mathcal{C}$'s minimum distance being twelve to the proof that no combination of four, three, two or one rows of G is of weight eight. Of course, we saw in section 3.7.3 that every single row of G is of weight sixteen and each combination of two rows of G is of weight either twelve or sixteen. Thus we have reduced our proof to the combinations of three and four rows of G.

Unfortunately, evaluating that the three- and four-row combinations of G are of weight at least twelve is quite a difficult task. The number of three-row combinations of G is two thousand and twenty-four and the number of four-row combinations is ten thousand, six hundred and sixty-six. Over the next few sections we will see that the proof can be done algebraically. We start by discussing how the proof relates to the basis elements of the group ring form of the code $\mathcal{C}$.

3.9 Dih-Cycling

We wish to prove that no combination of three rows and no combination of four rows of the matrix G is of weight eight. The i^{th} row of G is the group ring codeword $g_i u$ in vector form where g_i is the i^{th} element of the listing used of $\mathbf{D}_{48}$, for i an integer from one to twenty-four. The listing we have used is $\{1, b, b^2, \ldots, b^{23}, a, ab, ab^2, \ldots, ab^{23}\}$. Thus the i^{th} row of G is the vector form of the group ring codeword $b^{i-1}u$. Obviously then the elements $b^{i-1}u$, for i from one to twenty-four, form a basis for the group ring form of $\mathcal{C}$. The vector and group ring forms of group ring codes were discussed in section 1.9.2.

The proof that each three- and four-row combination of G is not of weight eight is thus equivalent to showing that no set of three and no set of four elements

of the form $b^{i-1}u$ for i from one to twenty-four in $\mathbb{Z}_2\mathbf{D}_{48}$ combine to an element of weight eight. This is a useful result because one can assume that one of the elements in such a set of three or four group ring elements is the element $b^0u = u$. Consider the combination $b^ju + b^ku + b^lu$ of the three arbitrary group ring elements b^ju, b^ku and b^lu for j, k and l distinct integers between zero to twenty-three inclusive. The combination $b^{-j}(b^ju+b^ku+b^lu) = u+b^{k-j}u+b^{l-j}u$ is of equal weight to the original combination. Thus if no combination of three basis elements of $\mathcal{C}$, where one of those elements is u itself, is of weight eight, then no combination of any three basis elements is of weight eight. The same argument can be applied to four basis elements.

Consider an arbitrary group ring matrix U' of u. The rows of the matrix that are labelled by the elements b^{i-1} for i from one to twenty-four are a basis for the code $\mathcal{C}$. The matrix formed by these rows in order are thus a generator matrix for the code. If we can show that every three-row and every four-row combination of such a generator matrix involving the row labelled by the identity b^0 of the group is not eight, then the code $\mathcal{C}$ is of minimum distance twelve.

Note that any combination of three basis elements $b^ju + b^ku + b^lu$ and any combination of four basis elements $b^ju + b^ku + b^lu + b^mu$ can be multiplied by any power of b and its weight will remain intact. Thus any of the three and four respective powers of b can be cancelled out by premultiplication of the combination by their inverse. We can therefore assume that any of the rows in a three or four row combination of such a generator matrix is that labelled by the identity. We will call the effect of multiplying such a combination of group ring basis elements by b^i 'dih-cycling' the combination i steps forwards. We'll also call the effect of multiplying such a combination by b^{-i} 'dih-cycling' i steps back(wards).

Throughout the rest of this chapter we will extensively use the concept of dih-cycling. Combined with a new generator matrix for $\mathcal{C}$ derived in the next section, dih-cycling enables us to algebraically prove that $\mathcal{C}$ is of minimum distance twelve.

3.10 A Different Group Ring Matrix

One of the main advantages of deriving a code from the group ring perspective, as we have done, is that we can create many different vector forms of the code, all of which are equivalent. This was discussed in section 1.9.2 of chapter 1. These various vector forms of the code are the row spaces of the group ring matrices of u under the different listings of $\mathbf{D}_{48}$. Previously in this chapter we have used the listing $\{1, b, b^2, \ldots, b^{23}, a, ab, ab^2, \ldots, ab^{23}\}$. We now change the listing, instead using the following one:

0	0	0	1	0	1	0	1	1	1	0	1	0	1	0	1	1	1	0	1	1	1	1	1
0	0	0	0	1	1	1	1	0	0	1	1	1	0	0	1	1	1	1	1	0	1	1	1
0	0	0	1	1	0	1	0	1	1	1	0	0	0	1	1	1	1	1	0	1	1	1	1
1	0	1	0	0	0	1	0	1	1	1	0	1	1	1	1	0	0	1	1	1	1	1	0
0	1	1	0	0	0	0	1	1	1	0	1	1	1	1	0	0	1	1	1	1	1	0	1
1	1	0	0	0	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	1	1
0	1	1	1	0	1	1	0	1	0	0	0	0	1	1	1	1	1	1	1	1	1	0	0
1	1	0	0	1	1	0	1	1	0	0	0	1	1	0	1	1	1	1	1	1	0	0	1
1	0	1	1	1	0	1	1	0	0	0	0	1	0	1	1	1	1	1	1	1	0	1	0
1	0	1	1	1	0	0	0	0	0	1	1	1	1	1	1	1	0	1	0	0	1	1	1
0	1	1	1	0	1	0	0	0	1	1	0	1	1	1	1	0	1	0	0	1	1	1	1
1	1	0	0	1	1	0	0	0	1	0	1	1	1	1	0	1	1	0	1	0	1	1	1
0	1	0	1	1	1	0	1	1	1	1	1	0	1	1	1	0	1	1	0	1	0	0	0
1	0	0	1	1	1	1	1	0	1	1	1	1	1	0	0	1	1	0	1	1	0	0	0
0	0	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	0	1	1	0	0	0	0
1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	1	1
1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	1	0	0	0	1	1	0
1	1	1	0	1	0	1	1	1	0	1	1	1	1	0	0	1	1	0	0	0	1	0	1
0	1	1	1	1	1	1	1	1	1	0	0	1	0	1	0	0	0	1	0	1	1	1	0
1	1	0	1	1	1	1	1	1	0	0	1	0	1	1	0	0	0	0	1	1	1	0	1
1	0	1	1	1	1	1	1	1	0	1	0	1	1	0	0	0	0	1	1	0	0	1	1
1	1	1	1	1	0	1	0	0	1	1	1	0	0	0	0	1	1	1	1	0	0	1	1
1	1	1	1	0	1	0	0	1	1	1	1	0	0	0	1	1	0	1	0	1	1	0	1
1	1	1	0	1	1	0	1	0	1	1	1	0	0	0	1	0	1	0	1	1	1	0	1

Fig. 3.2 — The Matrix B.

$$\{\quad b^0,\ b^8,\ b^{16},\ b^4,\ b^{12},\ b^{20},\ b^2,\ b^{10},\ b^{18},\ b^6,\ b^{14},\ b^{22},$$
$$b^1,\ b^9,\ b^{17},\ b^5,\ b^{13},\ b^{21},\ b^3,\ b^{11},\ b^{19},\ b^7,\ b^{15},\ b^{23},$$
$$ab^0,\ ab^8,\ ab^{16},\ ab^4,\ ab^{12},\ ab^{20},\ ab^2,\ ab^{10},\ ab^{18},\ ab^6,\ ab^{14},\ ab^{22},$$
$$ab^1,\ ab^9,\ ab^{17},\ ab^5,\ ab^{13},\ ab^{21},\ ab^3,\ ab^{11},\ ab^{19},\ ab^7,\ ab^{15},\ ab^{23}\quad \}.$$

According to this listing the group ring matrix W of u is of the form:

$$\left[\begin{array}{c|c} I & B \\ \hline B & I \end{array}\right]$$

where I is the twenty-four by twenty-four identity matrix and B is the twenty-four by twenty-four matrix[1] given in figure 3.2. The matrix B has been split into sixteen six by six submatrices indicated by the double black lines in figure 3.2, and each submatrix is further split into four three by three blocks indicated by the single black lines. We will refer to the rows of blocks as block rows and columns of blocks as block columns. Furthermore we will refer to the eight

[1]The matrix B here shouldn't be mistaken for the group ring matrix of the group ring element b, which we will not discuss in this chapter.

three-component subvectors of each row of B (as dictated by the vertical black lines) as segments. The first twelve columns of B will be referred to as the left-hand side of B or LHS for short. Likewise, the last twelve will be referred to as the right-hand side of B or RHS for short.

Note that according to the listing, the first twenty-four rows of W are labelled by the elements b^{i-1} for i from one to twenty-four. They thus form a generator matrix for a vector form of the code $\mathcal{C}$. The code they generate is equivalent to that generated by G earlier in the chapter. Furthermore, the first row is that labelled by the identity b^0 of $\mathbf{D}_{48}$ and thus is that corresponding to u. As we showed in the previous section, if all of the combinations of three and four rows of the first twenty-four rows of W that involve the first row are of weight greater than eight then the code $\mathcal{C}$ has minimum distance twelve. We will show this to be the case in the following sections.

Note that just like in the case of G, the first twenty-four rows of W are of the form $[I|B]$ with the twenty-four by twenty-four identity matrix as their left-most block. Thus to prove that each three-row combination of those twenty-four rows is of weight at greater than eight we need only show that each three-row combination of B involving its first row is of weight greater than five. Likewise we need only show that each four-row combination of B involving its first row is of weight greater than four. In a moment we will take the three and four row cases separately, proving each in turn. First we briefly mention some effects on the rows of B of dih-cycling the rows in a combination of rows of W.

3.11 The Matrix B

We are really only interested in dih-cycling as far as its effects of the matrix B. We will only concern ourselves with a few facts about the situation. First of all the block rows of B each contain three rows that are each eight or sixteen dih-cycles apart. This is thanks to the first twenty-four elements of the listing being $\{b^0, b^8, b^{16}, b^4, b^{12}, b^{20}, b^2, b^{10}, b^{18}, b^6, b^{14}, b^{22}, b^1, b^9, b^{17}, b^5, b^{13}, b^{21}, b^3, b^{11}, b^{19}, b^7, b^{15}, b^{23}\}$. Of course if two rows are eight dih-cycles apart in the forwards direction then they are sixteen apart in the backwards direction. Thus if two rows are in the same block row we can dih-cycle them until they become the first two rows in that block row. All of the other rows in the other block rows remain in those block rows, though their order within those block rows will change in the same way.

