# INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

**The quality of this reproduction is dependent upon the quality of the copy submitted.** Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

**UMI**

A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor MI 48106-1346 USA
313/761-4700 800/521-0600

# NON-ABELIAN GENERALIZATION OF CYCLIC CODES

by

**Yiren Shao**

A dissertation submitted to the Graduate Faculty
in Engineering in partial fulfillment of the requirements
for the degree of doctor of philosophy,
The City University of New York

1997

This manuscript has been read and accepted for the Graduate Faculty in Engineering in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

May 20, 1997 — Prof. Richard Tolimieri

Date — Chair of Examining Committee

5/28/97 — Dean Gerard Lowen

Date — Executive Officer

Prof. Joseph Barba

Prof. Patrick Combettes

Prof. Michael Conner

Dr. Myoung An

Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

## Abstract

NON-ABELIAN GENERALIZATION OF CYCLIC CODES

by

Yiren Shao

Advisor: Professor Richard Tolimieri

Every cyclic code of length n over a field F may be viewed as an ideal of the group algebra FG of the cyclic group G of order n. This observation creates the following generalization: let G be a finite non-abelian group, each left ideal W of the group algebra FG is called a non-abelian code over F. Based on the Clifford's theory of idempotents, algorithms for computing the complete set of primitive orthogonal idempotents for non-abelian groups of the form $A \triangleleft H$ (semidirect product), where A is a normal finite abelian group and H is an arbitrary finite group, and algorithms for constructing non-abelian codes by idempotents of non-abelian group algebra are developed. Then non-abelian Dihedral codes are constructed, characteristics of these codes are tested, and specific characterization for non-abelian Dihedral codes in Fourier transform domain is found. Based on these spectral characterization, encoding algorithm and decoding algorithm for non-abelian Dihedral codes are developed.

To
my Parents
and
my wife Cheng-jun Cao

# CONTENTS

# LIST OF FIGURES

# 1 INTRODUCTION

Digital signal processing is an engineering subject with many branches. Among them is the theory of error-control codes, a special topic with its own goals and its own arithmetic systems. Within these arithmetic systems, however, the most fruitful techniques are the familiar operations of signal processing--operations that involve convolutions, Fourier transforms, filters, and shift registers. Error-control coding is a topic with its own history and charm and has faces that touch many other subjects ([3], [7], [22]-[28], [33], [34], [37], [38], [43], [49], [56], [57], [59]).

The engineering problem treated by the subject of error-control coeds is that of protecting digital data against the errors that occur during transmission through a communication channel. These codes, however, have many other applications. Codes are used to protect data in computer memories and on digital tapes and disks, and to protect against circuit malfunction or noise in digital logic circuits. Codes have also been used for the compression of data, and coding theory is closely related to the theory of the design of statistical experiments.

Cyclic codes over finite fields constitute a class of codes

that has been studied extensively ([1], [2], [12], [13], [15], [18]-[21], [29], [35], [39]-[42], [46], [47], [50]-[52], [54], [55], [58]). It is well known that every cyclic code of length n over a field F may be viewed as an ideal of the group algebra FG of the cyclic group G of order n ([10], [44]). This observation suggests the following generalization: let G be a finite group, each left ideal W of the group algebra FG is called a code of length n over F. The left ideal W is also simply referred to as FG-code. If G is cyclic, abelian or non-abelian, then every ideal W of FG is denoted as cyclic code, abelian code or non-abelian code, respectively.

A class of codes, called abelian codes, that includes cyclic codes as a subclass has been studied by several authors ([5], [6], [14], [17], [36]). Camion [14] has recently shown that there exist ideals in abelian group algebras (i.e., abelian codes) that are not obtainable by taking direct products of cyclic codes. Berman ([5], [6]) has also proven the existence of asymptotically good abelian codes and shown that under certain conditions the general class of abelian codes has better error correction capabilities than the class of cyclic codes. Cyclic codes over finite fields have been studied in the transform domain ([8], [9]) using discrete Fourier transform (DFT) over finite fields.

In this work, we will study non-abelian codes, using discrete Fourier transform (DFT) over finite fields. We will develop algorithms for computing the complete set of primitive orthogonal idempotents based on the Clifford's theory of idempotents, construct non-abelian Dihedral codes by the complete set of primitive orthogonal idempotents of Dihedral group algebra, and investigate transform domain characterization for Dihedral codes; We will also develop encoding algorithm for Dihedral codes, test characteristic, and develop decoding algorithm for Dihedral codes.

## 1.1 Elementary Concepts

Suppose that all data of interest can be represented as binary (coded) information; that is, as a sequence of zeros and ones. This binary information is to be transmitted through a channel that causes occasional errors. The purpose of a code is to add extra symbols to the information symbols so that errors may be found and corrected at receiver. That is, a sequence of data symbols is represented by some longer sequence of symbols with enough redundancy to protect the data.

A binary code of size $M = 2^k$ and blocklengh n is a set of M binary words of length n called codewords. The code is referred

to as an (n,k) binary code. In general, we define block codes over an arbitrary finite alphabet, say the alphabet with q symbols {0,1,2,...,q-1}.

Definition 1.1: A block code of size $M = q^k$ over an alphabet with q symbols is a set of M q-ary sequences of length n called codewords.

Each sequence of k q-ary information symbols can be associated with a sequence of n q-ary symbols comprising a codeword. The code is called an (n,k) code.

Block codes are judged by three parameters: the blocklength n, the information length k, and the minimum distance $d^*$. The minimum distance is a measure of the amount of difference between the two most similar codewords. The minimum distance is given by the following definitions.

Definition 1.2: The Hamming distance d($\mathbf{x}$,$\mathbf{y}$) between two q-ary sequences $\mathbf{x}$ and $\mathbf{y}$ of length n is the number of places in which they differ.

Definition 1.3: Let $\mathbb{C}=\{\mathbf{c}_i,\ i=0,\ldots,M-1\}$ be a code. Then the

minimum distance of $\mathbf{C}$ is the Hamming distance of the pair of codewords with smallest Hamming distance. That is,

$$d^* = \min_{\substack{c_i, c_j \in \mathbf{C} \\ i \neq j}} d(\mathbf{c}_i, \mathbf{c}_j)$$

An (n,k) block code with minimum distance $d^*$ is also described as an $(n,k,d^*)$ block code.

## 1.2 Introduction to Algebra

The search for good error-control codes has relied to a large extent on the powerful and beautiful structures of modern algebra. A variety of important codes based on the structures of polynomial rings and finite fields have been discovered. Further, this algebraic framework provides the tools necessary to design encoders and decoders. This section is devoted to reviewing those topics in algebra that are significant to the theory of error-control codes.

The real numbers form a familiar set of mathematical objects that can be added, subtracted, multiplied, and divided. Similarly, the complex numbers form a set of objects that can be added, subtracted, multiplied, and divided. Both of these arithmetic systems are of fundamental importance in engineering disciplines. We will need to develop other less familiar

arithmetic systems that are useful in the study of error-control codes. These new arithmetic systems consist of sets together with operations on the elements. Although we will call the operations "addition," "subtraction," "multiplication," and "division", they need not be the same operations as those of elementary arithmetic.

### 1.2.1 Groups

A group is a mathematical abstraction of an algebraic structure. Although there are many concrete examples of interesting groups, the abstract idea is introduced into mathematics because it is easier to study all mathematical systems with a common structure at once rather than to study them one by one.

Definition 1.3: A group G is a nonempty set with a binary operation (denoted by juxtaposition) satisfying the following axioms:

1) Closure: For every a, b in G, c = ab is in G.

2) Associativity: For every a, b, c in G,

$$a(bc) = (ab)c.$$

3) Identity: There is an element e in G called the identity

element such that for every a in G,

$$ae = ea = a.$$

4) Inverses: If a is in G, then there is some element b in G called an inverse of a such that

$$ab = ba = e.$$

A group G is said to be Abelian (or commutative) if for every a,b in G, ab = ba.

The following examples of groups will be used later.

1) Abelian group:

(a) a cyclic group

$$C_n = \langle a;\ a^n=1 \rangle$$

$$= \{ 1, a, \ldots, a^{n-1} \},\ a^n = 1.$$

(b) $A_{nm} = C_n \times C_m = \langle a, b;\ a^n=b^m=1,\ ab=ba \rangle$

$$= \{ 1, a, \ldots, a^{n-1},\ b, ab, \ldots, a^{n-1}b,$$

$$\ldots,\ b^{m-1}, ab^{m-1}, \ldots, a^{n-1}b^{m-1} \},\ a^n=b^m=1,\ ab=ba.$$

2) Non-Abelian group:

(a) a group of a semidirect product $G = A \lhd H$,

where A is a normal abelian subgroup and H is an arbitrary subgroup of G.

(b) a Dihedral group $D_N = C_N \lhd C_2$,

where $C_N = \langle a;\ a^N=1 \rangle$, $C_2 = \langle t;\ t^2=1 \rangle$, and $tat = a^{N-1}$.

### 1.2.2 Rings

The next algebraic structure we will need is that of a ring. A ring is an abstract set that is an abelian group and also has an additional structure.

Definition 1.4: A ring R is a set with two operations defined: the first is called addition (denoted by +); the second is called multiplication (denoted by juxtaposition); and the following axioms are satisfied:

1) R is an abelian group under addition (+).

2) Closure: For any a, b in R, the product ab is in R.

3) Associative Law:

$$a(bc) = (ab)c.$$

4) Distributive Law:

$$a(b + c) = ab + ac,$$

$$(b + c)a = ba = ca.$$

The addition operation is always commutative in a ring, but the multiplication operation need not be commutative. A commutative ring is one in which multiplication is commutative; that is, $ab = ba$ for all a, b in R.

### 1.2.3 Fields

Loosely speaking, an abelian group is a set in which one can add and subtract, and a ring is a set in which one can add, subtract, and multiply. A more powerful algebraic structure, known as a field, is a set in which one can add, subtract, multiply, and divide.

Definition 1.5: A field F is a set that has two operations defined on it: addition and multiplication, such that the following axioms are satisfied.

1) The set is an abelian group under addition.

2) The field is closed under multiplication, and the set of nonzero elements is an abelian group under multiplication.

3) The distributive law:

$$(a + b)c = ac + bc$$

holds for all a, b, c in the field.

The following examples of fields are well known.

1) **R**: the set of real numbers.

2) **C**: the set of complex numbers.

3) **Q**: the set of rational numbers.

These fields all have an infinite number of elements. We are

interested in fields with a finite number of elements. A field with q elements, if it exists, is called a finite field, or a Galois field, and is denoted by the label GF(q). We will review it further in next chapter.

### 1.2.4 Vector Spaces

A familiar example of a vector space is the three-dimensional Euclidean space. This can be extended mathematically to an n-dimensional vector space over the real numbers. The concept of an n-dimensional vector space is closely related to the ideas of linear algebra and matrix theory and is important in many engineering applications.

Vector spaces also can be defined abstractly with respect to any field.

Definition 1.6: Let F be a field. The elements of F will be called scalars. A set V is called a vector space and its elements are called Vectors if there is defined an operation called vector addition (denoted by +) on pairs of elements from V, and an operation called scalar multiplication (denoted by juxtaposition) on an element from F and an element from V to produce an element from V, provided the following axioms are

satisfied.

1) V is an abelian group under vector addition.

2) Distributive Law: For any vectors $\mathbf{v}_1$, $\mathbf{v}_2$ and any scalar c,

$$c(\mathbf{v}_1 + \mathbf{v}_2) = c\mathbf{v}_1 + c\mathbf{v}_2.$$

3) Distributive Law: For any vector $\mathbf{v}$, and any scalars $c_1$, $c_2$,

$$1\mathbf{v} = \mathbf{v}$$

and

$$(c_1 + c_2)\mathbf{v} = c_1\mathbf{v} + c_2\mathbf{v}.$$

4) Associative Law: For any vector $\mathbf{v}$, and any scalars $c_1$, $c_2$,

$$(c_1c_2)\mathbf{v} = c_1(c_2\mathbf{v}).$$

The zero element of V is called the origin of V and is denoted by $\mathbf{0}$.

# 2 THE ARITHMETIC OF FINITE FIELDS

Because the most powerful and important ideas of coding theory are based on the arithmetic systems of finite fields, we will summarize the principal facts about finite fields as follows. Most of the properties reviewed in the section will be given without proofs, which can be found in ([4],[9]).

## 2.1 Finite Fields Based on Integer Rings

The set of integers (positive, negative, and zero) forms a ring under the usual operations of addition and multiplication. This ring is conventionally denoted by the label **Z**. We will describe the structure of the integer ring as follows.

Definition 2.1: Let q be a positive integer. The quotient ring, called the ring of integers modulo q and denoted by **Z**/(q), is the set {0,...,q-1} with addition and multiplication defined by

$$a + b = R_q[a + b],$$

$$a \cdot b = R_q[ab].$$

Theorem 2.2: The quotient ring **Z**/(q) is a field if and only if

q is a prime integer.

## 2.2 Finite Fields Based on Polynomial Rings

A polynomial over a field GF(q) is a mathematical expression

$$f(x) = f_{n-1}x^{n-1} + f_{n-2}x^{n-2} + \cdots + f_1x + f_0$$

where the symbol x is an indeterminate, the coefficients $f_{n-1}$, ..., $f_0$ are elements of GF(q), and the indices and exponents are integers. The zero polynomial is

$$f(x) = 0.$$

A monic polynomial is a polynomial with leading coefficient $f_{n-1}$ equal to 1. A polynomial ring is analogous in many ways to the ring of integers. A polynomial p(x) that is divisible only by $\alpha p(x)$ or $\alpha$, where $\alpha$ is an arbitrary field element in GF(q), is called an irreducible polynomial. A monic irreducible polynomial of degree of at least 1 is called a prime polynomial.

Finite fields can be obtained from polynomial rings by using constructions similar to those used to obtain finite fields from the integer ring. Suppose that we have F[x], the ring of polynomials over the field F. Just as we constructed quotient rings in the ring $\mathbf{Z}$, so can we construct quotient rings in F[x]. Choosing any polynomial p(x) from F[x], we can define the quotient ring by using p(x) as a modules for polynomial

arithmetic. We will restrict the discussion to monic polynomials because this restriction eliminates needless ambiguity in the constructions.

Definition 2.3: For any nomic polynomial p(x) with nonzero degree over the field F, the ring of polynomials modulo p(x) is the set of all polynomials with degree smaller than that of p(x), together with polynomial addition and polynomial multiplication modulo p(x). This ring is conventionally denoted by F[x]/(p(x)).

Theorem 2.4: F[x]/(p(x)) is a ring.

Theorem 2.5: The ring of polynomials modulo a monic polynomial p(x) is a field if and only if p(x) is a prime polynomial.

## 2.3 Properties of Finite Fields

Definition 2.6: A primitive field element of GF(q) is an element $\alpha$ such that every field element except zero can be expressed as a power of $\alpha$.

Theorem 2.7: Every finite field has a primitive element.

Definition 2.8: A primitive polynomial p(x) over GF(q) is a prime polynomial over GF(q) with the property that in extension field constructed modulo p(x), the field element represented by x is primitive.

Theorem 2.9: Every finite field has $p^m$ elements for some positive integer m and prime p.

Theorem 2.10: Two finite fields with the same number of elements are isomorphic.

Theorem 2.11: For every prime p and positive integer m, there is a finite field with $p^m$ elements; the smallest subfield of $GF(p^m)$ is GF(p), p is called its characteristic.

Theorem 2.12: For every finite field GF(q) and positive integer m, there exists at least one primitive polynomial over GF(q) of degree m.

Theorem 2.13: Let GF(q) have characteristic p. Then for any positive integer m and for any elements $\alpha$ and $\beta$ in GF(q),

$$(\alpha \pm \beta)^{p^m} = \alpha^{p^m} \pm \beta^{p^m}.$$

# 3 CYCLIC CODES

A linear code is a subspace of a vector space over a finite field. The class of cyclic codes is a subclass of the class of linear codes obrained by imposing an additional strong structrual requirement on the codes. Because of this structure, the search for good error-control codes has been most successful within the class of cyclic codes. Cyclic codes are also important because their underlying finite-field description leads to encoding and decoding procedures that are algorithmic and computationally efficient. In this section, we will review cyclic codes represented by polynomials. Most of the properties reviewed will be given without proofs, which can be found in ([9],[44]).

## 3.1 Polynomial Description of Cyclic Codes

A linear code $\mathbb{C}$ over GF(q) is called a cyclic code if whenever $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ is in $\mathbb{C}$, then $\mathbf{c}' = (c_{n-1}, c_0, \ldots, c_{n-2})$ is also in $\mathbb{C}$. The codeword $\mathbf{c}'$ is obtained by cyclically shifting the components of the codeword $\mathbf{c}$ one place to the right. Every linear code over GF(q) of length n is a subspace of $GF(q)^n$, and a cyclic code is a very special kind of subspace because it has this cyclic property.

Each vector in $GF(q)^n$ can be represented as a polynomial in x of degree of less than or equal to n - 1. The components of the vector are identified with the coefficients of the polynomial. The set of polynomials has a vector space structure identical to that of $GF(q)^n$. This set of polynomials also has a ring structure, called $GF(q)[x]/(x^n-1)$. As a ring, the set has a product

$$p_1(x) \cdot p_2(x) = R_{x^n-1}[p_1(x)p_2(x)] .$$

A cyclic shift can be written as a multiplication within this ring:

$$x \cdot p(x) = R_{x^n-1}[xp(x)] .$$

Hence, if the codewords of a code are denoted by polynomials, the code is a subset of $GF(q)[x]/(x^n-1)$. The code is a cyclic code if $x \cdot c(x)$ is a codeword polynomial whenever $c(x)$ is a codeword polynomial.

Theorem 3.1: In the ring $GF(q)[x]/(x^n-1)$, a subset is a cyclic code if and only if it satisfies the following two properties:

1) $\mathbb{C}$ is a subgroup of $GF(q)[x]/(x^n-1)$ under addition.

2) If $c(x) \in \mathbb{C}$, and $a(x) \in GF(q)[x]/(x^n-1)$, then $R_{x^n-1}[a(x)c(x)] \in \mathbb{C}$.

Proof: Suppose the subset satisfies the two properties. Then it is closed under addition and closed under multiplication by a scalar. Hence it is a subspace. It is also closed under multiplication by any ring element, in particular under multiplication by x. Hence it is a cyclic code.

Now suppose that it is a cyclic code. Then it is closed under addition and under multiplication by x. But then it is closed under multiplication by powers of x and linear combinations of powers of x. That is , it is closed under multiplication by an arbitrary polynomial. Hence it satisfies the two properties, and the theorem is proved.

In general, a subset I of a ring R is called an ideal of R if (1) I is a subgroup of the additive group of R, and (2) if $r \in R$ and $a \in I$, then $ar \in I$. From Theorem 3.1, we can reach an important result.

Theorem 3.2: A cyclic code is an ideal of the ring $GF(q)[x]/(x^n-1)$.

Now choose a nonzero codeword polynomial of smallest degree from cyclic code $\mathbb{C}$ and denote its degree by n-k (it must be less

than n). Multiply by a field element to make it a monic polynomial. This must also be in the code $\mathbb{C}$, because the code is linear. No other monic polynomial of this degree is in the code, because otherwise the differnce of the two minic polynomial would be in the code and have degree smaller than n-k, contrary to the choice of the original polynomial.

The unique nonzero monic polynomial of smallest degree is called the generator polynomial of $\mathbb{C}$ and is denotd by g(x).

Theorem 3.3: A cyclic code consists of all multiples of the generator polynomial g(x) by polynomials of degee k-1 or less.

Theorem 3.4: There is a cyclic code of blocklength n with generator polynomial g(x) if and only if g(x) divides $x^n-1$.

## 3.2 Minimal Polynomials and Conjugates

We have seen that a cyclic code of bolcklength n over GF(q) exists for each polynomial g(x) over GF(q) that divides $x^n-1$. We now wish to study such generator polynomials explicitly. First we wish to find the possible generator polynomials for a cyclic code of blocklength n. The most direct approach is to find divisors of $x^n-1$. This can be done by writing $x^n-1$ in

terms of its prime factors;

$$x^n-1 = f_1(x) f_2(x) \ldots f_s(x),$$

where s is the number of prime factors. Any subset of these factors can be multiplied together to produce a generator polynomial g(x). If the prime factors of $x^n-1$ are distinct, then there are $2^s-2$ different nontrivial cyclic codes of length n (excluding the trivial cases g(x) = 1 and g(x) = $x^n-1$).

In this section we will look at the relationship between the prime polynomials and their zeros in an extension field. In particular, we will learn how to find prime polynomials, and hence generator polynomials, that have specified zeros. Eventually, we will design codes by choosing desirable zeros in an extension field. We will see how the zeros should be specified so as to ensure a good code.

We will start with certain preferred values of n called primitive blocklengths.

Definition 3.5: A blokclength n of the form n = $q^m-1$ is called a primitive blocklength for a code over GF(q). A cyclic code over GF(q) of primitive blocklength is called a primitive cyclic code.

Definition 3.6: The minimal polynomial of $\beta_j$ is the smallest-degree polynomial with coefficients in the base field GF(q) that has $\beta_j$ as a zero in the extension field GF($q^m$).

Theorem 3.7: Suppose that f(x) is the minimal polynomial over GF(q) of $\beta$, an element of GF($q^m$). Then f(x) is also the minimal polynomial of $\beta^q$.

Definition 3.8: Two elements of GF($q^m$) that share the same minimal polynomial over GF(q) are called conjugates (with respect to GF(q)).

The conjugates of an element $\beta$ are easily found using Theorem 3.7. If f(x) is the minimal polynomial of $\beta$, then it is also that of $\beta^q$, and in turn $\beta^{q^2}$ and so forth. Hence, the elements in the set

$$\{\beta, \beta^q, \beta^{q^2}, \beta^{q^3}, \ldots, \beta^{q^{r-1}}\},$$

are all conjugates, where r is the smallest integer such that $\beta^{q^r} = \beta$. Note that because $\beta^{q^m} = \beta$, $r \leq m$. This set is called a set of conjugates. The conjugates are all zeros of f(x), and the following theorem shows that no others exist.

Theorem 3.8: The minimal polynomial of β is

$$f(x) = (x-\beta)(x-\beta^q)\ldots(x-\beta^{q^{r-1}}) .$$

## 3.3 BCH Codes

The class of Bose-Chaudhuri-Hocquenghem (BCH) codes ([11],[31]) is a large class of multiple-error-correcting cyclic codes that occupies a prominent place in theory and practice of error correction. We will now formally define BCH codes, which can correct t errors.

Definition 3.9: Let q and m be given and let β be any element of GF($q^m$) of order n. Then for any positive integer t and any integer $j_0$ the corresponding BCH code is the cyclic code of blocklength n with the generator polynomial

$$g(x) = LCM[f_{j_0}(x), f_{j_0+1}(x), \ldots, f_{j_0+2t-1}(x)] ,$$

where $f_j(x)$ is the minimal polynomial of $\beta^j$.

# 4 IDEMPOTENTS IN GROUP ALGEBRA

In this section, we will first introduce the group algebra, the idempotent of group algebra, and the ideal of group algebra; then, we will define any cyclic code alternatively as an ideal of cyclic group algebra; we will further construct a new class of codes, non-abelian codes, by the ideal of non-abelian group algebra.

## 4.1 Group Algebra

The group algebra of a finite group G over a field F, denoted by FG, is the F-vector space of all formal sums

$$f = \sum_{u \in G} f(u)\,u, \quad f(u) \in F \ .$$

Addition and multiplication with scalars $k \in F$ are defined as usual:

$$\sum_{u \in G} f(u)\,u + \sum_{u \in G} g(u)\,u = \sum_{u \in G} (f(u) + g(u))\,u \ ,$$

$$k\Big(\sum_{u \in G} f(u)\,u\Big) = \sum_{u \in G} (kf(u))\,u \ .$$

Moreover, F-algebra multiplication given by

$$fg = \sum_{v \in G} \Big(\sum_{u \in G} f(u)\,g(u^{-1}v)\Big)\,v .$$

As a F-vector space, FG has dimension the order of G and G is a basis. As F-algebra, FG is isomorphic to the F-algebra of all F-valued functions on G under convolution product.

A subset W of the F-algebra FG is called a left ideal if W is a subspace satisfying,

$$fW = \{fg: g \in W\} \subset W.$$

A left ideal W is called simple if (0) and W are the only left ideals contained in W.

Two left ideals W and W' are said to be isomorphic in FG if there exists a F-linear isomorphism

$$\phi: W \to W'$$

of W onto W' satisfying

$$\phi(uw) = u\phi(w), \quad u \in G, \quad w \in W.$$

Throughout this work we will assume that the characteristic of F is relatively prime to the order of G.

Theorem 4.1: FG is a semisimple F-algebra, i.e., FG is the direct sum

$$FG = W_1 \oplus \cdots \oplus W_M$$

of a finite number of simple left ideals $\{ W_1, \ldots, W_M \}$.

Although this decomposition is not unique, any other decomposition of FG into simple left ideals has the same number of factors and a bijection can be established which associates isomorphic simple left ideals.

A coarser but unique direct sum decomposition is given by the Wedderburn Decomposition of FG into the direct sum of simple two-sided ideals ([16], [32]).

## 4.2 Clifford's Theory of Idempotents

We assume throughout that G is a finite group and that F is a field whose characteristic does not divide N, the order of G. A nonzero element $e \in FG$ is called an idempotent if $e^2 = e$. Two idempotents $e_1$ and $e_2$ are said to be orthogonal if $e_1e_2 = e_2e_1 = 0$. A set of pairwise orthogonal idempotents

$$\{e_1, \cdots, e_J\}$$

is called a complete set of orthogonal idempotents if

$$1 = e_1 + \cdots + e_J \ .$$

A complete set of orthogonal idempotents determines a decomposition of FG into a direct sum of non-trivial left ideals

$$FG = W_1 \oplus \cdots \oplus W_J \ ,$$

where the left ideals are given by

$$W_j = FGe_j \ , \quad 1 \le j \le J \ .$$

Conversely such a decomposition determines a complete set of orthogonal idempotents defined by expanding $1 \in FG$ as follows,

$$1 = e_1 + \cdots + e_J \ , \quad e_j \in W_j \ , \quad 1 \le j \le J \ .$$

An idempotent $e \in FG$ is called primitive if it cannot be

written as a sum of two orthogonal idempotents. The left ideal $W = FGe$ is simple if and only if e is primitive. We say that e and e' are isomorphic in FG if the associated left-ideals FGe and FGe' are isomorphic in FG. If e and e' are primitive idempotents in FG, then e and e' are isomorphic in FG if and only if there exits an $u \in G$ such that

$$eue' \neq 0 \ .$$

An isomorphism from FGe onto FGe' is given by right-multiplication by eue'. It follows that we can construct a decomposition of FG into the direct sum of left ideals by constructing a complete set of primitive orthogonal idempotents.

## 4.3 Algorithms for Computing Idempotents

### 4.3.1 Finite Abelian Groups

We assume throughout that A is a finite abelian group of order N and F is a field whose characteristic does not divide N.

The character group $A^*$ of A over F is the set of all group homomorphisms $\tau$ of A into the multiplicative group of nonzero elements of F with group product

$$(\tau\tau')(a) = \tau(a)\tau'(a), \qquad \tau, \tau' \in A^*, \ a \in A.$$

We identify $\tau \in A^*$ with

$$\tau = \sum_{a \in A} \tau(a)\, a \in FA$$

and consider $A^{\cdot} \subset FA$. It should be noted that group product in $A^{\cdot}$ is not the same as the product in FA.

(1) Split Case

we say that A splits over F if A and $A^{\cdot}$ are isomorphic as groups. If A splits over F then $A^{\cdot}$ is a basis of the F-vector space FA. A necessary and sufficient condition for A to split over F is that F contains a primitive Mth root of unity where M is the least common multiple of the order of the elements in A. Since M divides N, A splits over F if F contains a primitive Nth root of unity. We assume throughout this section that A splits over F.

The following formulas are fundamental to many properties of characters.

$$\sum_{a \in A} \tau(a) = \begin{cases} 0 & \tau \neq \tau_0 \\ N & \tau = \tau_0 \end{cases},$$

where $\tau_0$ is the identity in the group $A^{\cdot}$.

$$\sum_{\tau \in A^{\cdot}} \tau(a) = \begin{cases} 0 & a \neq 1 \\ N & a = 1 \end{cases}.$$

Direct application of these formula proves the following result.

Theorem 4.2: The set

$$\frac{1}{N}A^{\cdot} = \{\frac{1}{N}\tau : \tau \in A^{\cdot}\}$$

is a complete set of primitive orthogonal idempotents in FA.

(2) Nonsplit Case

We assume only that the characteristic of F does not divide the order N of A. Then there exists a finite Galois extension E over F such that A splits over E. Denote the Galois group of E over F by $G$.

For $\sigma \in G$ and $f \in EA$ define $f^{\sigma} \in EA$ by the formula

$$f^{\sigma} = \sum_{a \in A} \sigma(f(a))\, a .$$

If $\tau \in A^{\cdot}$ then $\tau^{\sigma} \in A^{\cdot}$. $G$ acts on $A^{\cdot}$ and partitions $A^{\cdot}$ into $G$-orbits

$$G\tau = \{\tau^{\sigma} : \sigma \in G\} .$$

Denote the set of $G$-orbits in $A^{\cdot}$ by $A^{\cdot}/G$.

For $\tau \in A^{\cdot}$, define $e_{\tau} \in EA$ by the formula

$$e_{\tau} = \frac{1}{N} \sum_{\psi \in G\tau} \psi .$$

Since $\sigma \in G$ permutes the elements in $G\tau$, we have

$$e_{\tau}^{\sigma} = e_{\tau}$$

and $e_{\tau} \in FA$. $e_{\tau}$ is independent of the choice of $\psi \in G\tau$, i.e., $e_{\tau} = e_{\psi}$, $\psi \in G\tau$.

Theorem 4.3: The set

$$\{e_{\tau} : G\tau \in A^{\cdot}/G\} \qquad (4\text{-}1)$$

is a complete set of orthogonal idempotents for FA.

Proof: As a sum of orthogonal idempotents, $e_{\tau}$ is an idempotent in

FA. Distinct $e_\tau$ and $e_{\tau'}$ are associated with distinct $G$-orbits and hence orthogonal. Completeness follows from

$$\sum_{\tau \in A^*/G} e_\tau = \frac{1}{N} \sum_{\tau \in A^*} \tau = 1.$$

It remains to prove that $e_\tau$ is primitive. We first prove that each idempotent $e \in FA$ is a sum of idempotents from (4-1). Since $FA \subset EA$, we can write

$$e = \frac{1}{N} \sum_{\tau \in A^*} e(\tau)\tau, \quad e(\tau) \in E.$$

$e^2 = e$ implies $e(\tau) = 0$ or $e(\tau) = 1$, and $e^\sigma = e$, $\sigma \in G$ implies $e(\tau)$ is constant on $G$-orbits proving the claim. Since $e_\tau$ is associated with a unique $G$-orbit, it must be primitive by the preceding discussion completing the proof of the theorem.

### 4.3.2 Specific Non-abelian Groups

Consider a finite group G given as a semidirect product $G = A \lhd H$, where A is a normal abelian subgroup of order N and H is an arbitrary subgroup of G. Each $x \in G$ can be written uniquely in the form $x = ah$, $a \in A$, $h \in H$ and group multiplication is given by

$$xx' = aha'h^{-1}hh' .$$

We assume throughout that F is a field whose characteristic does not divide the order of G. Thus FG' is a semisimple algebra for any subgroup G' of G.