The second fact we wish to note is that if two rows are in the last four block rows of B and we dih-cycle one of them into the first four block rows then the other row also gets dih-cycled into the first four block rows. The rows in the first four block rows correspond to the group ring elements of the form $b^i u$ where i

is zero or an even integer. The rows in the last four block rows correspond to those where i is odd. Since the number of steps two rows are apart is preserved when both are dih-cycled by the same amount if both correspond to odd or even i indices before dih-cycling then that will be true after dih-cycling. Likewise dih-cycling two rows where one of them is in the first four block rows and the other in the last four, will always result in one of the rows residing in the first four sub-block rows and the other in the last four.

A third fact of note is regarding the first two block rows and the second two block rows of B. If one row is in the first block row of B and another is in the second block row then dih-cycling will leave one of the rows in block row one and the other in block row two, or leave one in block row three and one in block row four, or leave one in block row five and one in six, or one in seven and one in eight. This is because these pairs of block rows are all of those containing rows that are four, twelve and twenty dih-cycle steps apart. Note that if we continuously dih-cycle the two rows they will visit each block row of B eventually. We can now move on with the proof that no three-row combination of B is of weight five.

3.12 Three Rows of B

We will split the task of proving that no three-row combination of B is of weight five into three separate cases. The first is that all three-rows come from a single block row of B. The second is that two of the three rows do, and the third doesn't. Finally the third is that all three rows come from separate block rows.

The first case is the easiest. If all three rows come from a single block row of B we can assume that it's block row one. Every other three-row combination coming from a single block row can be dih-cycled until all three rows are contained in block row one. Sub-block row one contains two all ones blocks whose segments combine to give a weight three segment. Hence the combination of the three rows is of weight at least six and thus is not five. The other two cases are not so straight-forward, as we shall now see.

3.12.1 Two from a block row

We can assume that the two rows that are contained in a single block row are in block row one. Furthermore we can assume that they are rows one and two of B. This is all thanks to our ability to dih-cycle combinations of the rows of B. Of course the third row of the combination must also be dih-cycled by the same amount but that makes no difference, it is still contained in a separate block row.

The combination of rows one and two of B contains three weight zero segments arising from the two all ones blocks and the single all zeroes block. These are in block rows one, six and eight. The other segments are all of weight two, since they arise from the combination of two distinct weight two segments.

The third row contains a single weight zero segment a single weight one segment, four weight two segments and two weight three segments. The three weight zero segments in the combination of rows one and two of B thus contribute a weight of at least four to the three-row combination unless one of them combines with the weight zero segment of the third row, another combines with the weight one segment and the last combines with one of the weight two segments. We will use the weight zero segments in the combination of rows one and two to check if this ever happens.

Sub-block column one only contains weight zero segments in block row one and we are only interested in the third row coming from a separate block row. Sub-block column six contains weight zero segments only in block row seven. In this case the other two weight-zero segments from rows one and two combine with weight two segments, thus contributing at least four to the weight of the overall three-row combination. Sub-block column eight contains weight zero sub-segments in block row five. Only in this case do the three weight zero segments only contribute three to the overall weight, with block column one only contributing weight one. We will return to this case in a moment.

First we will discuss the combinations in block columns two, three and four. The segments in the combination of rows one and two of B in these columns are both $(1, 1, 0)$, $(1, 0, 1)$ and $(1, 1, 0)$ respectively. When the third row is taken from one of block rows two to four then one of these is combined with a segment of weight zero in the third row contributing weight two to the overall three row combination. Combined with the fact that those combinations were already of weight at least four from block columns one, six and eight these combinations all have weight at least six.

When the third row is taken from block rows five or seven two of these weight two segments combine with weight three segments in the third row. In the block row seven case the combinations are now all of weight at least six. In the block row five case we only have weight three coming form block columns one, six and eight so we now have these three-row combinations having at least weight five. Note that then block column three (which does not contain weight three segments in the third row) is always of weight two unless row fifteen of B is used. In that case the segment of the three-row combination in column five is of weight two, giving these combinations a weight of at least six.

Finally in the block rows six and eight cases one of the weight two segments combines with a weight three segment and another with a weight one segment.

This again contributes at least weight two to a combination already of weight at least four. Hence all of the combinations in these cases are of weight at least six. We are left then only to discuss the case in which all three rows come from separate block rows.

3.12.2 All from separate block rows

We will split the case of three-row combinations from different block rows into two separate sub-cases. The first is that all three rows come from the first four block rows of B. The other case is that two of them come from the first four block rows of B and the third comes from the last four. Note that the proof of the former of the two cases implies the proof for the situation in which all three rows come from separate blocks from the last four block rows. Furthermore the latter of the two cases implies the case in which two rows come from separate block rows in the last four block rows and the other row comes from the first four block rows.

All from one set of four

We can assume that the three rows come from the first three of these block rows. In the case that two of the rows are from block rows three and four, dih-cycling the rows backwards two steps will place those rows in block rows one and two. This is obvious from the fact that the three indices i in the group ring elements $b^i u$ corresponding to the rows in each of the first four block rows in order are: 0, 8 and 16; 4, 12 and 20; 2, 10 and 18; and 6, 14 and 22. Thus we can assume two of the rows are from block rows one and two.

Furthermore we can assume that the third row comes from block row three. If it is contained in block row four then dih-cycling all three rows backwards by four steps will place it in the third block row. This will switch the row in block row one to block row two and that in block row two to block row one. As always we can further assume that that from block row one is row one of B. Thus we only need check that all of the three-row combinations involving row one, one of the rows in block row two and one of the rows in block row three are of weight greater than five.

In these cases the segment of the combination in block column six is always of weight one and that in block column seven is always of weight two. Furthermore that in block column two is always of weight two unless row seven of B is used from block row three. That in block column five is always of weight two unless row nine of B from block row three is used. Together these three facts show that the segments in column two, five, six and seven contribute at least weight five to the three row combination. If we can show that the other four segments, those

in block columns one, three, four and eight are never all of weight zero then none of these combinations have weight five. The segment of the combination in block column four is always of weight two unless row five is used in block row two. In that case however the segment in block column three is always of weight two, since that segment is the combination of three weight two segments, two of which are equal. Thus no combination of three rows from distinct block rows from the top half of B is of weight five, implying no such combination from the bottom half is. We move on now to the case where two of the rows come from the first or last four block rows and the other comes from the last or first four respectively.

Two from one set of four

We can assume that the second row of the combination is contained in block row two or block row four. If it is contained in block row three then dih-cycling the two rows so that the second row becomes row one of B makes the other row become one of those in block row four. This is obvious by again looking at the indices of the rows of B: 0 with 18 becomes 6 with 0, 0 with 10 becomes 14 with 0 and 0 with 2 becomes 22 with 0.

On the LHS of such combinations the four segments in the combination of the first two rows of the combination are all of weight zero or two. The third row always contains three odd-weighted segments and the segments of the three-row combination in those block columns are thus always of weight at least one. Thus the LHS of the combination is always of weight at least three. On the RHS the first two rows of the combination each contain a single weight two segment and three odd-weighted segments. The weight two segments never combine with each other since the two rows come from separate block rows. The third row only contains segments of weight zero and two. Thus there are two block columns containing segments of odd weight on the RHS of the three-row combination. In total every combination in this case of weight at least five. If we can show that the other three columns are never all of weight zero then we have proven this case.

We now take the cases in which we use block row two and block row four separately. When we use block row two the even weighted segments of the combination on the RHS are in block columns five and six. That in block column five is only ever of weight zero if one of rows fifteen, sixteen and nineteen of B is the third row. When any of those rows is the third row the segment in block columns six is of weight two. Thus those combinations are of weight at least seven.

When the second row is in block row four the even-weighted segments on the

RHS of the three-row combination are then in block columns five and eight. The segment in block column eight is always of weight two unless the third row comes from block row five. In this case the segment in block column five is always of weight two unless the third row is row fifteen of B. The third even-weighted segment of the combination is then contained in block column three. When row fifteen is used this is of weight two. Thus none of the combinations arising in this case are of weight less than seven. So we've seen that no combination involving three rows from a single block row of B, none involving exactly two from any single block row and no combination involving three rows from distinct block rows of B are of weight five. This proves that in fact none are of weight less than nine, since as we've seen before $\mathcal{C}$ is a doubly even code. We now move on to the proof that no combination of four rows of B is of weight four.

3.13 Four Rows of B

Like in the three rows proof, we separate the four rows proof into three distinct cases. First we take the case where three of the four rows come from a single block row. Second we take that case that two of the rows share a block row and the other two rows are not in that block row. Lastly we prove the case in which all of the rows come from distinct block rows.

The first of these cases is proven easily. We are free to assume that one of the three rows sharing a block row is row one of B. In that case rows two and three of B are involved in the four-row combination also. The LHS of the combination of these three rows consists of all zeroes. The LHS's of the other twenty-one rows of B are all of weight six or greater. So when the fourth row is added to the combination the combination's LHS is of weight at least six. Hence no four-row combination of B where three of the rows share a block row is of weight four. We now move on to the second and third cases, which are a little trickier.

3.13.1 Two from one block row

We split the case of two rows coming from a single block row into five distinct sub-cases. We always assume that these two rows are the first and second of B. If they are not we can always dih-cycle the combination until this becomes the case. The first sub-case is that the other two rows come from the same block row and that is one of block rows two to four. The second sub-case is that in which the other two rows come from the same block row and that is one of the block rows five to eight. Thirdly we examine the sub-case in which the third row comes from the block rows two to four, and the fourth row comes from block rows five to eight. The fourth sub-case is that in which the third and fourth rows

come from distinct block rows in block rows two to four. Finally we examine the sub-case in which the third and fourth rows come from distinct block rows in block rows five to eight.