Assume that A splits over F. Denote the character group of A over F by $A^*$. For each $\tau \in A^*$, define

$$H(\tau) = \{h \in H : h\tau = \tau h\} .$$

$H(\tau)$ is a subgroup of H called the centralizer of $\tau$ in H.

Theorem 4.4: For $\tau \in A^*$ and a primitive idempotent f in $FH(\tau)$, we have that $\frac{1}{N}\tau f$ is a primitive idempotent in FG, where N is the order of A.

Proof: Since $\tau f = f\tau$, $\frac{1}{N}\tau f$ is an idempotent in FG, Suppose $\frac{1}{N}\tau f$ is not a primitive idempotent in FG and write

$$\frac{1}{N}\tau f = e + e' ,$$

where e and e' are orthogonal idempotents in FG. Then

$$e = \frac{1}{N}\tau e = \frac{1}{N} e\tau .$$

Since $A^*$ is a basis of FA, we can write

$$e = \sum_{h \in H} \sum_{\lambda \in A^*} e(\lambda, h)\lambda h , \quad e(\lambda, h) \in F .$$

Applying Theorem 4.2,

$$e = \frac{1}{N}\tau e = \tau \sum_{h \in H} e(\tau, h) h$$
$$= \frac{1}{N} e\tau = \tau \sum_{h \in H(\tau)} e(\tau, h) h$$

and we can write

$$e = \frac{1}{N}\tau m, \quad m \in FH(\tau) .$$

Arguing in the same way

$$e' = \frac{1}{N}\tau m', \quad m' \in FH(\tau) .$$

Then $\frac{1}{N}\tau f = \frac{1}{N}\tau(m+m')$, implying that

$$f = m + m'.$$

We have used the result that if $a \in FA$, $a \neq 0$ and $b$ and $b' \in FH$ satisfy ab = ab' in FG then $b = b' \in FH$. Applying the result once more to

$$e^2 = \frac{1}{N}\tau m^2 = \frac{1}{N}\tau m = e,$$

we have $m^2 = m$. The same argument shows that m and m' are orthogonal idempotents in FH(τ), completing the proof of the theorem.

Theorem 4.4 is the main part of the proof of the following result.

Theorem 4.5: For each $\tau \in A^*$, choose a complete set of primitive orthogonal idempotents for FH(τ)

$$f_\tau^1, \cdots, f_\tau^{r_\tau}.$$

Then the set of products

$$\frac{1}{N}\tau f_\tau^r, \quad \tau \in A^*, \quad 1 \leq r \leq r_\tau$$

is a complete set of primitive orthogonal idempotents for FG, where N is the order of A

### 4.3.3 Examples of Idempotents

(1) Suppose a cyclic group $C_N = \langle a; a^N=1 \rangle$ and a field F = GF(q), whose characteristic does not divide N. Suppose N divides (q-1), i.e. $C_N$ splits over F, denote the character group of $C_N$ by $C_N^{\cdot}$, then

$$C_N^{\cdot} = \{\alpha_k, \quad 0 \le k \le N-1\} \ ,$$

where $\alpha_k = 1 + w^k a + w^{2k} a^2 + \cdots + w^{(N-1)k} a^{N-1}$, $w^N = 1$, $w \in F$.

A complete set of idempotents for $FC_N$ is

$$\{\alpha_0/N, \alpha_1/N, \alpha_2/N, \cdots, \alpha_{N-1}/N\} .$$

(2) Suppose a cyclic group $C_N = \langle a; a^N=1 \rangle$ and a field F = GF(q), whose characteristic does not divide N. Suppose N does not divide (q-1), then there exists a finite Galois extension E = GF($q^m$) over F such that $C_N$ splits E. Denote the Galois group of E over F by $G$. Denote the character group of $C_N$ by $C_N^{\cdot}$, then

$$C_N^{\cdot} = \{\alpha_k, \quad 0 \le k \le N-1\} \ ,$$

where $\alpha_k = 1 + w^k a + w^{2k} a^2 + \cdots + w^{(N-1)k} a^{N-1}$, $w \in E$, $w^N = 1$.

A complete set of idempotents for $EC_N$ is

$$\{\alpha_0/N, \alpha_1/N, \alpha_2/N, \cdots, \alpha_{N-1}/N\} .$$

$G$ acts on $C_N^{\cdot}$ and partitions $C_N^{\cdot}$ into $G$-orbits

$$G_k = \{\alpha_k, \alpha_{kq}, \alpha_{kq^2}, \ldots, \alpha_{kq^{r-1}}\} ,$$

where r is the smallest integer such that $\alpha_{kq^r} = \alpha_k$. Denote the set of $G$-orbits in $C_N^{\cdot}$ by $C_N^{\cdot}/G$. From Theorem 4.3 in section

4.3.1, we have

$$e_k = \frac{1}{N}\sum_{\psi \in G_k} \psi \ ,$$

$e_k$ is an idempotent of $FC_N$ , and the set $\{e_k : G_k \in C_N^*/G\}$ is a complete set of orthogonal idempotents for $FC_N$.

(3) Suppose group G is a Dihedral group $D_N = C_N \triangleleft C_2$, where

$C_N = \langle a; a^N=1 \rangle$, $C_2 = \langle t; t^2=1 \rangle$, and $tat = a^{N-1}$.

Suppose finite field F is GF(q), whose characteristic does not divide 2N, and 2N divides (q-1), then

centralizer of $\alpha_k$ in $C_2$ is

$$C_2(\alpha_k) = \begin{cases} C_2 , & k = 0 \\ \{1\}, & otherwise \end{cases} ;$$

primitive idempotents of $C_2$ are

$$(1+t)/2, \ (1-t)/2 \ ;$$

a complete set of primitive orthognal idempotents of group algebra FG is

$$\frac{1}{N}\{\alpha_0(1+t)/2, \ \alpha_0(1-t)/2, \ \alpha_1, \ \alpha_2, \ \cdots , \ \alpha_{N-1}\},$$

where $\alpha_k = 1 + w^k a + w^{2k} a^2 + \cdots + w^{(N-1)k} a^{N-1}$ , $w^N = 1$, $w \in F$.

## 4.4 The Structure of Cyclic Codes in Group Algebra

We recall some facts on the structure of $GF(q)[x]/(x^n-1)$, where $(n,q) = 1$. Suppose $x^n-1$ factors into the polynomials $g_i(x)$, i=1,...,s. Then cyclic codes generated by $g_i(x)$ are

ideals of the ring GF(q)[x]/($x^n$-1). If we let $C_n$ be a cyclic group of order n with a generator x, then there is an obvious isomorphism between the group algebra GF(q)$C_n$ and GF(q)[x]/($x^n$-1), where we use the variable x for both algebras to emphasize the identification. So we reach that every cyclic code of length n over a finite field GF(q) may be viewed as an ideal of the group algebra GF(q)$C_n$ . From previous sections 4.2 and 4.3, we can construct any cyclic code by a new way. First, compute the set of primitive orthognal idempotents of a cyclic group algebra using the algorithms in section 4.3. Then choose a propriate idempotent, which is a sum of certain of these primitive orthognal idempotents. Last, construct the ideal of the group algebra from this idempotent.

## 4.5 Construction of Non-abelian Codes

In order to construct non-abelian codes, we will generalize the procedure of constructing cyclic codes in section 4.4 as follows:

1) Find the complete set of primitive orthognal idempotents of a non-abelian group algebra $FG$, where group $G$ is a non-abelian group, using the algorithms in section 4.3:

$$\{e_1, \cdots, e_J\}.$$

2) Choose an appropriate idempotent $e$, which is a sum of certain of these primitive orthognal idempotents.

3) Construct the ideal of the group algebra from this idempotent,

$$W = FGe,$$

which is a non-abelian code.

For example, we will construct a non-abelian Dihedral code from an idempotent of a non-abelian Dihedral group algebra $GF(7)D_3$.

1) Suppose a non-abelian Dihedral group $D_3 = C_3 \lhd C_2$, $C_3 = \langle a; a^3=1 \rangle$, $C_2 = \langle t; t^2=1 \rangle$, and $tat = a^2$, then a complete set of primitive orthognal idempotents of the Dihedral group algebra $GF(7)D_3$ is

$$\{e_1, e_2, e_3, e_4\},$$

where

$$e_1 = \frac{1}{6}\alpha_0(1+t),$$

$$e_2 = \frac{1}{6}\alpha_0(1-t),$$

$$e_3 = \frac{1}{3}\alpha_1 ,$$

$$e_4 = \frac{1}{3}\alpha_2 ,$$

$$\alpha_k = 1 + w^k a + w^{2k}a^2 \quad (k=0,1,2),$$

$$w \in GF(7),\ w^3 = 1 .$$

2) Choose $e = e_3 = \frac{1}{3}\alpha_1$ .

3) Construct the ideal of the group algebra $GF(7)D_3$ from this idempotent e,

$W = GF(7)D_3e$,

which is a non-abelian Dihedral code. The codewords of the non-abelian Dihedral code are as follows.

| | | | |
|---|---|---|---|
| 0 0 0 0 0 0 | 0 4 0 2 0 1 | 0 1 0 4 0 2 | 0 5 0 6 0 3 |
| 0 2 0 1 0 4 | 0 6 0 3 0 5 | 0 3 0 5 0 6 | 5 0 3 0 6 0 |
| 5 4 3 2 6 1 | 5 1 3 4 6 2 | 5 5 3 6 6 3 | 5 2 3 1 6 4 |
| 5 6 3 3 6 5 | 5 3 3 5 6 6 | 3 0 6 0 5 0 | 3 4 6 2 5 1 |
| 3 1 6 4 5 2 | 3 5 6 6 5 3 | 3 2 6 1 5 4 | 3 6 6 3 5 5 |
| 3 3 6 5 5 6 | 1 0 2 0 4 0 | 1 4 2 2 4 1 | 1 1 2 4 4 2 |
| 1 5 2 6 4 3 | 1 2 2 1 4 4 | 1 6 2 3 4 5 | 1 3 2 5 4 6 |
| 6 0 5 0 3 0 | 6 4 5 2 3 1 | 6 1 5 4 3 2 | 6 5 5 6 3 3 |
| 6 2 5 1 3 4 | 6 6 5 3 3 5 | 6 3 5 5 3 6 | 4 0 1 0 2 0 |
| 4 4 1 2 2 1 | 4 1 1 4 2 2 | 4 5 1 6 2 3 | 4 2 1 1 2 4 |
| 4 6 1 3 2 5 | 4 3 1 5 2 6 | 2 0 4 0 1 0 | 2 4 4 2 1 1 |
| 2 1 4 4 1 2 | 2 5 4 6 1 3 | 2 2 4 1 1 4 | 2 6 4 3 1 5 |
| 2 3 4 5 1 6. | | | |

Figure 4.1

Codewords of a (6,2) non-abelian Dihedral code over GF(7)

# 5 FOURIER TRANSFORMS IN A FINITE FIELD

The subject of digital signal processing is permeated with applications of the Fourier transform. When the time variable is continuous, the study of real-valued or complex-valued signals relies heavily on the Fourier transform. When the time variable is discrete, the discrete Fourier transform plays a parallel role. Fourier transforms also exist on the vector space of n-tuples over the finite field GF(q) for many values of n. Fourier transforms in a finite field can play an important role in the study and processing of GF(q)-valued signals; that is, of codewords. By using Fourier transforms, the ideas of coding theory can be described in a setting that is much different from that seen thus far. Cyclic codes can be defined as codes whose codewords have certain specified spectral components equal to zero. Also, the decoding of BCH codes and Reed-Solomon codes can be described spectrally.

In this work, We will use the frequency domain setting to develope encoding and decoding algorithms for a class of non-abelian codes. So, we first review some basic topics of the discrete Fourier transform over a finite field [45].

In the complex field, the definition of the discrete Fourier

transform of $\mathbf{p} = ( p_i \quad i=0,\ldots,N-1 )$, a vector of complex numbers, is a vector $\mathbf{P} = ( P_k \quad k=0,\ldots,N-1 )$ given by

$$P_k = \sum_{i=0}^{N-1} e^{-j2\pi N^{-1}ik} p_i \qquad k = 0, \ \ldots \ , N-1 \ ,$$

where $j = \sqrt{-1}$ . The Fourier kernel $\exp(-j2\pi N^{-1})$ is an Nth root of unity in the field of complex numbers. In the finite field $GF(q^m)$, an element $\alpha$ of order n is an nth root of unity. Drawing on the analogy between $\exp(-j2\pi N^{-1})$ and $\alpha$, we have the following definition.

DEFINITION 5.1: Let $\mathbf{v} = \{ v_i \quad i=0,\ldots,n-1 \}$ be a vector over GF(q), where n divides $q^m-1$ for some m, and let $\alpha$ be an element of $GF(q^m)$ of order n. The finite-field Fourier transform of the vecor $\mathbf{v}$ is the vector $\mathbf{V} = \{ V_j \quad j=0,\ldots,n-1\}$ given by

$$V_j = \sum_{i=0}^{n-1} \alpha^{ij} v_i \qquad j=0,\cdots,n-1 \ .$$

It is natural to call the discrete index i time and to call $\mathbf{v}$ the time-domain functin or the signal. Also, we might call the discrete index j frequency and $\mathbf{V}$ the frequency-domain function or the spectrum.

Any factor of $q^m-1$ can be used as the blocklength of a Fourier transform, but the most import values for n are the primitive blocklengths, $n = q^m-1$ . Then $\alpha$ is a primitive element of

GF($q^m$). In contrast to the situation for the complex field, Fourier transforms of every blocklength do not exist in a finite field because elements of every order do not exist. There are enough, hovever, for most purposes. If m is the smallest integer such that n divides $q^m$-1, then there is a finite-field Fourier transform over GF(q) of blodklength n, and the components of the Fourier transform are in GF($q^m$). Unfortunately, for some values of n, although the transform exists, it will be in a very large extension field and may not be practical for a given applcation.

In the case of the discrete Fourier transform, even though the time-domain function **p** is real, the transform **P** is complex. Similarly, in the finite-field Fourier transform, even though the time-domain function **v** is over the field GF(q), the spectrum **V** is over the extension field GF($q^m$). In error-control applications, all the decoding action really takes place in the big field GF($q^m$); it is just that we happen to start with a vector consistent with the channel input; that is, in the small field GF(q).

Theorem 5.2: Over GF(q), a field of characteristic p, a vector and its spectrum are related by

$$V_j = \sum_{i=0}^{n-1} \alpha^{ij} v_i$$

$$v_i = \frac{1}{n}\sum_{j=0}^{q-1} \alpha^{-ij} V_j \ ,$$

where n is interpreted as an integer of the field; that is, modulo p.

Proof: In any field,

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1) .$$

By the definition of $\alpha$, $\alpha^r$ is a zero of the left side for all r. Hence for all $r \neq 0$ modulo n, $\alpha^r$ is a zero of the last term. But this is equivalent to

$$\sum_{j=0}^{q-1} \alpha^{rj} = 0 \qquad r \neq 0 \ (\text{mod } n)$$

whereas if r = 0 modulo n,

$$\sum_{j=0}^{q-1} \alpha^{rj} = n \qquad (\text{mod } p),$$

which is not zero if n is not a multiple of the field characteristic p. Combining these facts, we have

$$\sum_{j=0}^{q-1} \alpha^{-ij} \sum_{k=0}^{q-1} \alpha^{kj} V_k = \sum_{k=0}^{q-1} V_k \sum_{j=0}^{q-1} \alpha^{(k-i)j} = (n \bmod p)\, V_i$$

Finally, $q^m - 1 = p^M - 1$ is a multiple of n, and consequently n is not a multiple of p. Hence $n \neq 0 \ (\text{mod } p)$. This proves the theorem.

The Fourier transform has many strong properties that carry over to the finite field case. An example is the convolution property of the next theorem. a dual theorem can be proved with the time domain and the frequency domain interchanged.

Theorem 5.3(Convolution Theorem): Suppose that

$$e_i = f_i g_i \qquad i = 0, \cdots, n-1.$$

Then

$$E_j = \frac{1}{n}\sum_{k=0}^{n-1} F_{((j-k))} G_k \qquad j = 0, \cdots, n-1,$$

where the double parentheses denote modulo-n arithmetic on the indices.

Proof: Take the Fourier transform of $e_i = f_i g_i$

$$E_j = \sum_{i=0}^{n-1} \alpha^{ij} f_i \left(\frac{1}{n}\sum_{k=0}^{n-1} \alpha^{-ik} G_k\right)$$

$$= \frac{1}{n}\sum_{k=0}^{n-1} G_k \left(\sum_{i=0}^{n-1} \alpha^{i(j-k)} f_i\right)$$

$$= \frac{1}{n}\sum_{k=0}^{n-1} G_k F_{((j-k))} .$$

Note also that setting j = 0 in the convolution formula,

$$E_j = \sum_{i=0}^{n-1} \alpha^{ij} f_i g_i = \frac{1}{n}\sum_{k=0}^{n-1} F_{((j-k))} G_k \ ,$$

yields the Parseval-type formula

$$\sum_{i=0}^{n-1} f_i g_i = \frac{1}{n}\sum_{k=0}^{n-1} F_{((n-k))} G_k \ .$$

Theorem 5.4(Translation Property): If $\{v_i\} \sim \{V_j\}$ is a Fourier transform pair, then the following are Fourier transform pairs:

$$\{\alpha^i v_i\} \sim \{V_{((j-1))}\}$$

$$\{v_{((i-1))}\} \sim \{\alpha^j V_j\} .$$

Proof: Immediate substitutions prove the theorem.

Sometimes we represent a vector **v** by a polynomial v(x). The polynomial

$$v(x) = v_{n-1}x^{n-1} + \cdots + v_1 x + v_0$$

can be transformed into a polynomial

$$V(x) = V_{n-1}x^{n-1} + \cdots + V_1 x + V_0$$

by means of the finite-field Fourier transform. The latter polynomial is called the spectrum polynomial or the associated polynomial of v(x). Properties of the spectrum are closely related to the zeros of polynomials, as stated in the following theorem.

Theorem 5.5:

(i) The polynomial v(x) has a zero at $\alpha^j$ if and only if the jth frequency component $V_j$ equals zero.

(ii) The polynomial V(x) has a zero at $\alpha^{-1}$ if and only if the ith time component $v_i$ equals zero.

Proof: The proof of part (i) is immediate because

$$v(\alpha^j) = \sum_{i=0}^{n-1} v_i \alpha^{ij} = V_j .$$

The proof of part (ii) follows in the same way.

Thus in finite fields, when one seaks of zeros of polynomials or of spectral components equal to zero, one really speaks of the same thing, but the terminology and the insights are different. In the first formulation, one draws on insight into the factoring of polynomials; in the second, one draws on understanding of the Fourier transform.

The Fourier transform over GF(q) of blocklength n takes values in an extension field GF($q^m$). If we start with an arbitrary n-vector over GF($q^m$) and take the inverse Fourier transform, we generally do not get a time-domain vector over GF(q); there may be components in the larger field. We must find constraints on the spectrum that will ensure a time-domain vector over GF(q).

Constraints of this sort are familiar in the field of complex numbers. Recall that over the complex field, a spectrum P(f) has a real-valued inverse Fourier transform if and only if P*(-f) = P(f). The next theorem gives a set of constraints, known as conjugacy constraints, that provide an analogous condition for a finite field.

Theorem 5.6: Let **V** be a vector of length n of elements of GF($q^m$) where n is a divisor of $q^m-1$. Then the inverse Fourier transform **v** is a vector of elements of GF(q) if and only if the

following equations are satisfied:

$$V_j^q = V_{((qj))} \quad j = 0, \cdots, n-1 .$$

Proof: By definition,

$$V_j = \sum_{i=0}^{n-1} \alpha^{ij} v_i \quad j = 0, \cdots, n-1 .$$

For a field of characteristic p, $(a+b)^{p^r} = a^{p^r} + b^{p^r}$ for any integer r. Further, if $v_i$ is an element of GF(q) for all i, then $v_i^q = v_i$. Consequently, combining these gives

$$V_j^q = (\sum_{i=0}^{n-1} \alpha^{ij} v_i)^q = \sum_{i=0}^{n-1} \alpha^{qij} v_i^q = \sum_{i=0}^{n-1} \alpha^{qij} v_i = V_{((qj))} .$$

Conversely, suppose that for all j, $V_j^q = V_{((qj))}$. Then

$$\sum_{i=0}^{n-1} \alpha^{iqj} v_i^q = \sum_{i=0}^{n-1} \alpha^{iqj} v_i \quad j = 0, \cdots, n-1 .$$

Let k =qj. Because q is relatively prime to $n = q^m-1$, as j ranges over all values between 0 and n - 1, k also takes on all values between 0 and n - 1. Hence

$$\sum_{i=0}^{n-1} \alpha^{ik} v_i^q = \sum_{i=0}^{n-1} \alpha^{ik} v_i \quad k = 0, \cdots, n-1 ,$$

and by uniqueness of the Fourier transform, $v_i^q = v_i$ for all i. Thus $v_i$ is a zero of $x^q-x$ for all i, and such zeros are all elements of GF(q).

To apply the theorem, the integers modulo n are divided into a collection of sets, known as conjugacy classes, as follows:

$$A_j = \{j, jq, jq^2, \cdots, jq^{m_j-1}\} ,$$

where $m_j$ is the smallest positive integer satisfying $jq^{m_j} = j$

modulo n. Because the field is finite, there must be such an $m_j$. For example, when q=2 and n=7, the conjugacy classes are

$A_0 = \{0\}$

$A_1 = \{1, 2, 4\}$

$A_3 = \{3, 6, 5\}$.

The conjugacy class $A_j$ specifies a set of frequencies in the spectrum. We call this set of frequencies a chord. Theorem 5.6 asserts that if the time-domain signal is in GF(q), then the value of the spectrum at any frequency in chord specifies the value of the spectrum at all other frequencies in the chord.

# 6 TRANSFORM DOMAIN CHARACTERIZATION FOR SPECIFIC CODES

## 6.1 Spectra of Cyclic Codes

Suppose a cyclic group $C_N = \langle a;\ a^n=1 \rangle$ and a field F = GF(q), whose characteristic does not divide N. Suppose N divides (q-1). Then a complete set of idempotents for $FC_N$ is

$$\{\alpha_0/N,\ \alpha_1/N,\ \alpha_2/N,\ \cdots,\ \alpha_{N-1}/N\},$$

where $\alpha_k = 1 + w^k a + w^{2k}a^2 + \cdots + w^{(N-1)k}a^{N-1}$, $0 \le k \le N-1$,

and $w^N = 1$, $w \in F$.

Suppose e is an idempotent of group algebra $FC_N$, then ideal $FC_N e$ will be a cyclic code. We will study transform domain characterization of codewords in the cyclic code.

Let $x \in FG$, $e = \frac{1}{N}\alpha_k$ is one of primitive orthognal idempotents in FG, $y = xe$, then

$$y(v) = \sum_{u \in G} x(u)\, e(u^{-1}v), \qquad v \in G.$$

Order the group $C_N$ by

$$g_0=1,\ g_1=a,\ g_2=a^2,\ \cdots,\ g_{N-1}=a^{N-1}.$$

Denote $x(g_i)$, $y(g_i)$ and $e(g_i)$ by $x(i)$, $y(i)$ and $e(i)$, respectively, where $0 \le i < N$, then we have

$$y(0) = x(0)e(0) + x(1)e(N-1) + \ldots + x(N-1)e(1),$$

$$y(1) = x(0)e(1) + x(1)e(0) + \ldots + x(N-1)e(2),$$

.....

$$y(N-1) = x(0)e(N-1) + x(1)e(N-2) + \ldots + x(N-1)e(0),$$

or

$$y(j) = \sum_{i=0}^{N-1} x(i)e((j-i \bmod N)), \quad 0 \le j \le N.$$

Take discrete Fourier transform (DFT) of **y**,

$$Y(j) = X(j)E(j) \quad 0 \le j < N.$$

$$\because \; e(i) = \frac{1}{N} w^{ik} \quad 0 \le i < N \;,$$

$$\therefore \; E(j) = e(0) + e(1)w^{j} + \cdots + e(N-1)w^{(N-1)j}$$

$$= \frac{1}{N}\left( 1 + w^{k-j} + w^{2(k-j)} + \cdots + w^{(N-1)(k-j)} \right)$$

$$= \begin{cases} 1 & \text{if } j = N-k \\ 0 & \text{if } j \neq N-k \end{cases},$$

then

$$Y(j) = \begin{cases} X(j) & \text{if } j = N-k \\ 0 & \text{if } j \neq N-k \end{cases}.$$

## 6.2 Spectra of Non-abelian Codes Constructed by Dihedral Groups

Suppose group G is a Dihedral group $D_N = C_N \triangleleft C_2$, where

$$C_N = \langle a;\ a^N = 1 \rangle,\ C_2 = \langle t;\ t^2 = 1 \rangle, \text{ and } tat = a^{N-1}.$$

Suppose F is a finite field GF(q), whose characteristic does not divide 2N, and 2N divides (q-1), then we have a complete set of primitive orthognal idempotents for group algebra FG:

$$\frac{1}{N}\{\alpha_0(1+t)/2,\ \alpha_0(1-t)/2,\ \alpha_1,\ \alpha_2,\ \cdots,\ \alpha_{N-1}\}$$

where $\alpha_k = 1 + w^k a + w^{2k} a^2 + \cdots + w^{(N-1)k} a^{N-1}$, $w^N = 1$, $w \in F$.

Suppose e is an idempotent of group algebra $FD_N$, then ideal $FD_N e$ will be a Dihedral code. We will study transform domain characterization of codewords in the Dihedral code.

Let $x \in FG$, $e \in FG$, $y = xe$,

then

$$y(v) = \sum_{u \in G} x(u)\, e(u^{-1}v), \qquad v \in G.$$

Order the group $D_N$ by

$$g_0=1,\ g_1=t,\ g_2=a,\ g_3=at,\ g_4=a^2,\ g_5=a^2t,\ \cdots,\ g_{2N-2}=a^{N-1},\ g_{2N-1}=a^{N-1}t.$$

Denote $x(g_i)$, $y(g_i)$ and $e(g_i)$ by $x(i)$, $y(i)$ and $e(i)$, respectively, where $0 \le i < 2N$, then we have

$$\begin{aligned}
y(0) &= x(0)e(0) + x(1)e(1) + x(2)e(2N-2) + x(3)e(3) + \ldots \\
&\quad + x(2N-2)e(2) + x(2N-1)e(2N-1), \\
y(1) &= x(0)e(1) + x(1)e(0) + x(2)e(2N-1) + x(3)e(2) + \ldots \\
&\quad + x(2N-2)e(3) + x(2N-1)e(2N-2), \\
y(2) &= x(0)e(2) + x(1)e(2N-1) + x(2)e(0) + x(3)e(1) + \ldots \\
&\quad + x(2N-2)e(4) + x(2N-1)e(2N-3), \\
y(3) &= x(0)e(3) + x(1)e(2N-2) + x(2)e(1) + x(3)e(0) + \ldots \\
&\quad + x(2N-2)e(5) + x(2N-1)e(2N-4), \\
&\ldots\ldots \\
y(2N-2) &= x(0)e(2N-2) + x(1)e(3) + x(2)e(2N-4) + x(3)e(5) + \ldots \\
&\quad + x(2N-2)e(0) + x(2N-1)e(1), \\
y(2N-1) &= x(0)e(2N-1) + x(1)e(2) + x(2)e(2N-3) + x(3)e(4) + \ldots
\end{aligned}$$

$$+ x(2N-2)e(1) + x(2N-1)e(0);$$

or

$$y(i) = \sum_{j=0}^{N-1} [x(2j)e((i-2j) \bmod 2N) + x(2j+1)e((2j+1-i) \bmod 2N)], \quad 0 \le i < 2N.$$

Assume e is one of primitive orthognal idempotents in FG.

1) Suppose $e = \frac{1}{N}\alpha_k \quad 0 < k < N$ ,

where $\alpha_k = 1 + w^k a + w^{2k} a^2 + \cdots + w^{(N-1)k} a^{N-1}$ and $w^N = 1$,

then $e(1) = e(3) = \ldots = e(2N-1) = 0$ ,

$$e(0) = \frac{1}{N}, \; e(2) = \frac{1}{N}w^k, \; \ldots, \; e(2N-2) = \frac{1}{N}w^{(N-1)k},$$

and $y(0) = x(0)e(0) + x(2)e(2N-2) + x(4)e(2N-4) + \ldots + x(2N-2)e(2),$

$y(1) = x(1)e(0) + x(3)e(2) + x(5)e(4) + \ldots + x(2N-1)e(2N-2),$

$y(2) = x(0)e(2) + x(2)e(0) + x(4)e(2N-2) + \ldots + x(2N-2)e(4),$

$y(3) = x(1)e(2N-2) + x(3)e(0) + x(5)e(2) + \ldots + x(2N-1)e(2N-2),$

$\ldots\ldots$

$y(2N-2) = x(0)e(2N-2) + x(2)e(2N-4) + x(4)e(2N-6) + \ldots + x(2N-2)e(0),$

$y(2N-1) = x(1)e(2) + x(3)e(4) + x(5)e(6) + \ldots$

$$+ x(2N-1)e(0).$$

Take discrete Fourier transform (DFT) of **y**, let $0 \le p < 2N$,

$$\begin{aligned}
Y(p) &= y(0) + y(1)w_{2N}^{p} + y(2)w_{2N}^{2p} + \cdots + y(2N-1)w_{2N}^{(2N-1)p} \\
&= x(0)[e(0) + e(2)w_{2N}^{2p} + e(4)w_{2N}^{4p} + \cdots + e(2n-2)w_{2N}^{(2N-2)p}] \\
&+ x(1)[e(0)w_{2N}^{p} + e(2N-2)w_{2N}^{3p} + e(2N-4)w_{2N}^{5p} + \cdots + e(2)w_{2N}^{(2N-1)p}] \\
&+ x(2)[e(2N-2) + e(0)w_{2N}^{2p} + e(2)w_{2N}^{4p} + \cdots + e(2n-4)w_{2N}^{(2N-2)p}] \\
&+ x(3)[e(2)w_{2N}^{p} + e(0)w_{2N}^{3p} + e(2N-2)w_{2N}^{5p} + \cdots + e(4)w_{2N}^{(2N-1)p}] \\
&\cdots\cdots \\
&+ x(2N-2)[e(2) + e(4)w_{2N}^{2p} + e(6)w_{2N}^{4p} + \cdots + e(0)w_{2N}^{(2N-2)p}] \\
&+ x(2N-1)[e(2N-2)w_{2N}^{p} + e(2N-4)w_{2N}^{3p} + e(2N-6)w_{2N}^{5p} + \cdots + e(0)w_{2N}^{(2N-1)p}] \\
&= [x(0) + x(2)w_{2N}^{2p} + \cdots + x(2N-2)w_{2N}^{(2N-2)p}][e(0) + e(2)w_{2N}^{2p} + e(4)w_{2N}^{4p} \\
&\quad + \cdots + e(2N-2)w_{2N}^{(2N-2)p}] \\
&+ [x(1) + x(3)w_{2N}^{3p} + \cdots + x(2N-1)w_{2N}^{(2N-1)p}][e(0) + e(2)w_{2N}^{(2N-2)p} \\
&\quad + e(4)w_{2N}^{(2N-4)p} + \cdots + e(2N-2)w_{2N}^{2p}].
\end{aligned}$$