Two from one of block rows two to four

The LHS of the combination of two rows from the same block row from block rows two to four contains a single weight zero segment and three weight two segments. When two of these two-row combinations from distinct block rows are combined the weight zero segments are never combined with each other, so they each contribute two to the weight of the over-all four-row combination. The RHS of each combination of two rows from the same block row contains two weight zero segments and two weight two segments. When two such two-row combinations from distinct block rows are combined at least one of the weight zero segments in each of the two row combinations is not combined with another weight zero segment. Therefore such four-row combinations are again of weight at least four. Thus all of the four-row combinations in this sub-case are of weight at least eight.

Two from one of block rows five to eight

Again in this sub-case we look at the weight zero segments in each of the two-row combinations. The combination of the first two rows of B contains a single weight zero segment in its LHS and two weight zero segments in its RHS. The combination of two rows from the same block row in the block rows five to eight contains two weight zero segments in its LHS and one in its RHS. All the other segments are of weight two. In the combinations from block rows five and seven the two weight zero segments on the LHS of those combinations are never contained in block column one, which is the block column in which that from the combination of rows one and two resides. Hence the LHS of those combinations is always of weight at least six. If a combination from block rows six or eight is used then the weight zero segment from the combination of rows one and two coincides with one of those in the other two-row combination, giving the LHS a weight of at least two. The RHS of the four-row combination however is of weight at least six if the rows come from block row six or eight and at least weight two otherwise, for the same reason. Thus all of the four-row combinations in this sub-case are of weight at least six.

3.13.2 One from two to four, one from five to eight

The segments in the combination of rows one and two of B are all of weight zero or two. Those in the LHS of all of the rows in block rows two to four are also

of weight zero or two. On the LHS of all of the rows in block rows five to eight however there are three odd-weight segments. Thus the LHS of a combination of four rows in this sub-case is of weight at least three. The RHS's of the rows in block rows two to four also contain three odd-weighted segments, while those in block rows five to eight contain only even weighted ones. Therefore the RHS of the four-row combinations in this sub-case are also of weight at least three. Thus these combinations all have weight at least six.

Distinct block rows two to four

The fifth segment of the combination of rows one and two of B is of weight two. In the four-row combinations in this sub-case it is combined with either two segments of weight three or one of weight three and one of weight one. Thus the fifth segment of every four-row combination in this sub-case is of weight either one or two. The segments in the combination of rows one and two in block columns six and eight are zero. These are each combined with a weight one segment and a weight two, or a weight one with a weight three or a weight two with a weight three segment. Thus those segments of the four-row combination are always of weight at least one. Therefore the RHS of the combinations in this sub-case are always of weight at least three. Now notice that the RHS of four rows in the combination in this sub-case are all of the same odd weight. Thus the RHS of the combination is always of even weight. Hence the RHS is always of weight at least four.

The LHS of these combinations is never of weight zero. When one of the rows involved is in block row two, the segments of the combination of this row with rows one and two of B in block columns three and four are either both zero (when it's row four) or both two (otherwise). Whether the other row comes from block row three or four the segment of that row in one of those columns is of weight zero and the segment in the other column is of weight two. Thus at least one of those segments of the four-row combination is of weight two. When a row from block row two isn't used then one from block row three and one from block row four are used. The segments in block columns one and two in the combination of those two rows are both of weight zero or both of weight two. The first two segments in the combination of rows one and two of B are of weight zero and two respectively. Thus when combined with the two segments from the other two rows, both of weight zero or both of weight two, at least one of the segments of the combination is of weight two.

Distinct block rows five to eight

The next sub-case for consideration is that in which rows one and two and combined with two rows from distinct block rows five to eight. There are six different ways to choose two block rows from four. We will investigate each of these individually. Note that there are exactly two odd-weighted segments in every such four-row combination arising from the two weight two segments, one in the LHS of each of the rows from the last four block rows. All of the other segments on the LHS of these rows are of odd weight and the four segments on the LHS of rows one and two are of weight two or zero.

The first three of the six choices of block rows we will deal with are those involving block row five. In these situations the last segment of the four-row combination is always of weight two. The segment in block column one is of weight two when a row from either of block rows six or eight is chosen. When a row from block row seven is chosen then the segment in block column two is of weight two. Combined with the two odd-weighted segments these result in all of the combinations involving a row from block row five being of weight at least six. There are then three choices of block rows left to cover. When a row from block six and one from block row seven are involved in the combination then the segments of the combination in block columns three and six are always both of weight two. Thus those combinations are always of weight at least six.

The case in which a row from each of block rows six and eight is involved is a little harder to see. In this case at least one of the segments of the combination in block columns six and eight is of weight two. The only way they can be zero is if the segments in the two rows in each of those columns are equal. It is evident that this never happens simultaneously in both block columns. The segment in block column three is of weight two unless row twenty-four of B is involved, whereas that in block column seven is of weight two unless row twenty-three is involved. Thus at least one of the segments in those two columns is of weight two. Together with the two odd-weighted segments these combinations are thus all of weight at least six.

Finally we come to the case in which a row from each of block rows seven and eight is involved. In this case the segment in block column six is always of weight two. The segment in block column four is of weight two unless row twenty is used, and that in block column five is of weight two unless row twenty-one is used. Thus at least one of those segments is of weight two, giving the overall combination a weight of at least six when the odd-weighted segments are considered. This concludes the proof that no combinations involving rows one and two and not row three of B are not of weight four. We move on now to proving that no four-row combination of four rows from distinct block rows of B

is of weight four.

3.13.3 Distinct block rows

We also split the case in which all four rows come from distinct block rows into sub-cases. The first of these is that all four rows come from the first four block rows of B. This sub-case also proves the situation in which the four rows come from the last four block rows, since those combinations can be dih-cycled backwards one place and they become rows in the first four block rows. The second sub-case is that three come from the first four block rows and one comes from the last four. Again, this incorporates the case in which three of the rows come from the last four block rows and the other from the first four. The third and final sub-case is that two come from each of the first and last four block rows.

The first sub-case is straight forward. The segments on the RHS of the four rows combination are all of odd weight so the RHS of the combination is of weight at least four. The segments on the LHS are only of weight zero if they are the combination of three weight-two segments that are all different. Thus the segment in block column is of weight two if row seven is involved in the combination, and that in block column three is of weight two if row eight is used. We must therefore use row nine from block row three if we are to get a four row combination of weight four. When we use row nine however, the segment in column five is of weight three and thus the combination has weight six anyway. Thus none of the combinations in this sub-case are of weight four.

The second sub-case is also straight-forward. Here we can assume that three of the rows are contained in the block rows one, two and three. If they are not they can be dih-cycled to this position. The LHS of the fourth row contains three odd-weighted segments which when combined with the even-weighted segments of the first three rows give the LHS a weight of at least three. Furthermore the segment in block column six is of odd weight and thus the four-row combination has weight at least four. Now, the segment in block column seven is of weight zero only if the fourth row of the combination is one of rows fourteen, twenty and twenty-four. When the fourth row is row fourteen, the segment in block column five is of weight two unless the third row is row seven, in which case the segment in block column three is of weight two. When it's row twenty, the segment in block column five is of weight two unless the third row is row eight, in which case the segment in block column one is of weight two. Finally, if row twenty-four is involved, then the segment in column five is of weight two unless the third row is row nine, in which case the segment in block column eight is of weight two. Thus none of the combinations in this sub-case are of weight four.

The final sub-case we will now examine is that in which two rows come from distinct block rows in the block rows one to four and the other two come from distinct block rows in the block rows five to eight.

Two from top, two from bottom

We come now to the last sub-case, that in which two rows come from block rows one to four and two come from block rows five to eight, all in separate block rows. We can reduce the number of possibilities by noticing that when row one of B and a row from block row four are used, the combination is equivalent to a combination in which row one and a row from block row three are used. This is true since we can dih-cycle the row in the fourth block row back to the first row of B and cycle the first row by the same amount in which case it becomes one of the rows in block row three: b^0 and b^6 become b^{18} and b^0, b^0 and b^{14} become b^{10} and b^0 and b^0 and b^0 and b^{22} become b^2 and b^0.

Note that there are always four segments of the combinations in this sub-case that are of odd weight. These arise on the LHS thanks to each of the segments of weight two in the last two rows of the combination combining with an odd-weighted segments and two other even-weighted ones. Similarly on the RHS the weight two segments in each of the first two rows of the combination lead to odd-weighted segments in the combination. We thus need only show that the other four segments are not all of weight zero.

We now simply work through the possibilities using block rows two and three. There are four choose two possibilities for two block rows from the last four, which is six. We investigate these six possibilities for each of block rows two and three.

The first possibility using block row two that we check is that of block rows five and six. In this case the even-weighted segments are in block columns one, two, five and six. The segment in block column two is of weight two unless row eighteen of B is used, in which case that in block column five is of weight two unless row thirteen is used. Then the segment in block column six is of weight two unless row five is used, in which case that in block column one is of weight two.

When block rows five and seven are used then the even-weighted segments are in block columns two, four, five and six. That in block column two is always of weight two.

In the case of block rows five and eight, the segments in block columns one, four, five and six are of even weight. That in block columns four is of weight two unless row five of B is used. The segment in block column one is of weight two unless row fourteen in block row five is used, but then that in block column

five is always of weight two.

Using block rows six and seven the even-weighted segments are in block columns two, three, five and six. That in block column six is two unless row four of B is used, in which case that in block column three is always of weight two.

In the case of block rows six and eight the even weighted segments are in block columns one, three, five and six. That in block column one is always of weight two.

Finally, for combinations involving a row from block row two, when block rows seven and eight are involved the even-weighted segments are in block columns three, four, five and six. That in block column five is of weight two unless row nineteen is involved in the combination, in which case that in block column four is of weight two unless row four is involved. In that case that in block column three is of weight two unless row twenty-three is used, in which case that in block column six is of weight two.

We turn then to the cases involving a row from block row three. The first of these is that a row from each of block rows five and six is used. Note however, that we can cycle these two rows back so that one of them becomes the first row of B and the other becomes one of those in block row two of B. Hence this case has already been covered.

The next case is the one in which block rows five and seven are involved. In this case the even weighted segments are in block columns two, four, six and eight. That in block column six is always of weight two.

The third case is that in which a row is used from each of block rows five and eight. The even weighted segments are in block columns one, four, six and eight. That in block column four is always of weight two.