$\because e(0) = \frac{1}{N}$, $e(2) = \frac{1}{N}w^{k}$, $\cdots$, $e(2N-2) = \frac{1}{N}w^{(N-1)k}$,

$w = w_{2N}^{2}$, $w^{N} = 1$,

$$\begin{aligned}
\therefore\ & e(0) + e(2)w_{2N}^{2p} + \cdots + e(2N-2)w_{2N}^{(2N-2)p} \\
&= e(0) + e(2)w^{p} + \cdots + e(2N-2)w^{(N-1)p} \\
&= \frac{1}{N}(1 + w^{k-p} + w^{2(k-p)} + \cdots + w^{(N-1)(k-p)}) \\
&= \begin{cases} 1 & \text{if } p = N-k \text{ or } p = 2N-k \\ 0 & \text{if } p \neq N-k \text{ and } p \neq 2N-k \end{cases},
\end{aligned}$$

$$e(0) + e(2)\,w_{2N}^{(2N-2)p} + e(4)\,w_{2N}^{(2N-4)p} + \cdots + e(2N-2)\,w_{2N}^{2p}$$

$$= e(0) + e(2)\,w^{-p} + \cdots + e(2N-2)\,w^{-(N-1)p}$$

$$= \frac{1}{N}\left( 1 + w^{k-p} + w^{2(k-p)} + \cdots + w^{(N-1)(k-p)} \right)$$

$$= \begin{cases} 1 & \text{if } p = k \text{ or } p = N+k \\ 0 & \text{if } p \neq k \text{ and } p \neq N+k \end{cases} .$$

When $k \neq \frac{N}{2}$ ,

we have $k \neq N-k$ , $N+k \neq 2N-k$ , and

$$Y(p) = \begin{cases} x(0) + x(2)\,w_{2N}^{2p} + \cdots + x(2N-2)\,w_{2N}^{(2N-2)p} & \text{if } p=N-k \text{ or } p=2N-k \\ x(1)\,w_{2N}^{p} + x(3)\,w_{2N}^{3p} + \cdots + x(2N-1)\,w_{2N}^{(2N-1)p} & \text{if } p=k \text{ or } p=N+k \\ 0 & \text{otherwise} \end{cases} ,$$

then

$$Y(N-k) = Y(2N-k) = x(0) + x(2)\,w_{2N}^{2(N-k)} + \cdots + x(2N-2)\,w_{2N}^{(2N-2)(N-k)} ,$$

$$Y(k) = -Y(N+k) = x(1)\,w_{2N}^{k} + x(3)\,w_{2N}^{3k} + \cdots + x(2N-1)\,w_{2N}^{(2N-1)k} ,$$

$$Y(p) = 0 \qquad \text{if } p \neq k \text{ and } p \neq N-k \text{ and } p \neq N+k \text{ and } p \neq 2N-k \ ;$$

When $k = \frac{N}{2}$ ,

we have $k = N-k$ , $N+k = 2N-k = 3k$ , and

$$Y(p) = \begin{cases} x(0) + x(1)\,w_{2N}^{p} + x(2)\,w_{2N}^{2p} + \cdots + x(2N-1)\,w_{2N}^{(2N-1)p} & \text{if } p=k \text{ or } p=3k \\ 0 & \text{otherwise} \end{cases} ,$$

then

$$Y(k) = X(k) ,$$

$$Y(3k) = X(3k) ,$$

$Y(p) = 0 \qquad if\ p \neq k\ and\ p \neq 3k.$

2) Suppose $e = \frac{1}{2N}\alpha_0(1 + t)$

$= \frac{1}{2N}\ (\ 1\ \ 1\ \ 1\ \ 1\ \ldots\ \ 1),$

then

$$y(0) = y(1) = \ldots = y(2N-1)$$

$$= \frac{1}{2N}[x(0)+x(1)+\ldots+x(2N-1)],$$

$$Y(p) = y(0) + y(1)w_{2N}^{p} + y(2)w_{2N}^{2p} + \cdots + y(2N-1)w_{2N}^{(2N-1)p}$$

$$= \frac{1}{2N}[x(0)+x(1)+\cdots+x(2N-1)][1 + w_{2N}^{p} + w_{2N}^{2p} + \cdots + w_{2N}^{(2N-1)p}],$$

thus

$$Y(0) = x(0) + x(1) + \ldots + x(2N-1) = X(0),$$

$Y(p) = 0 \qquad if\ p \neq 0.$

3) Suppose $e = \frac{1}{2N}\alpha_0(1 - t)$

$= \frac{1}{2N}\ (\ 1\ \ -1\ \ 1\ \ -1\ \ldots\ \ 1\ \ -1),$

then

$$y(0) = y(2) = \ldots = y(2N-2)$$

$$= \frac{1}{2N}[x(0)+x(2)+\ldots+x(2N-2)-(x(1)+x(3)+\ldots+x(2N-1)],$$

$$y(1) = y(3) = \ldots = y(2N-1)$$

$$= \frac{1}{2N}[x(1)+x(3)+\ldots+x(2N-1)-(x(0)+x(2)+\ldots+x(2N-2)],$$

$$Y(p) = y(0) + y(1)w_{2N}^{p} + y(2)w_{2N}^{2p} + \cdots + y(2N-1)w_{2N}^{(2N-1)p}$$

$$= y(0)[1 + w_{2N}^{2p} + w_{2N}^{4p} + \cdots + w_{2N}^{(2N-2)p}]$$

$$+ \; y(1)\,[w_{2N}^{p} + w_{2N}^{3p} + \cdots + w_{2N}^{(2N-1)p}]$$

$$= [y(0) + y(1)\,w_{2N}^{p}]\,[1 + w_{2N}^{2p} + w_{2N}^{4p} + \cdots + w_{2N}^{(2N-2)p}] .$$

$$\because \; 1 + w_{2N}^{2p} + w_{2N}^{4p} + \cdots + w_{2N}^{(2N-2)p} = \begin{cases} N & \text{if } p=N \\ 0 & \text{if } p\neq N \end{cases},$$

$$w_{2N}^{N} = -1 ,$$

$$\therefore \; Y(N) = (y(0) - y(1))N$$

$$= x(0)+x(2)+\ldots+x(2N-2) - [x(1)+x(3)+\ldots+x(2N-1)]$$

$$= x(0) + x(1)\,w_{2N}^{N} + x(2)\,w_{2N}^{2N} + \cdots + x(2N-1)\,w_{2N}^{(2N-1)N}$$

$$= X(N) ,$$

$$Y(p) = 0 \qquad \text{if } p \neq N .$$

# 7 ENCODING ALGORITHM

## 7.1 Spectral Description of Cyclic Codes

In a cyclic code, every codeword c(x) is represented by a polynomial of degree n-1. A nonsystematic form can be written as c(x) = g(x)d(x), where d(x) is a data polynomial of degree of k-1. This is a (cyclic) convolution in the time domain:

$$c_i = \sum_{k=0}^{n-1} g_{((i-k))} d_k .$$

Therefore in the frequency domain, the encoding operation can be written as a product

$$C_j = G_j D_j .$$

Any spectrum that satisfies this expression is a frequency-domain codeword, provided that all components in the time domain are GF(q)-valued. Because the data spectrum is arbitrary, according to Theorem 5.5 in section 5, the only significant role of $G_j$ is to specify frequencies where the codeword spectrum $C_j$ is zero.

We can define a cyclic code alternatively as an ideal of group algebra $GF(q)C_n$. For simplicity, we assume n=q-1. Let

$$\{e_1, \ldots, e_n\}$$

is a complete set of primitive orthogonal idempotents of $GF(q)C_n$, and an idempotent e is a sum of certain of these primitive orthogonal idempotents:

$$e = 1 - (e_{j_1} + \ldots + e_{j_\varepsilon}),$$

which includes every primitive orthogonal idempotents of the complete set except $e_{j_1}, \ldots$ *and* $e_{j_\varepsilon}$. According to the transform domain characterization of cyclic codes in section 6.1, the cyclic code $GF(q)C_n e$ is the set of words over GF(q) whose spectrum is zero in corresponding components $(C_{n-j_1}, \ldots, C_{n-j_\varepsilon})$, and arbitrary in the remaining components.

The BCH codes are the cyclic codes that one obtains if the parity frequencies are chosen consecutively. A t-error-correcting BCH code of blocklength $n = q^m-1$ is the set of all word over GF(q) whose spectrum is zero in a specified block of 2t consecutive components.

When n = q-1 (or a factor of q-1), the BCH code is a Reed-Solomon code, which is a maximum-distance code; the codeword and the spectrum are in the same field. One can encode directly in the frequency domain by using the information symbols to specify spectral components. Every spectrum consistent with the parity constraints yields a codeword. Encoding is as follows. Some set of 2t consecutive frequencies (e.g., the first 2t) are chosen as the symbols constrained to zero. The n-2t unconstrained components of the spectrum are filled with information symbols from GF(q). The inverse Fourier transform then produces a

(nonsystematic) codeword. Because there are n-2t frequency components that can take on information values, we obtain a codeword of an (n, n-2t) Reed-Solomon code.

For the more general BCH codes, the encoding is more complex. Now there are two fields: the symbol field GF(q) and the locator field GF($q^m$) used for the spectrum. To get codewords in GF(q). we must choose only spectra that satisfy the conjugacy constraints of Theorem 5.6. Again, 2t consecutive components of the spectrum are chosen to be zero. The remaining symbols must be chosen from GF($q^m$) to represent the k information symbols only in those $q^k$ possible ways that have inverse Fourier transforms that are q-ary valued.

In the general case, the integers modulo n are divided into conjugacy classes:

$$A_j = \{j, jq, jq^2, \ldots, jq^{m_j-1}\}.$$

If the spectral component $C_j$ is specified, then every other spectral component whose index is in the conjugacy class of j must be a power of $C_j$ and hence cannot be separately specified. Further, if the conjugacy class has r members, then we must have

$$C_j^{q^r} = C_j$$

and

$$C_j^{q^r-1} = 1.$$

Consequently, we are not free to choose any element of Gf($q^m$) for $C_j$, but only those of order dividing $q^r-1$ or the zero element. Every element of Gf($q^m$) has order dividing $q^m-1$; hence $q^r-1$ divides $q^m-1$, and it is clear that the size of every conjugacy class divides m.

To specify an encoder, we break the first $q^m-1$ integers into conjugacy classes, and select one integer to represent each class. These representatives specify the uniquely assignable symbols. To form a BCH code, a block of 2t spectral components are chosen as parity frequencies and set to zero. The remaining assignable symbols are information symbols, arbitrary except for occasional constraints on the order. All other symbols indexed from the same conjugacy class are not free; they are obligatory frequencies.

Figure 7.1 shows the situation for GF(64). We choose the first column to be free symbols. If we take $C_1$, $C_2$, $C_3$, $C_4$, $C_5$ and $C_6$ to be parity frequencies, then we have a triple-error-correcting BCH code. Then $C_0$, $C_7$, $C_9$, $C_{11}$, $C_{13}$, $C_{15}$, $C_{21}$, $C_{23}$, $C_{27}$, and $C_{31}$ are the information symbols. $C_9$ and $C_{27}$ must be zero or symbols of order 7 (because $C_9^8 = C_9$ and $C_{27}^8 = C_{27}$). These are the elements of the subfield GF(8). $C_{21}$ must be zero or an element of order 3, (because $C_{21}^4 = C_{21}$). These are the elements of the subfield

GF(4). $C_0$ must be zero or an element of order 1. These are the elements of the subfield GF(2). All other symbols are arbitrary elements of GF(64). It requires a total of 45 information bits to specify these symbols. Hence, we have the (63, 45) triple-error-correcting BCH code.

| Free Frequencies | Obligatory Frequencies | Bit Content |
|---|---|---|
| $\{C_0\}$ | | 1 |
| $\{C_1$ | $C_2\ C_4\ C_8\ C_{16}\ C_{32}\}$ | 6 |
| $\{C_3$ | $C_6\ C_{12}\ C_{24}\ C_{48}\ C_{33}\}$ | 6 |
| $\{C_5$ | $C_{10}\ C_{20}\ C_{40}\ C_{17}\ C_{34}\}$ | 6 |
| $\{C_7$ | $C_{14}\ C_{28}\ C_{56}\ C_{49}\ C_{35}\}$ | 6 |
| $\{C_9$ | $C_{18}\ C_{36}\}$ | 3 |
| $\{C_{11}$ | $C_{22}\ C_{44}\ C_{25}\ C_{50}\ C_{37}\}$ | 6 |
| $\{C_{13}$ | $C_{26}\ C_{52}\ C_{41}\ C_{19}\ C_{38}\}$ | 6 |
| $\{C_{15}$ | $C_{30}\ C_{60}\ C_{57}\ C_{51}\ C_{39}\}$ | 6 |
| $\{C_{21}$ | $C_{42}\}$ | 2 |
| $\{C_{23}$ | $C_{46}\ C_{29}\ C_{58}\ C_{53}\ C_{43}\}$ | 6 |
| $\{C_{27}$ | $C_{54}\ C_{45}\}$ | 3 |
| $\{C_{31}$ | $C_{62}\ C_{61}\ C_{59}\ C_{55}\ C_{47}\}$ | 6 |

Figure 7.1 Structure of the spectrum over GF(64)

## 7.2 Encoding Algorithm for Dihedral Codes

We define a Dihedral code as an ideal of the group algebra $GF(q)D_N$ in section 4.5, where $D_N$ is a Dihedral group.

Suppose a Dihedral group $D_N = C_N \lhd C_2$, where $C_N$ is a cyclic group with a generator a and $C_2$ is a cyclic group with a generator t,

$$a^N = t^2 = 1,\ tat = a^{N-1}.$$

Suppose finite field F is GF(q), whose characteristic does not divide 2N, and 2N divides (q-1). Then a complete set of primitive orthognal idempotents of group algebra FG are

$$e_1 = \frac{1}{2N}\alpha_0(1+t),$$

$$e_2 = \frac{1}{2N}\alpha_0(1-t),$$

$$e_{k-2} = \frac{1}{N}\alpha_k \qquad 0 < k < N,$$

where $\alpha_k = 1 + w^k a + w^{2k}a^2 + \cdots + w^{(N-1)k}a^{N-1}$, $w \in F$, $w^N = 1$.

Any idempotent e will be a sum of certain of these primitive orthognal idempotents. We can generate a left ideal by an idempotent e:

$$W = GF(q)D_N e,$$

which is a non-abelian Dihedral code.

According to the transform domain characterization of Dihedral codes in section 6.2, the non-zero spectral components will only overlap for pairs of primitive idempotents $\frac{1}{N}\alpha_k$ and $\frac{1}{N}\alpha_{N-k}$, where 0<k<N, and there are following properties in spectra of Dihedral

codes: if $\frac{1}{N}\alpha_k$ and $\frac{1}{N}\alpha_{N-k}$ both are chosen, then the spectrum of the Dihedral code is arbitrary in corresponding components of $C_k$ , $C_{N-k}$ , $C_{N-k}$ *and* $C_{2N-k}$ ; if $\frac{1}{N}\alpha_k$ is chosen and $\frac{1}{N}\alpha_{N-k}$ is not chosen, then the spectrum of the Dihedral code is constrained in corresponding components $C_k = -C_{N-k}$ *and* $C_{N-k} = C_{2N-k}$ ; if $\frac{1}{N}\alpha_k$ or $\frac{1}{N}\alpha_{N-k}$ neither is chosen, then the spectrum of the Dihedral code is zero in corresponding components of $C_k$ , $C_{N-k}$ , $C_{N-k}$ and $C_{2N-k}$ . Then, using these spectral properties of Dihedral codes, we can easily encode Dihedral codes in the frequency domain as follows:

1) Find the complete set of primitive orthognal idempotents of a Dihedral group algebra $GF(q)D_N$ :

$$\{e_1, \cdots, e_{N-1}\}.$$

2) Choose an appropriate idempotent $e$, which is a sum of certain of these primitive orthognal idempotents,

$$e = e_{j_1} + \ldots + e_{j_t}.$$

3) Using above spectral properties of Dihedral codes, determine in which corresponding spectral components of chosen idempotents are arbitrary or contrained; information symbols will be assigned to these spectral components. Then set the remaining spectral components to zero.

4) The inverse Fourier transform then produces codewords of the

non-abelian Dihedral code.

For example, we will encode a Dihedral code generated by following idempotent:

$$e = e_1 + e_3 + e_4 + \cdots + e_N = 1 - (e_2 + e_{N-1}) .$$

Because the idempotent $e$ does not include $e_2$ *and* $e_{N-1}$ , where $e_2 = \frac{1}{2N}\alpha_0(1-t)$ and $e_{N-1} = \frac{1}{N}\alpha_{N-1}$ , and the idempotent $e$ does include $e_3 = \frac{1}{N}\alpha_1$ , the spectrum of the code satisfy:

$$C_1 = -C_{N-1} ,$$

$$C_{N-1} = C_{2N-1} ,$$

$$C_N = 0 ,$$

and arbitrary in the other spectral components.

Suppose the finite field is GF(7), the Dihedral group is $D_3$ and the idempotent is $e = e_1 + e_3 = 1 - (e_2 + e_4)$ . Then the spectrum of the code satisfy:

$$C_1 = -C_4 ,$$

$$C_2 = C_5 ,$$

$$C_3 = 0 ,$$

and $C_0$ is arbitrary. The inverse Fourier transform then produces codewords of the non-abelian Dihedral code as follows.

| | | | |
|---|---|---|---|
| 0 0 0 0 0 0 | 0 4 0 2 0 1 | 0 1 0 4 0 2 | 0 5 0 6 0 3 |
| 0 2 0 1 0 4 | 0 6 0 3 0 5 | 0 3 0 5 0 6 | 5 0 3 0 6 0 |
| 5 4 3 2 6 1 | 5 1 3 4 6 2 | 5 5 3 6 6 3 | 5 2 3 1 6 4 |

| | | | |
|---|---|---|---|
| 5 6 3 3 6 5 | 5 3 3 5 6 6 | 3 0 6 0 5 0 | 3 4 6 2 5 1 |
| 3 1 6 4 5 2 | 3 5 6 6 5 3 | 3 2 6 1 5 4 | 3 6 6 3 5 5 |
| 3 3 6 5 5 6 | 1 0 2 0 4 0 | 1 4 2 2 4 1 | 1 1 2 4 4 2 |
| 1 5 2 6 4 3 | 1 2 2 1 4 4 | 1 6 2 3 4 5 | 1 3 2 5 4 6 |
| 6 0 5 0 3 0 | 6 4 5 2 3 1 | 6 1 5 4 3 2 | 6 5 5 6 3 3 |
| 6 2 5 1 3 4 | 6 6 5 3 3 5 | 6 3 5 5 3 6 | 4 0 1 0 2 0 |
| 4 4 1 2 2 1 | 4 1 1 4 2 2 | 4 5 1 6 2 3 | 4 2 1 1 2 4 |
| 4 6 1 3 2 5 | 4 3 1 5 2 6 | 2 0 4 0 1 0 | 2 4 4 2 1 1 |
| 2 1 4 4 1 2 | 2 5 4 6 1 3 | 2 2 4 1 1 4 | 2 6 4 3 1 5 |
| 2 3 4 5 1 6 | 6 6 6 6 6 6 | 6 3 6 1 6 0 | 6 0 6 3 6 1 |
| 6 4 6 5 6 2 | 6 1 6 0 6 3 | 6 5 6 2 6 4 | 6 2 6 4 6 5 |
| 4 6 2 6 5 6 | 4 3 2 1 5 0 | 4 0 2 3 5 1 | 4 4 2 5 5 2 |
| 4 1 2 0 5 3 | 4 5 2 2 5 4 | 4 2 2 4 5 5 | 2 6 5 6 4 6 |
| 2 3 5 1 4 0 | 2 0 5 3 4 1 | 2 4 5 5 4 2 | 2 1 5 0 4 3 |
| 2 5 5 2 4 4 | 2 2 5 4 4 5 | 0 6 1 6 3 6 | 0 3 1 1 3 0 |
| 0 0 1 3 3 1 | 0 4 1 5 3 2 | 0 1 1 0 3 3 | 0 5 1 2 3 4 |
| 0 2 1 4 3 5 | 5 6 4 6 2 6 | 5 3 4 1 2 0 | 5 0 4 3 2 1 |
| 5 4 4 5 2 2 | 5 1 4 0 2 3 | 5 5 4 2 2 4 | 5 2 4 4 2 5 |
| 3 6 0 6 1 6 | 3 3 0 1 1 0 | 3 0 0 3 1 1 | 3 4 0 5 1 2 |
| 3 1 0 0 1 3 | 3 5 0 2 1 4 | 3 2 0 4 1 5 | 1 6 3 6 0 6 |
| 1 3 3 1 0 0 | 1 0 3 3 0 1 | 1 4 3 5 0 2 | 1 1 3 0 0 3 |
| 1 5 3 2 0 4 | 1 2 3 4 0 5 | 5 5 5 5 5 5 | 5 2 5 0 5 6 |

| | | | |
|---|---|---|---|
| 5 6 5 2 5 0 | 5 3 5 4 5 1 | 5 0 5 6 5 2 | 5 4 5 1 5 3 |
| 5 1 5 3 5 4 | 3 5 1 5 4 5 | 3 2 1 0 4 6 | 3 6 1 2 4 0 |
| 3 3 1 4 4 1 | 3 0 1 6 4 2 | 3 4 1 1 4 3 | 3 1 1 3 4 4 |
| 1 5 4 5 3 5 | 1 2 4 0 3 6 | 1 6 4 2 3 0 | 1 3 4 4 3 1 |
| 1 0 4 6 3 2 | 1 4 4 1 3 3 | 1 1 4 3 3 4 | 6 5 0 5 2 5 |
| 6 2 0 0 2 6 | 6 6 0 2 2 0 | 6 3 0 4 2 1 | 6 0 0 6 2 2 |
| 6 4 0 1 2 3 | 6 1 0 3 2 4 | 4 5 3 5 1 5 | 4 2 3 0 1 6 |
| 4 6 3 2 1 0 | 4 3 3 4 1 1 | 4 0 3 6 1 2 | 4 4 3 1 1 3 |
| 4 1 3 3 1 4 | 2 5 6 5 0 5 | 2 2 6 0 0 6 | 2 6 6 2 0 0 |
| 2 3 6 4 0 1 | 2 0 6 6 0 2 | 2 4 6 1 0 3 | 2 1 6 3 0 4 |
| 0 5 2 5 6 5 | 0 2 2 0 6 6 | 0 6 2 2 6 0 | 0 3 2 4 6 1 |
| 0 0 2 6 6 2 | 0 4 2 1 6 3 | 0 1 2 3 6 4 | 4 4 4 4 4 4 |
| 4 1 4 6 4 5 | 4 5 4 1 4 6 | 4 2 4 3 4 0 | 4 6 4 5 4 1 |
| 4 3 4 0 4 2 | 4 0 4 2 4 3 | 2 4 0 4 3 4 | 2 1 0 6 3 5 |
| 2 5 0 1 3 6 | 2 2 0 3 3 0 | 2 6 0 5 3 1 | 2 3 0 0 3 2 |
| 2 0 0 2 3 3 | 0 4 3 4 2 4 | 0 1 3 6 2 5 | 0 5 3 1 2 6 |
| 0 2 3 3 2 0 | 0 6 3 5 2 1 | 0 3 3 0 2 2 | 0 0 3 2 2 3 |
| 5 4 6 4 1 4 | 5 1 6 6 1 5 | 5 5 6 1 1 6 | 5 2 6 3 1 0 |
| 5 6 6 5 1 1 | 5 3 6 0 1 2 | 5 0 6 2 1 3 | 3 4 2 4 0 4 |
| 3 1 2 6 0 5 | 3 5 2 1 0 6 | 3 2 2 3 0 0 | 3 6 2 5 0 1 |
| 3 3 2 0 0 2 | 3 0 2 2 0 3 | 1 4 5 4 6 4 | 1 1 5 6 6 5 |
| 1 5 5 1 6 6 | 1 2 5 3 6 0 | 1 6 5 5 6 1 | 1 3 5 0 6 2 |

| | | | |
|---|---|---|---|
| 1 0 5 2 6 3 | 6 4 1 4 5 4 | 6 1 1 6 5 5 | 6 5 1 1 5 6 |
| 6 2 1 3 5 0 | 6 6 1 5 5 1 | 6 3 1 0 5 2 | 6 0 1 2 5 3 |
| 3 3 3 3 3 3 | 3 0 3 5 3 4 | 3 4 3 0 3 5 | 3 1 3 2 3 6 |
| 3 5 3 4 3 0 | 3 2 3 6 3 1 | 3 6 3 1 3 2 | 1 3 6 3 2 3 |
| 1 0 6 5 2 4 | 1 4 6 0 2 5 | 1 1 6 2 2 6 | 1 5 6 4 2 0 |
| 1 2 6 6 2 1 | 1 6 6 1 2 2 | 6 3 2 3 1 3 | 6 0 2 5 1 4 |
| 6 4 2 0 1 5 | 6 1 2 2 1 6 | 6 5 2 4 1 0 | 6 2 2 6 1 1 |
| 6 6 2 1 1 2 | 4 3 5 3 0 3 | 4 0 5 5 0 4 | 4 4 5 0 0 5 |
| 4 1 5 2 0 6 | 4 5 5 4 0 0 | 4 2 5 6 0 1 | 4 6 5 1 0 2 |
| 2 3 1 3 6 3 | 2 0 1 5 6 4 | 2 4 1 0 6 5 | 2 1 1 2 6 6 |
| 2 5 1 4 6 0 | 2 2 1 6 6 1 | 2 6 1 1 6 2 | 0 3 4 3 5 3 |
| 0 0 4 5 5 4 | 0 4 4 0 5 5 | 0 1 4 2 5 6 | 0 5 4 4 5 0 |
| 0 2 4 6 5 1 | 0 6 4 1 5 2 | 5 3 0 3 4 3 | 5 0 0 5 4 4 |
| 5 4 0 0 4 5 | 5 1 0 2 4 6 | 5 5 0 4 4 0 | 5 2 0 6 4 1 |
| 5 6 0 1 4 2 | 2 2 2 2 2 2 | 2 6 2 4 2 3 | 2 3 2 6 2 4 |
| 2 0 2 1 2 5 | 2 4 2 3 2 6 | 2 1 2 5 2 0 | 2 5 2 0 2 1 |
| 0 2 5 2 1 2 | 0 6 5 4 1 3 | 0 3 5 6 1 4 | 0 0 5 1 1 5 |
| 0 4 5 3 1 6 | 0 1 5 5 1 0 | 0 5 5 0 1 1 | 5 2 1 2 0 2 |
| 5 6 1 4 0 3 | 5 3 1 6 0 4 | 5 0 1 1 0 5 | 5 4 1 3 0 6 |
| 5 1 1 5 0 0 | 5 5 1 0 0 1 | 3 2 4 2 6 2 | 3 6 4 4 6 3 |
| 3 3 4 6 6 4 | 3 0 4 1 6 5 | 3 4 4 3 6 6 | 3 1 4 5 6 0 |
| 3 5 4 0 6 1 | 1 2 0 2 5 2 | 1 6 0 4 5 3 | 1 3 0 6 5 4 |

| | | | |
|---|---|---|---|
| 1 0 0 1 5 5 | 1 4 0 3 5 6 | 1 1 0 5 5 0 | 1 5 0 0 5 1 |
| 6 2 3 2 4 2 | 6 6 3 4 4 3 | 6 3 3 6 4 4 | 6 0 3 1 4 5 |
| 6 4 3 3 4 6 | 6 1 3 5 4 0 | 6 5 3 0 4 1 | 4 2 6 2 3 2 |
| 4 6 6 4 3 3 | 4 3 6 6 3 4 | 4 0 6 1 3 5 | 4 4 6 3 3 6 |
| 4 1 6 5 3 0 | 4 5 6 0 3 1 | 1 1 1 1 1 1 | 1 5 1 3 1 2 |
| 1 2 1 5 1 3 | 1 6 1 0 1 4 | 1 3 1 2 1 5 | 1 0 1 4 1 6 |
| 1 4 1 6 1 0 | 6 1 4 1 0 1 | 6 5 4 3 0 2 | 6 2 4 5 0 3 |
| 6 6 4 0 0 4 | 6 3 4 2 0 5 | 6 0 4 4 0 6 | 6 4 4 6 0 0 |
| 4 1 0 1 6 1 | 4 5 0 3 6 2 | 4 2 0 5 6 3 | 4 6 0 0 6 4 |
| 4 3 0 2 6 5 | 4 0 0 4 6 6 | 4 4 0 6 6 0 | 2 1 3 1 5 1 |
| 2 5 3 3 5 2 | 2 2 3 5 5 3 | 2 6 3 0 5 4 | 2 3 3 2 5 5 |
| 2 0 3 4 5 6 | 2 4 3 6 5 0 | 0 1 6 1 4 1 | 0 5 6 3 4 2 |
| 0 2 6 5 4 3 | 0 6 6 0 4 4 | 0 3 6 2 4 5 | 0 0 6 4 4 6 |
| 0 4 6 6 4 0 | 5 1 2 1 3 1 | 5 5 2 3 3 2 | 5 2 2 5 3 3 |
| 5 6 2 0 3 4 | 5 3 2 2 3 5 | 5 0 2 4 3 6 | 5 4 2 6 3 0 |
| 3 1 5 1 2 1 | 3 5 5 3 2 2 | 3 2 5 5 2 3 | 3 6 5 0 2 4 |
| 3 3 5 2 2 5 | 3 0 5 4 2 6 | 3 4 5 6 2 0 | |

Figure 7.2

Codewords of a (6,3) non-abelian Dihedral code over DF(7)

# 8 TEST OF CHARACTERISTIC

Suppose we define Dihedral codes as ideals of the Dihedral group algebra $GF(7)D_3$, where $D_3 = C_3 \triangleleft C_2$, $C_3 = \langle a; a^3=1 \rangle$, $C_2 = \langle t; t^2=1 \rangle$, and $tat = a^2$, then we can construct Dihedral codes from idempotents of the group algebra. A complete set of primitive orthognal idempotents of the Dihedral group algebra $GF(7)D_3$ is

$$\{e_1, e_2, e_3, e_4\},$$

where

$$e_1 = \frac{1}{6}\alpha_0(1+t),$$

$$e_2 = \frac{1}{6}\alpha_0(1-t),$$

$$e_3 = \frac{1}{3}\alpha_1 ,$$

$$e_4 = \frac{1}{3}\alpha_2 ,$$

$$\alpha_k = 1 + w^k a + w^{2k} a^2 \quad (k=0,1,2),$$

$$w \in GF(7),\ w^3 = 1 .$$

Figure 8.1 shows the minimum Hamming distance for each Dihedral code of $GF(7)D_3$.