Fourth is the case that block rows six and seven are involved. The even-weighted segments are in block columns two, three, six and eight. That in block column two is of weight two unless row eighteen of B is used, in which case that in block column three is of weight two unless row five is used. Then that in block column eight is of weight two.

Next is the case in which block rows six and eight are involved. The even-weighted segments are in block columns one, three, six and eight. That in block column one is always of weight two.

Finally comes the case in which a row from each of block rows seven and eight are used. Like in the first case, however such combinations can be dih-cycled to a case in which these two rows reside in block rows one and two. Therefore, this case has already been covered.

Thus none of the combinations involving four rows from different block rows are of weight four. This completes the proof that no combination of four rows of B is of weight four. The minimum distance of $\mathcal{C}$ is thus twelve.

Conclusion

In this chapter we have seen that the $(48, 24, 12)$ extremal type II code can be constructed from a zero divisor in a group ring. The group ring in question is $\mathbb{Z}_2\mathbf{D}_{48}$, the dihedral group of order forty-eight over the finite field with two elements. We proved algebraically that the code is of dimension twelve, self-dual, doubly-even and can be generated as quasi cyclic of index two by a reverse circulant generator matrix. Most importantly we algebraically proved that the code is of minimum distance twelve.

In conjunction with the construction of the $(24, 12, 8)$ extended binary Golay code in the previous chapter the construction of the $(48, 24, 12)$ code here suggests that, in general, codes constructed in this way using zero divisors in dihedral group rings are quite good. In the next chapter we thus deal with more general constructions of such codes in dihedral group rings. Most interesting among the codes constructed in the chapter are the $(72, 36, 12)$ and $(96, 48, 16)$ type II codes. They are the best known type II codes of their lengths, and the existence of longer type II codes of their lengths is a famous open problem in coding theory.

Chapter 4

Further Type II Codes

In this chapter we will discuss some general properties of codes constructed from zero divisors in dihedral group rings. Along the way we outline some ideas for future work in the area of dihedral group ring codes. Towards the end of the chapter we give some zero divisors we have found that generate two codes that are the best known type II codes for their length: a $(72, 36, 12)$ code and a $(96, 48, 16)$ code.

We begin with section 4.1 where we discuss the general construction of type II codes from zero divisors in dihedral group rings. As discussed in the previous chapters type II codes are binary, self-dual and doubly even codes [8, p. 96]. Such codes are called extremal if their minimum distance achieves the upper bound $4\lfloor n/24 \rfloor + 4$ where n is the code's length [8, p. 270]. It is straight-forward to construct type II codes using the group rings. Proofs are provided in sections 4.3, 4.4, 4.6 and 4.7 showing that, given the right kind of zero divisor, the code it generates is automatically self-dual, doubly even, generated by a reverse circulant generator matrix and quasi cyclic of index two. Given a few further conditions on the zero divisor we can show algebraically that such codes are of minimum distance at least eight.

Illustrating these proofs, we give examples of zero divisors generating extremal type II codes of each length that is a multiple of eight, up to length forty-eight. Amongst them are two codes we have constructed in previous chapters. The $(8, 4, 4)$ extended Hamming code was constructed in chapter 1 using a zero divisor in the group ring $\mathbb{Z}_2\mathbf{D}_8$ consisting of the finite field with two elements $\mathbb{Z}_2$ and the dihedral group with eight elements $\mathbf{D}_8$. This was followed by the construction of the $(24, 12, 8)$ extended binary Golay code in chapter 2. It was constructed from a zero divisor in the group ring $\mathbb{Z}_2\mathbf{D}_{24}$ where $\mathbf{D}_{24}$ is the dihedral group with twenty-four elements. The proofs given here are more general forms of those given in those chapters.

For lengths forty-eight and above type II codes are extremal only if their minimum distances are at least twelve. This is the case for the $(48, 24, 12)$ type II code constructed in another dihedral group ring, $\mathbb{Z}_2\mathbf{D}_{48}$, in chapter 3. As we witnessed there, it is difficult to show algebraically that such codes are of minimum distances greater than eight. We can however employ some algebraic techniques to hasten the calculation of their minimum distances. These are discussed in section 4.10. They allow the quick analysis of the longer codes by computer.

Extremal type II codes of longer lengths than forty-eight have received much attention in the past. The existence of such codes for lengths seventy-two and ninety-six, amongst others, is unknown. Neil J. Sloane called for attention to be given to the case of length seventy-two in 1973 [22]. Furthermore, S. T. Dougherty and Masaaki Harada offered monetary prizes as recently as 2001 for the proof of such a code's existence or proof of its non-existence [16]. The problem is still open to date.

In section 4.11 we will give an example of a zero divisor we have found in the group ring $\mathbb{Z}_2\mathbf{D}_{72}$ that generates a $(72, 36, 12)$ type II code. While this code is not extremal, twelve is the greatest minimum distance for which a type II code of length seventy-two is known. Indeed should a $(72, 36, 16)$ code not exist then this is the greatest minimum distance for a type II code of length seventy-two. We were unable to find, using computer search, a zero divisor that generates a type II length seventy-two code of minimum distance sixteen.

Along with the extremal $(72, 36, 16)$ code, the existence of an extremal $(96, 48, 20)$ type II is a long-standing open problem. Again we were unable to find a zero divisor to generate such a code. However, a zero divisor generating a length ninety-six type II code of minimum distance sixteen was found. This is discussed in section 4.12. Sixteen is the highest minimum distance for which a length ninety-six type II code is known.

While we have almost exclusively dealt with type II codes in this thesis, it is quite easy to construct type I codes using the same techniques. Such codes are discussed in section 4.5. In section 4.13 we discuss some reasons why the generators we have listed throughout this thesis generate the codes they do. The goal of further research into this topic could be to construct longer type II codes with good minimum distances. We conclude the chapter with a brief discussion of groups other than the dihedral ones, over which we have found generators for some of the same codes as we have already constructed. There appears to be a connection between these groups and the automorphism groups of the codes.

Throughout the chapter we refer to possibilities for further research in the area of group ring codes. We begin now with a general discussion of dihedral codes.

4.1 Dihedral Codes

In the following chapter we will discuss some properties of codes generated by zero divisors in the group ring formed from the finite field with two elements and a general dihedral group with $2k$ elements. We denote the dihedral group by $\mathbf{D}_{2k} = \langle a, b \mid a^2, b^k, (ab)^2 \rangle$. So a is a generator of order two and b is a generator of order k. The zero divisors in question are of the form $u = 1 + a\mathbf{f}$ where $\mathbf{f}$ is a sum of powers of b, and where u^2 is zero. The codes we consider are the principal left ideals of such u's: $\mathcal{C} = (\mathbb{Z}_2\mathbf{D}_{2k})u$.

The length of a group ring code is the order of the underlying group. We will only consider type II codes. Codes generated by zero divisors of the form $1 + a\mathbf{f}$ are not always type II but we show in the following sections when they are and when they are not. Type II codes only exist at lengths a multiple of eight [9]. Thus in the following k we assume k is even. We now show that the codes in question are always of dimension k.

4.2 Dimension k

Let $\mathcal{C}$ be the code $(\mathbb{Z}_2\mathbf{D}_{2k})u$, generated by a zero divisor of the form $u = 1 + a\mathbf{f}$ where f is a sum of powers of the group element b and where u^2 equals zero. Under the listing $D_{2k} = \{1, b, b^2, \ldots, b^{k-1}, a, ab, ab^2, \ldots, ab^{k-1}\}$ the group ring matrix U of u has the form:

$$\left[\begin{array}{c|c} I & A \\ \hline A & I \end{array}\right]$$

where I is the k by k identity matrix and A is a k by k reverse circulant matrix. The row space of U is a vector form of the code $\mathcal{C}$, as discussed in section 1.9.2.

We use a well known result from linear algebra to show that the dimension of (this vector form of) $\mathcal{C}$ is k. This result is that the rank of a matrix plus the dimension of its null space is equal to the number of columns it has [17, p. 245]. It is used here to show that rank of U is less than or equal to the dimension of its null space. We first prove that the rows of U are contained in its own null space

The element u is equal to its own transpose. The transpose u^{T} of a group ring element u is the element in which the coefficient in u of each group element g is the coefficient of g^{-1}. Every element of the form ab^i in $\mathbf{D}_n$ for i from zero to $k = n/2$ is its own inverse. All of the elements in $a\mathbf{f}$ are of this form. The group identity element 1 is also its own inverse. Therefore the coefficient in u of each element g is that of $g^{-1} = g$ in the transpose u^{T} of u. This implies that U is equal to its own transpose and thus the rows of U are exactly its columns (albeit transposed). Since U^2 is zero the dot product of each row with each column

is zero and hence U's columns are contained in its null space. Hence all of U's rows are contained in its null space.

The rank of U is thus less than or equal to the dimension of its null space. The rank plus the dimension of the null space is $2k$. Therefore the rank of U is at most k and the dimension of the null space is $2k$ minus the rank. Now notice that the rank of U is at least k since the k by k identity matrix forms its top left block. Hence the rank and the dimension of the null space of U are both k. The dimension of $\mathcal{C}$, which is equal to the rank of U, is therefore k. We can use some of the above facts to easily see that the code $\mathcal{C}$ is in fact self-dual.

4.3 Self-Duality

In the last section we saw that the row space of U was contained in its null space. The row space of U is a vector form of the code $\mathcal{C}$ and thus the null space of U is the dual code of the code $\mathcal{C}$. Recall that the dual code of a code is the set of all vectors orthogonal to each of the codewords. Codes that are subsets of their dual codes are called self-orthogonal codes. Thus $\mathcal{C}$ is self-orthogonal.

The rank of U and the dimension of the null space of U are both k. Since one is contained in the other the row space and null space of U must in fact be the same space. Thus not only is the code $\mathcal{C}$ contained in its dual code, it is in fact exactly its dual code. Such codes are called self-dual codes and thus $\mathcal{C}$ is a self-dual code.

Every self-dual code has dimension half its length [10, p. 6], in accordance with our calculation of $\mathcal{C}$'s dimension. Self-dual codes also have the property that every non-zero codeword is of even weight [10, p. 338]. Some of these codes are doubly even, meaning that all of their non-zero codewords only have weights divisible by four. We now discuss doubly even codes as they arise in the context of our group ring codes.