| GF | Dihedral Group | Idempotents of $GF(7)D_3$ | Lengths of Dihedral Codes | Dimensions of Dihedral Codes | Minimum Distances |
|---|---|---|---|---|---|
| Z/7 | $D_3$ | $e_1$ | 6 | 1 | 6 |
| | | $e_2$ | 6 | 1 | 6 |
| | | $e_3$ | 6 | 2 | 3 |

| | | | | | |
|---|---|---|---|---|---|
| | | $e_4$ | 6 | 2 | 3 |
| | | $e_1+e_2$ | 6 | 2 | 3 |
| | | $e_1+e_3$ | 6 | 3 | 3 |
| | | $e_1+e_4$ | 6 | 3 | 3 |
| | | $e_2+e_3$ | 6 | 3 | 3 |
| | | $e_2+e_4$ | 6 | 3 | 3 |
| | | $e_3+e_4$ | 6 | 4 | 2 |
| | | $e_1+e_2+e_3$ | 6 | 4 | 2 |
| | | $e_1+e_2+e_4$ | 6 | 4 | 2 |
| | | $e_1+e_3+e_4$ | 6 | 5 | 2 |
| | | $e_2+e_3+e_4$ | 6 | 5 | 2 |

Figure 8.1 Minimum Distances of Dihedral Codes of $GF(7)D_3$

The Singleton Bound D = n-k+1 provides an upper bound of the minimum weight of any linear code (n,k). The Griesmer Bound [53] provides a lower bound on the length, n, of a linear code over GF(q) for a given dimension k and a given minimum distance d

$$n(k,d) \geq G(k,d) = \sum_{i=0}^{k-1} \left[\frac{d}{q^i}\right]$$

where [x] denotes the smallest integer than or equal to x. We can also use Griesmer Bound to determine if d is the maximum minimum distance found for an (n,k) linear code: If G(k,d+1) > n then d is the maximum minimum distance. For example, the (6,5) code over GF(7) has a minimum distance d = 2, and G(k,d+1) = 3 + $[\frac{3}{7}]$ + $[\frac{3}{7^2}]$ + $[\frac{3}{7^3}]$ + $[\frac{3}{7^4}]$ = 7 > 6, so d is the maximum minimum distance and the code is optimal. Unfortunately, the (6,5) code

is trivial and just a parity-check cyclic code; the (6,5) code constructed by $e_2+e_3+e_4$ consist of all sequences **c** in $(GF(7))^6$ such that $\sum c_k=0$ and the (6,5) code constructed by $e_1+e_3+e_4$ consist of all sequences **c** in $(GF(7))^6$ such that $\sum_{k\ odd} c_k = \sum_{k\ even} c_k$. The (6,1) code is also trivial and just a repetition cyclic code; the (6,1) code constructed by $e_1$ consist of $\{(c,c,c,c,c,c), c\in GF(7)\}$ and the (6,1) code constructed by $e_2$ consist of $\{(c,-c,c,-c,c,-c), c\in GF(7)\}$. It can be checked that the (6,2) code constructed by $e_1+e_2$ and the (6,4) code constructed by $e_3+e_4$ are cyclic codes also. We could find that minimum distances of Dihedral codes except above mentioned trivial cyclic codes do not reach the maximum minimum distance in the sense of Singleton Bound or the Griesmer Bound.

When we compare codes with the same length, we can say that: if we have two codes of the same dimension, we prefer the code with the larger Hamming distance; if we have two codes of the same Hamming distance, we prefer the code with the larger dimension. To generalize these rules, we can use the sum of dimension and Hamming distance of the code as a criterion to judge: if the sum is larger, the code is better. Comparing above Dihedral codes of $GF(7)D_3$, we could find that good Dihedral codes of $GF(7)D_3$ are the (6,3) codes constructed by $e_1+e_3$, $e_1+e_4$, $e_2+e_3$

or $e_2+e_4$, which have a minimum distance 3 and can correct a single error.

Suppose we define Dihedral codes as ideals of the Dihedral group algebra $GF(11)D_5$, where $D_5 = C_5 \triangleleft C_2$, $C_5 = \langle a; a^5=1 \rangle$, $C_2 = \langle t; t^2=1 \rangle$, and $tat = a^4$. Then we can construct Dihedral codes from idempotents of the group algebra. A complete set of primitive orthognal idempotents of the Dihedral group algebra $GF(11)D_5$ is

$$\{e_1, e_2, e_3, e_4, e_5, e_6\},$$

where

$$e_1 = \frac{1}{10}\alpha_0(1+t),$$

$$e_2 = \frac{1}{10}\alpha_0(1-t),$$

$$e_3 = \frac{1}{5}\alpha_1 ,$$

$$e_4 = \frac{1}{5}\alpha_2 ,$$

$$e_5 = \frac{1}{5}\alpha_3 ,$$

$$e_6 = \frac{1}{5}\alpha_4 ,$$

$$\alpha_k = 1 + w^k a + w^{2k} a^2 + w^{3k} a^3 + w^{4k} a^4 \qquad (k=0,1,2,3,4),$$

$$w \in GF(11),\ w^5 = 1 .$$

The minimum Hamming distance for each Dihedral code of $GF(11)D_5$ shows in Figure 8.2.

| GF | Dihedral Group | Idempotents of $GF(11)\,D_5$ | Lengths of Dihedral Codes | Dimensions of Dihedral Codes | Minimum Distances |
|---|---|---|---|---|---|
| Z/11 | $D_5$ | $e_1$ | 10 | 1 | 10 |
| | | $e_2$ | 10 | 1 | 10 |
| | | $e_3$ | 10 | 2 | 5 |
| | | $e_4$ | 10 | 2 | 5 |
| | | $e_5$ | 10 | 2 | 5 |
| | | $e_6$ | 10 | 2 | 5 |
| | | $e_1+e_2$ | 10 | 2 | 5 |
| | | $e_1+e_3$ | 10 | 3 | 5 |
| | | $e_1+e_4$ | 10 | 3 | 5 |
| | | $e_1+e_5$ | 10 | 3 | 5 |
| | | $e_1+e_6$ | 10 | 3 | 5 |
| | | $e_2+e_3$ | 10 | 3 | 5 |
| | | $e_2+e_4$ | 10 | 3 | 5 |
| | | $e_2+e_5$ | 10 | 3 | 5 |
| | | $e_2+e_6$ | 10 | 3 | 5 |
| | | $e_3+e_4$ | 10 | 4 | 4 |
| | | $e_3+e_5$ | 10 | 4 | 4 |
| | | $e_3+e_6$ | 10 | 4 | 4 |
| | | $e_4+e_5$ | 10 | 4 | 4 |
| | | $e_4+e_6$ | 10 | 4 | 4 |
| | | $e_5+e_6$ | 10 | 4 | 4 |
| | | $e_1+e_2+e_3$ | 10 | 4 | 4 |
| | | $e_1+e_2+e_4$ | 10 | 4 | 4 |
| | | $e_1+e_2+e_5$ | 10 | 4 | 4 |

| | | | | | |
|---|---|---|---|---|---|
| | | $e_1+e_2+e_6$ | 10 | 4 | 4 |
| | | $e_1+e_3+e_4$ | 10 | 5 | 4 |
| | | $e_1+e_3+e_5$ | 10 | 5 | 4 |
| | | $e_1+e_3+e_6$ | 10 | 5 | 4 |
| | | $e_1+e_4+e_5$ | 10 | 5 | 4 |
| | | $e_1+e_4+e_6$ | 10 | 5 | 4 |
| | | $e_1+e_5+e_6$ | 10 | 5 | 4 |
| | | $e_2+e_3+e_4$ | 10 | 5 | 4 |
| | | $e_2+e_3+e_5$ | 10 | 5 | 4 |
| | | $e_2+e_3+e_6$ | 10 | 5 | 4 |
| | | $e_2+e_4+e_5$ | 10 | 5 | 4 |
| | | $e_2+e_4+e_6$ | 10 | 5 | 4 |
| | | $e_2+e_5+e_6$ | 10 | 5 | 4 |
| | | $e_3+e_4+e_5$ | 10 | 6 | 3 |
| | | $e_3+e_4+e_6$ | 10 | 6 | 3 |
| | | $e_3+e_5+e_6$ | 10 | 6 | 3 |
| | | $e_4+e_5+e_6$ | 10 | 6 | 3 |
| | | $e_1+e_2+e_3+e_4$ | 10 | 6 | 3 |
| | | $e_1+e_2+e_3+e_5$ | 10 | 6 | 3 |
| | | $e_1+e_2+e_3+e_6$ | 10 | 6 | 3 |
| | | $e_1+e_2+e_4+e_5$ | 10 | 6 | 3 |
| | | $e_1+e_2+e_4+e_6$ | 10 | 6 | 3 |
| | | $e_1+e_2+e_5+e_6$ | 10 | 6 | 3 |
| | | $e_1+e_3+e_4+e_5$ | 10 | 7 | 3 |
| | | $e_1+e_3+e_4+e_6$ | 10 | 7 | 3 |
| | | $e_1+e_3+e_5+e_6$ | 10 | 7 | 3 |

| | | | | | |
|---|---|---|---|---|---|
| | | $e_1+e_4+e_5+e_6$ | 10 | 7 | 3 |
| | | $e_2+e_3+e_4+e_5$ | 10 | 7 | 3 |
| | | $e_2+e_3+e_4+e_6$ | 10 | 7 | 3 |
| | | $e_2+e_3+e_5+e_6$ | 10 | 7 | 3 |
| | | $e_2+e_4+e_5+e_6$ | 10 | 7 | 3 |
| | | $e_3+e_4+e_5+e_6$ | 10 | 8 | 2 |
| | | $e_1+e_2+e_3+e_4+e_5$ | 10 | 8 | 2 |
| | | $e_1+e_2+e_3+e_4+e_6$ | 10 | 8 | 2 |
| | | $e_1+e_2+e_3+e_5+e_6$ | 10 | 8 | 2 |
| | | $e_1+e_2+e_4+e_5+e_6$ | 10 | 8 | 2 |
| | | $e_1+e_3+e_4+e_5+e_6$ | 10 | 9 | 2 |
| | | $e_2+e_3+e_4+e_5+e_6$ | 10 | 9 | 2 |

Figure 8.2 Minimum Distances of Dihedral Codes of $GF(11)D_5$

The (10,1) codes and (10,9) codes are trivial cyclic codes. It can be checked that the (10,2) code constructed by $e_1+e_2$, the (10,4) codes constructed by $e_3+e_6$ and $e_4+e_5$, the (10,5) codes constructed by $e_1+e_3+e_6$, $e_1+e_4+e_5$, $e_2+e_3+e_6$ and $e_2+e_4+e_5$, and the (10,6) codes constructed by $e_2+e_3+e_6$ and $e_2+e_4+e_5$, are cyclic codes also. Comparing Dihedral codes of $GF(11)D_5$, we could find that good Dihedral codes of $GF(11)D_5$ are the (10,7) codes constructed by $e_1+e_3+e_4+e_5$, $e_1+e_3+e_4+e_6$, $e_1+e_3+e_5+e_6$, $e_1+e_4+e_5+e_6$, $e_2+e_3+e_4+e_5$, $e_2+e_3+e_4+e_6$, $e_2+e_3+e_5+e_6$ or $e_2+e_4+e_5+e_6$, which have a minimum distance 3 and can correct a single error.

In general, suppose we define Dihedral codes as ideals of a

group algebra $GF(q)D_N$ , where a Dihedral group $D_N = C_N \triangleleft C_2$, $C_N$ is a cyclic group with a generator a and $C_2$ is a cyclic group with a generator t,

$$a^N = t^2 = 1,\ tat = a^{N-1}.$$

Suppose characteristic of GF(q) does not divide 2N, and 2N divides (q-1). Then a complete set of primitive orthognal idempotents of the Dihedral group algebra $GF(q)D_N$ is

$$\{e_1, \cdots, e_{N-1}\},$$

where

$$e_1 = \frac{1}{2N}\alpha_0(1+t),$$

$$e_2 = \frac{1}{2N}\alpha_0(1-t),$$

$$e_{k-2} = \frac{1}{N}\alpha_k \qquad 0 < k < N ,$$

$$\alpha_k = 1 + w^k a + w^{2k}a^2 + \cdots + w^{(N-1)k}a^{N-1} , \quad w \in F,\ w^N = 1 .$$

Comparing all codes constructed by each idempotent of the Dihedral group algebra $GF(q)D_N$ , we could find that good Dihedral codes of $GF(q)D_N$ are the (2N, 2N-3) codes constructed by $1-(e_1+e_3)$, $1-(e_1+e_4)$, ..., $1-(e_1+e_{N-1})$, $1-(e_2+e_3)$, $1-(e_2+e_4)$, ... or $1-(e_2+e_{N-1})$, which have a minimum distance $d^*=3$ and can correct a single error.

We can construct a new family of single-error-correcting non-abelian Dihedral codes $(n,k,d^*)$ over GF(q) as follows

| q | n | k | $d^*$ |
|---|---|---|---|
| 7 | 6 | 3 | 3 |
| 9 | 8 | 5 | 3 |
| 11 | 10 | 7 | 3 |
| 13 | 12 | 9 | 3 |
| 17 | 16 | 13 | 3 |
| 19 | 18 | 15 | 3 |
| 23 | 22 | 19 | 3 |
| 25 | 24 | 21 | 3 |
| 27 | 26 | 23 | 3 |
| 29 | 28 | 25 | 3 |
| 31 | 30 | 27 | 3 |
| 37 | 36 | 33 | 3 |
| 41 | 40 | 37 | 3 |
| ... | ... | ... | ... |

Figure 8.3 Single-error-correcting Dihedral Codes

# 9 DECODING ALGORITHM

## 9.1 Spectral Techniques for Decoding of Cyclic Codes

An error-control code must be judged not only by its rate and minimum distance, but also by whether a decoder can be built economically for it. Usually there are many ways to decode a given code. Included here are decoding techniques by working in the frequency domain. We will show decoding procedures for BCH codes using the termnology of the Fourier transform.

A received word **v** with components $v_i = c_i + e_i$ for i=0,...,N-1 is the sum of a codeword **c** and an errorword **e**. The decoder must process the received word so as to remove the error word **e**; the information is then recovered from **e**. The syndromes of this noisy BCH codeword **v** are given by the following set of equations:

$$S_j = \sum_{i=0}^{n-1} \alpha^{i(j+j_0-1)} v_i = v(\alpha^{j+j_0-1}) \qquad j=1,\ldots,2t.$$

Obviously, the syndromes are computed as 2t components of a Fourier transform. The received noisy codeword **v** = **c** + **e** has Fourier transform with components $V_j = C_j + E_j$ for j=0,...,N-1, and the syndromes are the 2t components of this spectrum from $j_0$ to $j_0+2t-1$. But by construction of the BCH code, the parity frequencies (for j = $j_0$,..., $j_0+2t-1$) have spectral components equal to zero:

$$C_j = 0 \quad j=j_0,\cdots,j_0+2t-1 .$$

Hence

$$S_j = V_{j+j_0-1} = E_{j+j_0-1} \quad j=1,\cdots,2t .$$

The block of syndromes gives us a window through which we can look at 2t of the n components of the spectrum of the error pattern. But we know from the BCH bound that if the error pattern has weight of at most t, then these 2t syndromes are enough to uniquely determine the error pattern.