4.4 Doubly Evenness

A doubly even code is a code for which every non-zero codeword has weight divisible by four. Type II codes are by definition doubly even. The generator u of the code $\mathcal{C}$ is a codeword itself. Thus for $\mathcal{C}$ to be doubly even u itself must be of weight divisible by four. Since u is of the form $1 + a\mathbf{f}$, this is the case if and only if $\mathbf{f}$ is of weight congruent to three modulo four.

We can easily prove that when u is of weight divisible by four the self-dual code it generates is doubly even. First observe that the rows of U are permutations of the first row, which is the vector form of u. Thus when u is

of weight divisible by four all of the rows of U are. Self-orthogonal codes with generator matrices whose rows are all of weight divisible by four are doubly even [10, p. 10]. We saw in section 4.3 that $\mathcal{C}$ is self-orthogonal.

Since the code $\mathcal{C}$ in vector form is the row space of the matrix U, some subset of the rows of U forms a basis for the code. These rows can be used to form a generator matrix for $\mathcal{C}$. Thus the self-orthogonal code $\mathcal{C}$ can be generated by a matrix all of the rows of which are of weight divisible by four. The code $\mathcal{C}$ is therefore doubly even when u is of weight divisible by four.

Group ring codes that are the principal left ideals of zero divisors of u's form where u is of weight divisible by four are thus type II codes. Note that the code $\mathcal{C}$ is a binary self-dual code irrespective of whether of not u is of weight divisible by four. When u is not of weight divisible by four the code is singly-even but not doubly even. Binary self-dual codes that are singly even but not doubly even are called type I codes. While in this thesis we are mainly interested in those of type II, we now take a brief digression to discuss those arising in the same way that are type I.

4.5 Type I Codes

Singly even codes are codes whose non-zero codewords each have weight divisible by two. Self-dual binary codes that are singly even but not doubly even are called type I codes [10, p. 339]. In section 4.3 we showed that a code $\mathcal{C} = (\mathbb{Z}_2\mathbf{D}_{2k})u$, where u is a zero divisor of the form $1 + a\mathbf{f}$ and $u^2 = 0$, is self-dual. All self-dual codes are singly even and some are doubly even [10, p. 338]. Thus when a binary self-dual code is not type II it is type I.

Dihedral codes as we have constructed them are doubly even whenever u is of weight divisible by four. The self-dual code $\mathcal{C}$ can not be doubly even when u is not of weight divisible by four. Thus the code must be singly even in that case. So $\mathcal{C}$ is a type I code when the weight of u is divisible by two but not by four.

Note the implication here that $u = 1 + a\mathbf{f}$ can only equal zero when squared if the weight of u is even. We've seen that such a u generates a self-dual code when it multiplies with itself to produce zero. The element u is a codeword itself and every codeword in a self-dual code is singly even. Thus u must be of even weight. This fact is also obvious from a purely theoretical group ring perspective. The element u when squared is zero if and only if $\mathbf{f}^{\mathrm{T}}\mathbf{f}$ is one. This is only possible if $\mathbf{f}$ is of odd weight since this is the only case in which the number of terms in the multiplication is odd.

As an example of a type I code we construct the unique [9] type I code of length eight. The principal left ideal of the zero divisor $1 + ab^3$ in the group ring $\mathbb{Z}_2\mathbf{D}_8$ is the code in question. The zero divisor is easily seen to multiply with

itself to produce zero. It is of the form $1 + a\mathbf{f}$ and so generates a self-dual code. The minimum distance of this code is two which, while being very small, is the best distance a type I code of length eight can achieve [9].

More interestingly, an extremal Type I code of length sixteen is the principal left ideal of the zero divisor $u = 1 + a(1 + b + b^2 + b^4 + b^6)$ in the group ring $\mathbb{Z}_2\mathbf{D}_{16}$. Again the element u when squared is zero. Since u is of weight six the code can not be doubly-even. A vector form of the code can be constructed as the row space of any group ring matrix of u. Such a matrix will only have rows of weight six and thus the code is singly even [10, p. 11]. The code is of minimum distance four which can be shown by simply calculating the weights of the combinations of the first row of U with each of the rows two to five. This fact will be proven in section 4.7. The proof relies on the fact that the code $\mathcal{C}$ is quasi cyclic of index two, a property we discuss now.

4.6 Quasi Cyclicity

Again we are considering the case of a zero divisor $u = 1 + a\mathbf{f}$ the group ring $\mathbb{Z}_2\mathbf{D}_{2k}$, where u^2 is zero. The code $\mathcal{C}$ is the principal left ideal of this element in the group ring and is of dimension k. We showed in section 4.2 that under the listing $D_{2k} = \{1, b, b^2, \ldots, b^{k-1}, a, ab, ab^2, \ldots, ab^{k-1}\}$ the group ring matrix U of the element u has the form:

$$\left[\begin{array}{c|c} I & A \\ \hline A & I \end{array}\right]$$

where I is the k by k identity matrix and A is a k by k reverse circulant matrix. The row space of the group ring matrix is a vector form of the group ring code $\mathcal{C}$, as discussed in section 1.9.2. Since the code is of dimension k and the first k rows of U are obviously linearly independent, the matrix $G = [I|A]$ is a generator matrix for the code in vector form.

Let $\underline{c}$ be a combination of rows of G and let $\underline{a}$ be the subvector of $\underline{c}$ containing its first k components and $\underline{b}$ that containing its last k. Then the concatenation $\underline{d} = \underline{ba}$ of the subvector $\underline{a}$ to the end of $\underline{b}$ must also be in $\mathcal{C}$. This is due to the fact that every combination of the rows of U is a codeword in $\mathcal{C}$. The submatrix consisting of the last k rows of U is of the form $[A|I]$. The vector $\underline{d}$ is the combination of the same rows of $[A|I]$ as are combined from G to form the codeword $\underline{c}$.

Codes of length $2k$ for which the k^{th} cyclic shift of each codeword is also a codeword in this way are called quasi cyclic codes of index two. Thus every code generated by an element $u = 1 + a\mathbf{f}$ where u^2 equals zero can be generated

quasi cyclically of index two by the generator matrix consisting of the first k rows of U. Note that we have made no reference in this discussion as to whether $\mathcal{C}$ is singly or doubly even. Thus both type I and type II codes constructed in this way are quasi cyclic of index two. This quasi cyclic property is very useful in assessing the minimum distance of such codes. We discuss this topic now in relation to type II codes.

4.7 Minimum Distance at Least Eight

In the following sections we will assume that the zero divisor $u = 1 + a\mathbf{f}$ is of weight divisible by four unless otherwise stated. This implies that u generates a type II code. It is in general easier to calculate the minimum distance of type II codes, as opposed to their singly even type I counterparts, due to the extra restriction on the possible weights of codewords. As in the previous sections the code $\mathcal{C}$ is the principal left ideal of u. Again the matrix $G = [I|A]$ is a generator matrix for the vector form of $\mathcal{C}$ consisting of the first k rows of U, u's group ring matrix according to the usual listing $\{1, b, b^2, \ldots, b^{k-1}, a, ab, ab^2, \ldots, ab^{k-1}\}$ of $\mathbf{D}_{2k}$.

The non-zero codewords of a type II code are each of weight divisible by four. Thus the only possible weights of non-zero codewords are four, eight, sixteen, and so on. The minimum distance of a linear code (which $\mathcal{C}$ is since $\mathbb{Z}_2$ is a field) is equal to the minimum of the weights of its non-zero codewords [10, p. 8]. Thus the minimum distance of a non-zero type II code is a multiple of four.

To show that such a code's minimum distance is exactly $4l$ for some positive integer l we need only show that no codeword is of weight $4m$ for m an integer from one to $l - 1$. In the case of the code $\mathcal{C}$ we will now show that no codeword is of weight four so long as the first row and k different two-row combinations of its generator matrix $G = [I|A]$ are not. We begin by discussing the fact that no combination of five or more rows of G can be of weight four.

4.7.1 Combinations of Five or More Rows

We can easily see that every combination of five or more rows of G is of weight at least weight eight. The subvector containing the first k components of a combination of i rows of G is of weight exactly i. This is due to the fact that it is the combination of i rows of the identity matrix. Hence every combination of five or more rows of G is of weight at least five. Thus such combinations of rows of G are not of weight four and must be of weight at least eight. The only way for a codeword can be of weight less than eight is if it is the combination of four or less rows of G. In the next section we see that every combination of four

rows is of weight at least eight.

4.7.2 Combinations of Four Rows

The subvector consisting of the first k components of the combination of four rows of G is of weight four. For such a combination to be of weight exactly four the subvector consisting of the last k components of the combination must thus be of weight zero. We will now see that the subvector consisting of the last k components is of weight at least one. We show this by proving that the rows of the matrix A are linearly independent.

The rows of A are linearly independent because the group ring matrix U when squared is equal to zero. Working block-wise:

$$\begin{aligned}
& U^2 = \underline{0}_{2k} \\
\Leftrightarrow & \begin{bmatrix} I & A \\ A & I \end{bmatrix} \begin{bmatrix} I & A \\ A & I \end{bmatrix} = \underline{0}_{2k} \\
\Leftrightarrow & \begin{bmatrix} I + A^2 & A + A \\ A + A & I + A^2 \end{bmatrix} = \begin{bmatrix} \underline{0}_k & \underline{0}_k \\ \underline{0}_k & \underline{0}_k \end{bmatrix} \\
\Leftrightarrow & \begin{bmatrix} I + A^2 & \underline{0}_k \\ \underline{0}_k & I + A^2 \end{bmatrix} = \begin{bmatrix} \underline{0}_k & \underline{0}_k \\ \underline{0}_k & \underline{0}_k \end{bmatrix}.
\end{aligned}$$

Thus U^2 is equal to zero if and only if A^2 is equal to the identity matrix.

This implies that A is its own inverse and matrices with inverses are of full rank. The rows of A are therefore linearly independent and so combinations of four of these are non-zero. Thus each combination of four rows of G is not of weight four. Hence the combinations of four rows of G are each of weight at least eight.

We are now in the position that no non-zero combination of rows of G is of weight less than eight unless some non-zero combination of three or less rows of G is. We will see in the next section that a three-row combination of G can only be of weight four if row one of G is.

4.7.3 One and Three Rows

We consider now the combinations of three rows of G and their relation to the single rows of G. Such combinations are of weight at least three due to the identity matrix in G. Consider the possibility that such a three-row combination of G is of weight four. Since the subvector of the first k components of the codeword are of weight exactly three, that of the last k must be of weight one.

In section 4.6 we showed that $\mathcal{C}$ as generated by G is quasi cyclic of index

two. Suppose the vector $\underline{c} = \underline{ab}$ is a combination of three rows of G that is of weight four. The result, $\underline{d} = \underline{ba}$, of switching the first k components with the last k is also a codeword, and is of the same weight as $\underline{c}$. The subvector $\underline{b}$ is of weight one and is therefore, in $\underline{d}$, the result of a linear combination of a single row of the identity matrix by itself. Thus $\underline{d}$ is one of the rows of G. A combination of three rows of G can only therefore be of weight four if one of the rows of G is of weight four.

Every row of G is a permutation of the first row and hence has the same weight as this first row. The weight of a single row of G is therefore only of weight less than eight if the first row is. When it is not, the only combinations of rows of G that could possibly be of weight less than eight are those of two-row combinations. These are discussed in the next section.

4.7.4 Two Rows

We now discuss the possibility that a two-row combination of G is of weight four. If no such combination is of weight four then, provided that the first row of G is not of weight four, the code $\mathcal{C}$ is of minimum distance at least eight. In the following we prove that each combination of two rows of G is equal in weight to at least one of the combinations of row one with one of the rows two to $k/2 + 1$ of G.

Let r_{i+1} be the $(i+1)^{\text{th}}$ row of G for i from zero to $k-1$. Recall from section 1.9.2 that the group ring codeword corresponding to r_{i+1} is $b^i u$. Thus the combination of two distinct rows, r_{j+1} and r_{k+1}, of G for $0 \leq j < k \leq k-1$, corresponds to the group ring codeword $b^j u + b^k u$. Multiplying this group ring codeword by the inverse b^{-j} of b^j will not affect its weight. Thus it is equal in weight to the group ring codeword $u + b^{k-j}u$. In vector form this codeword is the combination of rows one and $(k-j)+1$ of G, where the calculation $(k-j)$ is done modulo k in accordance with the group multiplication. Thus the combination of two rows of G is equal to at least one combination of row one of G with one of the other rows of G.

We could likewise have multiplied the original group ring codeword $b^j u + b^k u$ by b^{-k}, leaving its weight intact. This would result in the codeword that is the group ring form of the combination of rows one and $(j-k)+1$ of G. Thus the combination of rows j and k of G is in fact equal in weight to the two combinations of row one of G with each of rows $(j-k)+1$ and $(k-j)+1$. Modulo k the two numbers $j-k$ and $k-j$ are both non-zero but sum together to give zero. Therefore either they are both $k/2$ or one is congruent to an integer between one and $(k/2)-1$ inclusive. At least one of the rows $(j-k)+1$ and $(k-j)+1$ is thus one of rows two to $k/2+1$ of G.

To check that every combination of two rows of G is not of weight four we therefore need only check that the combinations of row one with each of rows two to $k/2+1$ are not. There are $k/2$ such combinations. We saw in section 4.7.3 that all of the other non-zero combinations of G are of weight at least eight if the first row of G is. Therefore to prove that a code $\mathcal{C}$ is of minimum distance at least eight we need only check $k/2+1$ different combinations of rows of the generator matrix G. This is quite a nice result as the total number of codewords in such a code $\mathcal{C}$ is 2^k.

Note that the fact that we need only check the weight of these given $k/2$ two-row combinations of G can be extended to checking that the dot product of distinct rows of A is zero. In section 4.7.2 we showed that u^2 was equal to zero if and only if A^2 was equal to the identity matrix. Since A is symmetric[1] it is equal to zero when squared if and only if the dot product of each pair of distinct rows is zero and that of each row with itself is one. We can easily adapt the above proof to show that the dot product of each pair of distinct rows of A is zero if and only if that of row one with each of rows two to $k/2+1$ is. The generator u is of weight divisible by four and so $\mathbf{f}$ is of odd weight and so is each row of A. The dot product of each row of A with itself is thus one. These observations are useful when searching for zero divisors of the form $u = 1 + \mathbf{f}$ with u^2 equal to zero.

The idea that the minimum distance of the code $\mathcal{C}$ is at least eight works quite nicely on zero divisors that generate codes of length less than forty-eight. In the next section we show that, using the techniques just discussed, we can find generator for extremal type II codes for every possible length less than forty-eight.

4.8 Up To Length Forty-Eight

The highest minimum distance a type II code of length less than twenty-four can have is four [10, p. 346]. The maximum a type II code of length at least twenty-four and up to length forty-eight can have is eight [10, p. 346]. Codes achieving these minimum distances are termed 'extremal' [10, p. 346]. We have been able to find zero divisors in the relevant group rings that generate extremal codes of every length under forty-eight. We used the programs listed in appendix A to find them. Remember that type II codes are only ever a multiple of eight. The proofs in the previous sections show that they are principal ideals in their dihedral group rings, self-dual, doubly even, quasi cyclic of index two, generated by reverse circulant generator matrices and that they are of their

[1] A consequence of it being reverse circulant.

claimed minimum distance.

We begin with the $(8, 4, 4)$ extended Hamming code, which was discussed in section 1.11. The code is of length eight so the dihedral group ring in question is $\mathbb{Z}_2\mathbf{D}_8$, that of the finite field with two elements $\mathbb{Z}_2$ and the dihedral group with eight elements $\mathbf{D}_8 = \langle a, b \mid a^2, b^4, (ab)^2 \rangle$. The only elements of the form $1 + a\mathbf{f}$, where $\mathbf{f}$ is sum of powers of the generator b, in this group ring that are of weight a multiple of four are then $1 + a(1 + b + b^2)$, $1 + a(1 + b^2 + b^3)$, $1 + a(1 + b + b^3)$ and $1 + a(b + b^2 + b^3)$. Multiplying any of these elements by themselves gives zero. Hence they all generate self-dual codes that are doubly even. Since such a code has minimum distance a multiple of four, the minimum distance of the codes generated by each of these is four.

The next length of code in the series of extremal type II codes is sixteen. Again, type II codes of length sixteen have minimum distance at most four. We found sixteen elements in $\mathbb{Z}_2\mathbf{D}_{16}$ that generate such a code. We denote $\mathbf{D}_{16}$ as $\langle a, b \mid a^2, b^8, (ab)^2 \rangle$. They are the elements $1 + ab^i(1 + b^2 + b^4)$ and $1 + ab^i(1 + b + b^2 + b^3 + b^4 + b^5 + b^6)$ for i from zero to seven. Note that in section 2.10.1 we showed that then so should the elements $1 + ab^j(1 + b^2 + b^4)^{\mathrm{T}}$ and $1 + ab^j(1 + b + b^2 + b^3 + b^4 + b^5 + b^6)^{\mathrm{T}}$ for j from zero to seven generate the code. This is indeed the case, however those elements are all equal to one of the former types of elements, giving only sixteen unique generators.

We now move on to the case of length twenty-four. At length twenty-four the upper bound $(4\lfloor n/24 \rfloor + 4)$ on the minimum distance of a type II code increases from four to eight [10, p. 346]. The extended binary Golay code is the unique extremal type II code of this length [10, p. 401]. We showed in chapter 2 that it is generated by twenty-four different elements. These are the elements $1 + a\mathbf{f} = 1 + a(b + b^2 + b^4 + b^5 + b^6 + b^7 + b^9)$, $1 + ab^i\mathbf{f}$ for i from one to eleven and $1 + ab^j\mathbf{f}^{\mathrm{T}}$ for j from zero to eleven.

The next length that is a multiple of eight is thirty-two. We searched for elements of the form $1 + a\mathbf{f}$ in the group ring $\mathbb{Z}_2\mathbf{D}_{32}$ that generated codes of minimum distance eight. We found one hundred and twenty-eight generators of codes of minimum distance eight. Half of these are the elements $1 + ab^i(1 + b^3 + b^{10} + b^{11} + b^{12} + b^{13} + b^{14})$, $1 + ab^i(1 + b^5 + b^6 + b^{10} + b^{11} + b^{12} + b^{13})$, $1 + ab^i(1 + b^2 + b^5 + b^7 + b^{12} + b^{13} + b^{14})$ and $1 + ab^i(1 + b^4 + b^5 + b^7 + b^{10} + b^{13} + b^{14})$ for i from zero to sixteen. The other half are same elements with the $\mathbf{f}$ part transposed.

The only length left before forty-eight is forty. The group ring is then $\mathbb{Z}_2\mathbf{D}_{40}$. We found nine hundred and twenty $(40, 20, 8)$ type II code generating elements of the form $1 + a\mathbf{f}$ in the group ring. Some are of weight seven and some of weight eleven. An example of a weight seven generator is $1 + a(1 + b + b^3 + b^4 + b^{14} + b^{15} + b^{16})$ and that of a weight eleven generator is $1 + a(1 + b^2 + b^4 + b^7 + b^9 + b^{10} + b^{12} +$

$b^{13} + b^{16} + b^{17} + b^{18}$). An interesting topic for further research would be to asses the equivalence of the codes generated by these elements.

The upper bound on the minimum distance of codes of length forty-eight and above is greater than eight. Unfortunately we have not been able to find nice quick results to prove that the minimum distance of such a type II code is larger than eight. To prove that the minimum distance is twelve for instance, we must prove that no combination of rows of G is of weight four or eight, as opposed to just four. The proof we used in the last chapter to prove that the minimum distance of the $(48, 24, 12)$ type II code is twelve was complex and relied on the specific properties of the zero divisor used to construct the code. It can therefore not be easily adapted to the general case. We can however, use some of the properties of the construction to vastly reduce the number of combinations of rows of G that must be checked to verify the code is of a general minimum distance. We discuss these properties and their uses in the next two sections.

4.9 Dih-Cycling

In the previous chapter we discussed the idea of dih-cycling three-row and four-row combinations of the basis elements given there for the $(48, 24, 12)$ type II code. Here in this section we discuss the fact that dih-cycling works for any code of the form we have been talking about. Let $u = 1 + a\mathbf{f}$ be an element in the group ring $\mathbb{Z}_2\mathbf{D}_{2k}$. As we have been doing all along, we let $\mathbf{D}_{2k} = \langle a, b \mid a^2, b^k, (ab)^2 \rangle$ and then $\mathbf{f}$ is a sum of powers of b. Furthermore we assume that u^2 is equal to zero. The first k rows of the group ring matrix of u according to the listing $\{1, b, b^2, \ldots, b^{k-1}, a, ab, ab^2, \ldots, ab^{k-1}\}$ of $\mathbf{D}_{2k}$ then form a generator matrix for the code $\mathcal{C} = (\mathbb{Z}_2\mathbf{D}_{2k})u$. These k rows correspond to the group ring elements $u, bu, b^2u, \ldots, b^{k-1}u$ as discussed in section 1.9.2. These elements thus form a basis for the group ring code $\mathcal{C} = (\mathbb{Z}_2\mathbf{D}_{2k})u$ over $\mathbb{Z}_2$.

Any combination of those basis elements is equal in weight to at least one involving u. Let $b^{i_1}u + b^{i_2}u + \ldots + b^{i_l}u$ be such a combination of l elements for l a positive integer with $1 \leq l < k$. We can multiply this combination by the group ring element by b^{-i_j} for any j and it is still a combination of basis elements. In particular one of the basis elements in the new combination is u. Thus each combination of l basis elements is equal in weight to a combination of l basis elements where one of those is u. In the next section we discuss how dih-cycling can reduce the calculations in the determination of the minimum distance of a dihedral code.

4.10 Minimum Distance Checking

We use the same notation here as in the last section. The code $\mathcal{C}$ is the span of the elements $u, bu, b^2u, \ldots, b^{k-1}u$. An arbitrary codeword is a combination $b^{i_1}u + b^{i_2}u + \ldots + b^{i_l}u$ for i_j an integer for all j. To check that the minimum distance of the code $\mathcal{C}$ is a given value d we check that every non-zero combination of them is of weight at least d [10, p. 8]. To do this we can just check those combinations involving u, since as we saw in the last section we can dih-cycle any combination to become one involving u leaving its weight intact. Note that dih-cycling does not change the number of basis elements with non-zero coefficient in a combination.

Of course, we can dih-cycle according to any of the indices i_1, i_2, ..., i_l in the combination $b^{i_1}u + b^{i_2}u + \ldots + b^{i_l}u$ and arrive at a combination of basis elements involving u. We can thus, out of all these dih-cycled combinations of equal weight, pick one such combination and check only its weight. Consider the quantities $i_k - i_j$ modulo k for all $1 \leq j < k \leq l$. At least one of these has the property that it is less than or equal to all of the others. Since we are free to dih-cycle any of the basis elements in a combination until it becomes u, we can therefore choose to check only the weights of the combinations $u + b^{m_1}u + \ldots + b^{m_{l-1}}u$ where $m_1 \leq (m_k - m_j)$ for all k and j.

Remember of course that this dih-cycling technique is applied after many of the 2^k combinations of the basis elements have already been ruled out as possibly having low minimum distance. Every combination of l such basis elements has weight at least l since the first k components of the first k rows of the group ring matrix U is the identity matrix. Thus to show that the minimum distance is some multiple of four d we need only show that every combination of less than $d-3$ rows is of weight at least d. Furthermore no set of $d-4$ rows can be of weight $d-4$ as we showed in section 4.7.2. The quasi cyclic nature of the code also reduces the possibilities. We saw in section 4.7.3 that if for instance three of the rows combine to a vector of weight four then at least one row is of weight four.

These techniques are extremely useful in dealing with large dihedral codes. As examples we now discuss two codes, one of length seventy-two and one of length ninety-six.

4.11 A $(72, 36, 12)$ Code

As discussed in the introduction to this chapter the proof or disproof of the existence of a putative $(72, 36, 16)$ type II code is a long-standing open problem in coding theory. We performed an exhaustive search for zero divisors of the

form $1 + a\mathbf{f}$ in $\mathbb{Z}_2\mathbf{D}_{72}$ that generate codes of minimum distance sixteen. As before, the zero divisors we searched had the property that u^2 was equal to zero and $\mathbf{f}$ was a sum of powers of the generator b where $\mathbf{D}_{72} = \langle a, b \mid a^2, b^{36}, (ab)^2 \rangle$. No such zero divisors were found. We did however discover zero divisors that generate type II $(72, 36, 12)$ codes. Twelve is the best known minimum distance for such a type II code of length seventy-two to date.

We found one thousand, seven hundred and sixty-four such zero divisors of the form $1 + a\mathbf{f}$. Two examples of these are $1 + a(1 + b + +b^2 + b^5 + b^6 + b^7 + b^8 + b^{10} + b^{11} + b^{12} + b^{14} + b^{15} + b^{16} + b^{17} + b^{19} + b^{22} + b^{23} + b^{25} + b^{26} + b^{27} + b^{28} + b^{29} + b^{30})$ and $1 + a(1 + b + b^2 + b^5 + b^6 + b^7 + b^8 + b^{10} + b^{11} + b^{13} + b^{14} + b^{15} + b^{17} + b^{18} + b^{19} + b^{21} + b^{22} + b^{23} + b^{25} + b^{26} + b^{27} + b^{28} + b^{29})$. As discussed in section 4.7, it is easy to show that these elements generate codes of minimum distance at least eight. A computer check, perhaps using the techniques in section 4.10, will convince the reader that these elements actually generate type II codes of minimum distance twelve. In the next section we discuss a longer code, of length ninety-six, which also has the best known minimum distance for its type and length.

4.12 A $(96, 48, 16)$ Code

As well as searching for a $(72, 36, 16)$ type II code, we also conducted a search for a $(96, 48, 20)$ type II code. Again the existence of such a code is a long-standing open problem. We were not able to find a generator of the form $1 + a\mathbf{f}$ for such a code, in $\mathbb{Z}_2\mathbf{D}_{96}$. The search was not exhaustive however, as the search space is extensive and beyond the ability of our algorithms and computers.

We were able to find generators of $(96, 48, 16)$ type II codes, however. Two of these are the zero divisors $1 + a(1 + b^2 + b^4 + b^5 + b^6 + b^7 + b^8 + b^{10} + b^{11} + b^{14} + b^{15} + b^{17} + b^{18} + b^{22} + b^{23} + b^{24} + b^{25} + b^{26} + b^{31} + b^{33} + b^{36} + b^{38} + b^{39})$ and $1 + a(1 + b + b^3 + b^6 + b^8 + b^{13} + b^{14} + b^{15} + b^{16} + b^{17} + b^{21} + b^{22} + b^{24} + b^{25} + b^{28} + b^{29} + b^{31} + b^{32} + b^{33} + b^{34} + b^{35} + b^{37} + b^{39})$. Again the techniques in section 4.10 can be employed to show these generate codes of minimum distance sixteen.

Length ninety-six is at the very limit of the abilities of our computers to date. Further research into the algebraic nature of the generators might help to discover why the generators we have found generate the codes they do. In chapter 2 we discussed some properties unique to the generators of the extended binary Golay code in their group ring. In the next section we discuss these properties further and in terms of the zero divisors listed above for the longer codes.

4.13 Properties of the Generators

The second part of chapter 2 was dedicated to showing that the twenty-four zero divisors of the form $1 + a\mathbf{f}$ listed there were the only ones of that form in the group ring $\mathbb{Z}_2\mathbf{D}_{24}$ that could possibly generate the extended binary Golay code. The reason behind pursuing such a result was the potential of finding out what made those generating elements work. Perhaps in the future we will discover general properties of zero divisors of this form in dihedral group rings that always generate codes that are of good minimum distance.

A unique property we discovered to the generators of the extended binary Golay code was that their multiset of differences was of the form $(\mathbf{10}\times 4)+(\mathbf{1}\times 2)$. Remember that this means that ten of the non-identity powers of the group element b appear four times and one of them appears twice in the multiset of differences $\mathcal{D} = \{b^{k-l} \mid b^k, b^l \in \mathbf{f}, k \neq l\}$ of $\mathbf{f}$ where the generator is $u = 1 + a\mathbf{f}$. This property was sufficient to guarantee that the zero divisor generated the code.

We also, in the previous chapter, discussed the $(48, 24, 12)$ type II code. All of the zero divisors in $\mathbb{Z}_2\mathbf{D}_{48}$ that are listed there have multisets of differences of the form[2] $(\mathbf{13}\times 10)+(\mathbf{10}\times 8)$. We have found this form to not be unique to those generators however. Some zero divisors of the form $1 + a\mathbf{f}$ have a mutliset of differences of that form and do not generate a code of minimum distance twelve. In our efforts to prove algebraically, as we did, that the minimum distance of the code is twelve we discovered that the zero divisors that do generate a code of minimum distance twelve all had generator matrices of the form $G = [I|A]$ where rows one, nine and seventeen have exactly six 1-components in common. These three rows are evenly spaced throughout the reverse circulant generator matrix. Along with the multiset of differences, this property appears sufficient to lead to the generation of the $(48, 24, 12)$ type II code. This eventually led to our discovery that the group ring listing in which the group elements corresponding to those three rows come first enabled us to prove the minimum distance of the code.

In the length seventy-two case however, two different values are allowed for the number of 1-components shared between three evenly spaced rows throughout the generator matrix. It seems that these rows can share either six or nine 1-components and still manage to generate a minimum distance twelve code. All of those with nine shared generate a code of minimum distance twelve, but some of those with six shared do not. Further research into the sets of differences and the numbers of 1-components shared between three rows evenly spaced throughout the generator matrices of good dihedral codes may lead to the ability

[2]The form of a multiset of differences is defined in section 2.12.

to generate good codes of longer length using the same techniques as given in this thesis. Another interesting topic for further research would be the investigation of other group rings in which it is possible to find generators for the same codes, as discussed in the next section.

4.14 Using Other Regular Subgroups

One of the reviewers of our publication of our construction of the extended binary Golay code [19] referred to the fact that the dihedral group is a regular subgroup of the automorphism group of the code. The automorphism group of the extended binary Golay code is the Mathieu group on twenty-four points $\mathcal{M}_{24}$ [10, p. 251]. The reviewer conjectured that, having found generators for the code in the dihedral group ring, we should be able to find generators for the code in group rings using any of the regular subgroups of the automorphism group of the code. He was correct.

Using some of the GAP code listed in appendix A we were able to find generators of the code in the group rings composed of the finite field with two elements $\mathbb{Z}_2$ and each of the following groups: $\mathbf{D}_{24}$; $\mathbf{C}_2 \times \mathbf{A}_4$, the direct product of the cyclic group of order two and the alternating group of order twelve; $\mathbf{S}_4$, the symmetric group of degree four; $\mathbf{C}_3 \times \mathbf{D}_8$, the direct product of the cyclic group of order three and the dihedral group of order eight; and $(\mathbf{D}_8 \times \mathbf{C}_3)$ the direct product of the dihedral group of order eight with the cyclic group of order three. These are all of the regular subgroups of $\mathcal{M}_{24}$. Investigation of the nature of the connection between generators of the same code in different group rings would be an extremely interesting topic for further study. For more on regular subgroups of the automorphism groups of group ring matrices the reader is referred to Horadam's book on the subject of Hadamard matrices [6]. This concludes our discussion of general dihedral codes.

Conclusion

In this thesis we have seen that a number of type II codes can be generated by zero divisors in group rings. The group rings in question are dihedral groups over the finite field with two elements. The codes have been constructed in much the same way as cyclic codes in the past have been constructed in residue class rings. Among these codes are many extremal type II codes.

The zero divisors are of the form $1 + a\mathbf{f}$ where a is the generator of order two of the group and $\mathbf{f}$ is a sum of powers of the other generator. The advantages of working with such zero divisors are many. In chapter 2 the zero divisors offered constructions of the code in which it was immediately obvious that the code was self-dual, doubly even and a principal left ideal of the zero divisor in the group ring. A reverse circulant generator matrix for the code was then given, which generated the code as quasi cyclic of order two. Using a little algebra it was readily verifiable that the code was of minimum distance eight.

The zero divisors given in chapter 3 generated the $(48, 24, 12)$ extremal type II code. Again the same properties were readily identifiable in this case. The code was seen to be self-dual, doubly even, quasi cyclic of index two and generated by a reverse circulant matrix. We saw that the code was of minimum distance at least eight. The proof that the code was actually of minimum distance twelve was lengthy, but nonetheless algebraic.

Finally in chapter 4 we discussed the more general case of constructing a type II code in a dihedral group ring. Generators of numerous type II codes were given, each submitting to the general proofs that such codes were self-dual, doubly even, quasi cyclic of index two, reverse circulantly generated and of minimum distance at least eight. Properties of the codes were discussed that allow the rapid calculation of such codes minimum distance by computer. Some examples of type I codes were also given that submitted readily to many of the proofs.

We hope to have convinced the reader by this stage that the use of the dihedral group rings in the construction of self-dual error correcting codes warrants further research.

Thank you for reading.

Appendix A

Computer Programs

In this appendix some snippets of code we wrote during the course of this thesis are listed. These snippets can be used to easily construct whole programs for finding zero divisors.

Finding Zero Divisors in C

The following C functions attempt to find zero divisors of the form $1 + a\mathbf{f}$ in the dihedral group ring $\mathbb{Z}_2\mathbf{D}_{2k}$. The dihedral group $\mathbf{D}_{2k}$ is generated by two generators, a of order two and b of order k. The element $\mathbf{f}$ is a sum of powers of b. The last k bits of the sixty-four bit integer f are the coefficients in $\mathbf{f}$ according to the listing of group elements $\{ab^{k-1}, \ldots, ab^2, ab, a\}$.

Two preliminary functions are needed here to facilitate the main snippets of code. The first of these is called *weight* which calculates the Hamming weight of a codeword and returns this as an integer. The function code is not listed here, as the Hamming weight calculation we used is the standard one for calculating the weight of a sixty-four bit unsigned integer. The second, also not listed but easily written, is called *ith_row* which returns the i^{th} cycle of a codeword. It requires two macros, K and *MASK*, to be defined. The first is the dimension of the code we are looking for and the second is a bit mask for the last K components of a sixty-four bit integer. The function *usq_zero* then returns one if and only if $1 + a\mathbf{f}$ squared is zero. It is listed in listing 1.

Minimum Distance Eight

The previous code can easily be adapted to ensure that the code that is the principal left ideal of u in the group ring is of minimum distance at least eight.

```
int usq_zero(unsigned long long f) {
  if ((weight(f) & 1) == 0)
          return(0);

  for (int i = 1; i <= K/2; i++)
    if (weight(f & ith_row(f, i)) & 1)
          return 0;

  return 1;
}
```

Listing 1: Test whether $(1 + a\mathbf{f})^2$ is zero.

Here, as in the previous listing, we are using the techniques described in chapter 4. Such an adaptation is given in listing 2.

```
int min_dist_8(unsigned long long f) {
  if (weight(f) < 7)
    return 0;

  for (int i = 1; i <= K/2; i++)
    if (weight(f ^ ith_row(f, i)) < 6)
          return 0;

  return 1;
}
```

Listing 2: Test whether the code has minimum distance eight or more.

General Groups

The GAP code in listing 3 can be used to create the group matrix of any listing of a group. The group listing is denoted by *listing*.

This can be used along with the code in listing 4 to create the group ring matrix of an element u. Here u is a list containing the coefficients of the elements in the group listing in order in u. The variable *gmat* is the group matrix according to the listing and can be the return value of the previous function *ListingToGMat*.

```
ListingToGMat := function(listing)
  local ROW_LABS, i, G_MAT;
  ROW_LABS := List(listing, Inverse);

  G_MAT := [];
  for i in listing do
    Add(G_MAT, i*listing);
  od;

  return G_MAT;
end;;
```

Listing 3: Create the group matrix.

```
VectorToRGMat := function(u, gmat)
  local RGMat, i, j, k, N;
  RGMat := [];
  N := Size(gmat[1]);
  for i in [1..N] do
    Add(RGMat, []);
    for j in [1..N] do
      for k in [1..N] do
        if (gmat[i][j] = gmat[1][k]) then
          Add(RGMat[i], u[k]);
        fi ;
      od ;
    od ;
  od;
  return RGMat;
end;;
```

Listing 4: Create the group ring matrix.

Bibliography

[1] F. Bernhardt, P. Landrock, and O. Manz, "The extended Golay codes considered as ideals," *J. Comb. Theory*, vol. 55, pp. 235–246, Sep. 1990.

[2] R. E. Blahut, *Algebraic Codes for Data Transmission.* Cambridge University Press, 2003.

[3] *GAP – Groups, Algorithms, and Programming, Version 4.4.10*, The GAP Group, 2008. [Online]. Available: http://www.gap-system.org

[4] M. J. E. Golay, "Notes on Digital Coding," *Proceedings of the IRE*, vol. 37, pp. 657–657, 1949.

[5] T. A. Gulliver and M. Harada, "Double Circulant Self-Dual Codes over $\mathbb{Z}_{2k}$," *IEEE Trans. Inf. Theory*, vol. 44, pp. 3105–3123, Nov. 1998.

[6] K. J. Horadam, *Hadamard Matrices and their Applications.* Princeton University Press, 2006.

[7] S. K. Houghten, C. W. H. Lam, L. H. Thiel, and J. A. Parker, "The Extended Quadratic Residue Code is the only (48,24,12) Self-Dual Doubly-Even Code," *IEEE Trans. Inf. Theory*, vol. 49, pp. 53–59, Jan. 2003.

[8] W. C. Huffman and V. Pless, *Handbook of Coding Theory.* Elsevier Science, 1998, vol. 1.

[9] W. C. Huffman, "On the classification and enumeration of self-dual codes," *Finite Fields Appl.*, vol. 11, pp. 451–490, Aug. 2005.

[10] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes.* Cambridge University Press, 2003.

[11] G. Hughes, "Constacyclic Codes, Cocycles and a $u + v|u - v$ Construction," *IEEE Trans. Inf. Theory*, vol. 46, pp. 674–680, Mar. 2000.

[12] P. Hurley and T. Hurley, "Module Codes in Group Rings," in *IEEE Symp. Inf. Theory 2007*, Jun. 2007, pp. 1981–1985.

[13] P. Hurley and T. Hurley, "Codes from zero divisors and units in group rings," *Int. J. Information and Coding Theory*, vol. 1, pp. 57–87, 2009.

[14] T. Hurley, "Group rings and rings of matrices," *Int. J. of Pure and Applied Mathematics*, vol. 31, pp. 319–335, 2006.

[15] R. Jenson, "A Double Circulant Presentation for Quadratic Residue Codes," *IEEE Trans. Inf. Theory*, vol. 26, pp. 223–227, Mar. 1980.

[16] J.-L. Kim, "A Prize Problem in Coding Theory," *Gröbner Bases, Coding, and Cryptography*, vol. 2, Jul. 2008.

[17] S. M. Lane and G. Birkhoff, *Algebra*, 3rd ed. AMS Chelsea, 1999.

[18] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[19] I. McLoughlin and T. Hurley, "A Group Ring Construction of the Extended Binary Golay Code," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4381–4383, Sep. 2008.

[20] C. P. Milies and S. K. Sehgal, *An Introduction to Group Rings*. Kluwer, 2002.

[21] M. Musa, "On Some Double Circulant Binary Extended Quadratic Residue Codes," *IEEE Trans. Inf. Theory*, vol. 54, pp. 898–905, Feb. 2008.

[22] N. Sloane, "Is There a (72,36) d = 16 Self-Dual Code?" *IEEE Trans. Inf. Theory*, vol. 19, pp. 251–251, Mar. 1973.

[23] N. Sloane and J. G. Thompson, "Cyclic Self-Dual Codes," *IEEE Trans. Inf. Theory*, vol. 29, pp. 364–366, May 1983.