Supoose there are $\nu<t$ errors at locations $\alpha^{i_k}$ for $k=1,\cdots,\nu$. The errorlocator polynomial is

$$\Lambda(x) = \prod_{k=1}^{\nu} (1 - x\alpha^{i_k}) .$$

The inverse Fourier transform of the vector $\Lambda$ is the same as $\Lambda(\alpha^{-i})$, which is $\Lambda(x)$ evaluatd at $\alpha^{-i}$. Clearly, $\Lambda(\alpha^{-i})$ equals zero if and only if i is an error location. Thus $\Lambda(x)$ has been defined so that in the time domain, $\lambda_i=0$ whenever $e_i\neq 0$. Therefore $\lambda_i e_i=0$ for all i, and thus, by the convolution theorem, the convolution in the frequency domain is zero:

$$\sum_{j=0}^{N-1} \Lambda_j E_{k-j} = 0 \quad k = 0, \cdots, N-1$$

Because $\Lambda(x)$ is a polynomial of degree of at most t, $\Lambda_j=0$ for $j>t$. Then

$$\sum_{j=0}^{t} \Lambda_j E_{k-j} = 0 \quad k = 0, \cdots, N-1$$

Because $\Lambda_0$ equals one, this can be written in the form

$$E_k = -\sum_{j=1}^{t} \Lambda_j E_{k-j} \qquad k = 0, \cdots, N-1$$

This is a set of n equations in n-t unknowns (t coefficients of $\Lambda(x)$ and n-2t components of **E**) and in 2t known values of **E** given by the syndromes. Of the n equations, there are t equations that involve only components of $\Lambda$ and the known components of **E** given by the syndromes. That is, the t equations

$$S_k = -\sum_{j=1}^{t} \Lambda_j S_{k-j} \qquad k = t+1, \cdots, 2t$$

involve only the known syndromes and the t unknown components of $\Lambda$. These are always solvable for $\Lambda$, as we saw in (*8), using for example the Berlekamp-Massey algorithm.

The remaining components of **S** can then be obtained by recursive extension; that is, using the above convolution equation to find $S_{2t-1}$ from the known components of **S** and $\Lambda$, then to find $S_{2t-2}$, and so on. This computation can be described as the operation of a linear-feedback shift register with tap weights given by the coefficients $\Lambda$ and initialized with $S_1, \ldots, S_t$. In this way $S_j$ is computed for all j, $E_j$ equals $S_{j-j_0+1}$ and

$$C_j = V_j - E_j.$$

An inverse Fourier transform completes the decoding. If the encoder uses the information symbols in the frequency domain to specify the values of the spectrum, then the corrected spectrum gives the information symbols directly. The decoder does not

have an inverse transform.

## 9.2 Decoding Algorithm for Dihedral Codes

Suppose group G is a Dihedral group $D_N = C_N \triangleleft C_2$, where $C_N$ is a cyclic group with a generator a and $C_2$ is a cyclic group with a generator t,

$$a^N = t^2 = 1,\ tat = a^{N-1}.$$

Suppose finite field F is GF(q), whose characteristic does not divide 2N, and 2N divides (q-1). Then a complete set of primitive orthognal idempotents of group algebra FG are

$$e_1 = \frac{1}{2N}\alpha_0(1+t),$$

$$e_2 = \frac{1}{2N}\alpha_0(1-t),$$

$$e_{k-2} = \frac{1}{N}\alpha_k \qquad 0 < k < N,$$

where $\alpha_k = 1 + w^k a + w^{2k} a^2 + \cdots + w^{(N-1)k} a^{N-1}$, $w^N = 1$, $w \in F$.

Any idempotent e will be a sum of certain of these primitive orthognal idempotents. We can generate a left ideal by an idempotent e:

$$W = GF(q) D_N e,$$

which is a non-abelian Dihedral code.

Now, we will develop a decoding algorithm for the Dihedral code generated by an idempotent:

$$e = 1 - (e_1 + e_m) \qquad 3 \le m \le N+1$$

or

$$e = 1 - (e_2 + e_m) \qquad 3 \le m \le N+1 .$$

We will only show the decoding algorithm for the Dihedral code generated by an idempotent $e = 1 - (e_2 + e_m)$ here; the decoding algorithm for the other case is similar. Let p=N-(m-2). From the results in section 7.2, knowing that the idempotent e excludes $e_2$ *and* $e_m$ , and

$$e_m = \frac{1}{N}\alpha_{m-2} ,$$

we have that the DFT coefficients of the code satisfy:

$$C_p = -C_{N-p} ,$$

$$C_{N-p} = C_{2N-p} ,$$

$$C_N = 0 ,$$

and arbitrary in the other spectral components.

This code can correct a single error. We will show the decoding algorithm in the frequency domain as follows:

Suppose there is a single error at location $\alpha^i$. The error location polynomial is

$$\Lambda(x) = 1 - x\alpha^i$$

*where* $\Lambda_0 = 1$ , $\Lambda_1 = -\alpha^i$ and $\alpha$ is an element of order 2N in F.

Suppose spectral components of a received word, a codeword and an errorword are

$V_j$, $C_j$ *and* $E_j$ (j = 0, 1, ... , 2N-1), respectively,

then

$$V_j = C_j + E_j \quad (j = 0, 1, \ldots, 2N-1),$$

$$V_N = E_N ,$$

$$V_{N-p} - V_{2N-p} = E_{N-p} - E_{2N-p} ,$$

and $V_p + V_{N-p} = E_p + E_{N-p}$ .

$$\because \quad \sum_{j=0}^{2N-1} \Lambda_j E_{k-j} = 0 \qquad k = 0, \cdots, 2N-1 ,$$

$$\Lambda_j = 0 \qquad j>1 ,$$

$$\therefore \quad E_k = -\Lambda_1 E_{k-1} \qquad k = 0, \cdots, 2N-1 .$$

Then $E_{N-p} = (-\Lambda_1) E_{N-p-1} = (-\Lambda_1)^2 E_{N-p-2} = \cdots = (-\Lambda_1)^p E_N$ ,

$$E_{2N-p} = (-\Lambda_1) E_{2N-p-1} = (-\Lambda_1)^2 E_{2N-p-2} = \cdots = (-\Lambda_1)^{N-p} E_N ,$$

$$E_{N-p} = (-\Lambda_1)^{-p} E_N ,$$

and $E_p = (-\Lambda_1)^{-(N-p)} E_N$ .

We have

$$V_{N-p} - V_{2N-p} = ((-\Lambda_1)^{-p} - (-\Lambda_1)^{N-p}) V_N$$

and $V_p + V_{N-p} = ((-\Lambda_1)^{-(N-p)} + (-\Lambda_1)^p) V_N$ .

Because $N$ , $p$ , $V_N$ , $V_p$ , $V_{N-p}$ , $V_{N+p}$ , $V_{2N-p}$ are known, and there are only a finite number of field elements to check for the unknown $\Lambda_1$, we can find $\Lambda_1$ by trial and error. Because $E_N = V_N$ is known, we can obtain remaining components $E_k$ ($k = 0, \cdots N-1, N+1, \cdots 2N-1$) by $E_k = -\Lambda_1 E_{k-1}$ $k = 0, \cdots, 2N-1$.

Then we have

$$C_j = V_j - E_j \quad (j = 0, 1, \ldots, 2N-1).$$

Because the encoder uses the information symbols in the frequency domain to specify the values of the spectrum, then the corrected spectrum gives the information symbols directly.

Now, We will prove following property: the solution for $\Lambda_1$ is unique.

Theorem 9.1: If a single error occurs, i.e. following equations

$$V_{N-p} - V_{2N-p} = ((-\Lambda_1)^{-p} - (-\Lambda_1)^{N-p}) V_N \qquad (9\text{-}1)$$

and $$V_p + V_{N+p} = ((-\Lambda_1)^{-(N-p)} + (-\Lambda_1)^{p}) V_N \qquad (9\text{-}2)$$

has a non-zero solution for $\Lambda_1$ , then the solution is unique.

Proof: Because $V_N = E_N \neq 0$ , for simplicity, let

$$x = -\Lambda_1 ,$$

$$a = (V_{N-p} - V_{2N-p}) / V_N ,$$

and $$b = (V_p + V_{N+p}) / V_N ,$$

then we have equivalent equations:

$$x^{-p} - x^{N-p} = a$$

and $$x^{-(N-p)} + x^{p} = b ,$$

or

$$x^{-p}(1 - x^{N}) = a \qquad (9\text{-}3)$$

and $$x^{p}(x^{-N} + 1) = b . \qquad (9\text{-}4)$$

Lemma 9.2: If a = b = 0, no non-zero solution for above set of

equations (9-3) and (9-4).

Proof: Assume equation (9-3) has a solution $x_0 \neq 0$.

$\because \quad a = 0 \ , \ x_0 \neq 0$

Then $x_0^N = 1$ from equation (9-3), and $x_0^{-N} + 1 = 1 + 1$ .

From assumption that F=GF(q) and 2N divides (q-1), we have

$$x_0^{-N} + 1 = 1 + 1 \neq 0 \ .$$

$\therefore \ x_0^P (x_0^{-N} + 1) \neq 0 \ ,$

i.e. $x_0$ is not a solution of equation (9-4).

Lemma 9.3: (1) If $a \neq 0$ and equation (9-3) has a solution, then the solution is unique;

(2) If $b \neq 0$ and equation (9-4) has a solution, then the solution is unique.

Proof: (1) Suppose $a \neq 0$ and $x_0$ is a solution of equation (9-3), then

$$x_0^{-P}(1 - x_0^N) = a \ ,$$

$$x_0 \neq 0 \ .$$

Suppose $x_0 = \alpha^i$ where $\alpha$ is a primitive element of the finite field F=GF(q), then

$$x_0^N = (\alpha^i)^N = (\alpha^N)^i \ .$$

$\because \quad \alpha^{2N} = 1 \ \textit{and} \ \alpha^N = -1 ,$

$$\therefore \quad x_0^N = (-1)^i = \begin{cases} 1 & \textit{if } i \textit{ is even} \\ -1 & \textit{if } i \textit{ is odd} \end{cases} .$$

$\because \quad a \neq 0$,

$\therefore \quad x_0^N = -1$ ,

then $1 - x_0^N = 2$,

$$2x_0^{-P} = a \ ,$$

$$x_0 = (\frac{a}{2})^{-P} = (\frac{2}{a})^P \ .$$

Thus $x_0$ is unique.

(2) Similarly, we can prove second part of lemma 9.3. If one error occurs, from lemma 9.2, we have $a \neq 0$ *or* $b \neq 0$. According to lemma 9.3, the solution of equations (9-3) and (9-4) is unique. Equivalently, the solution of equations (9-1) and (9-2) is unique.

# 10 CONCLUSION

In this dissertation, we have developed algorithms for computing the complete set of primitive orthogonal idempotents for non-ablian groups of the form $A \triangleleft H$, where A is a normal finite abelian group and H is an arbitrary finite group. Although this class of groups is limited from a mathematical view point, it contains a rich set of non-abelian groups for coding applications. Then we have constructed non-abelian Dihedral codes by the complete set of primitive orthogonal idempotents of Dihedral group algebra and found specific characterization for Dihedral codes in Fourier transform domain. Based on these spectral characterization, we have developed encoding algorithm and decoding algorithm for Dihedral codes.

The algorithms for computing the complete set of primitive orthogonal idempotents for non-abelian groups offer many avenues for further research:

* Because we have a rich set of non-abelian groups and non-abelian codes have total new structures, we still do not know much of their features. It is well worth continuing our studies in different kind of non-abelian codes.

* If group algebras is taken relative to fields of

characteristic 0 such as real and complex fields, we will have a rich set of application for digital signal processing. Complete sets of orthogonal idempotents will determine special classes of multirate filters.

## BIBLIOGRAPHY

[1] D. Augot, P. Charpin, and N. Sendrier, "The minimum distance of some binary codes via Newton's identities," *Lecture Notes in Computer Science*, vol. 514. Also in *Eurocode '90: Int. Symp. on Coding Theory and Applications* (Udine, Italy, Nov. 5-9, 1990), pp. 65-73.

[2] D. Augot, and F. Levy-dit-Vehel, "Bounds on the minimum distance of the duals of BCH codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1257-1260, 1996.

[3] L. R. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing sybmol error rate," *IEEE Trans. Inform. Theory*, vol. IT-20, pp.284-287, 1974.

[4] E. R. Berlekamp, *Algebraic Coding Theory*, New York: McGraw-Hill, 1968.

[5] S. D. Berman, "On the theory of group codes," *Kibernetika*, vol. 3, pp. 31-39, 1967.

[6] _____, "Semisimple cyclic and abelian codes," *Kibernetika*, vol. 3, pp. 21-30, 1967.

[7] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: turbo codes," in Proc. *IEEE Int. Conf. on Communications* (Geneva, Switzerland, 1993), pp. 1064-1070.

[8] R. E. Blahut, "Algebraic codes in the frequency domain," CISM Courses and Lectures, no. 258, pp. 447-494, 1979.

[9] _____, *Theory and Practice of Error Control Codes*, New York: Addison-Wesley, 1983.

[10] I. F. Blake and R. C. Mullin, *The Mathematical Theory of Coding*, New York: Academic Press, 1975.

[11] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error-correcting binary group codes," *Inf. and Contr.*, no. 3, pp. 68-79, 1960.

[12] P. Bours, J. C. M. Janssen, M. van Asperdt, and H. C. A. van Tilborg, "Algebraic decoding beyond $e_{BCH}$ of some binary cyclic codes, when $e > e_{BCH}$," *IEEE Trans. Inform. Theory*, vol. 36, pp. 214-222, 1990.

[13] S. A. Brown, "Implementing extended Newton's identities to genrate decoding syndrome matrices for cyclic codes," NSF Research Experiences for Undergraduates (REU) Program Summer Project Rep., Dept. Elec. Eng. and Comput. Sci., Lehigh Univ., Bethlehem, PA, Aug. 1994.

[14] P. Camion, "Abelian codes," Tech. Rep. No.1059, Mathematical Res. Center, 1971.

[15] R. T. Chien, "A new proof of the BCH bound," *IEEE Trans. Inform. Theory*, vol. IT-18, p. 541, 1972.

[16] M. Clausen, "Fast Generalized Fourier Transforms," Theoret, Comput. Sci., in press.

[17] P. Delsarte, "Automorphisms of abelian codes," *Phillips Res. Rep.*, vol. 25, pp. 389-402, 1970.

[18] M. Elia, "Algebraic decoding of the (23, 12,7) Golay code," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 150-151, 1987.

[19] G. L. Feng and K. K. Tzeng, "A generalization of the Berlekamp-Massey algorithm for multisequence shift-register synthesis with applications to decoding cyclic codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1274-1287, 1991.

[20] _____, "Decoding cyclic and BCH codes up to actual minimum distance using nonrecurrent syndrome dependence relations," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1716-1723, 1991.

[21] _____, "A new procedure for decoding cyclic and BCH codes up to actual minimum distance," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1364-1374, 1994.

[22] G. D. Forney, Jr., *Concatenated Codes*. Cambridge, MA: MIT Press, 1966.

[23] _____, "Generalized minimum distance decoding," *IEEE Trans. Inform. Theory*, vol. IT-12, pp.125-131, 1966.

[24] _____, "Final report on a coding system design for advanced solar missions," Contract NAS2-3637, NASA Ames Res. Ctr., Moffet Field CA, Dec. 1967.

[25] _____, "Convolutional codes I: Algebraic structure," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 720-738, 1970.

[26] _____, "Coset coedes II: Binary lattices and related codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1152-1187, 1988.

[27] _____, "Dimension/length profiles and trellis complexity of lattices," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1753-1772, 1994.

[28] R. G. Gallager, *Low Density Parity-Check Codes*. Cambridge, MA: MIT Press, 1962.

[29] C. R. P. Hartmann and K. K. Tzeng, "Generalizations of the BCH bound," *Inform. Contr.*, vol. 20, pp. 489-498, 1972.

[30] C. R. P. Hartmann, K. K. Tzeng, and R. T. Chien, "Some results on the minimum distance structure of cyclic codes," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 402-409, 1972.

[31] A. Hocquenghem, "Codes correcteurs d'erreurs," *Chiffres*, no. 2, pp. 147-156, 1959.

[32] R. B. Holmes, "Signal Processing on Finite Groups," MIT Lincoln Laboratory, technical report 873, 1990.

[33] H. Imai and S. Hirakawa, "A new multilevel coding method using error-correcting codes," *IEEE Trans. Inform. Theory*, vol. 23 pp. 371-377, 1977.

[34] D. Lind and B. H. Marcus, *An Introduction to Symbolic Dynamics and Coding*. New York: Cambridge Univ. Press, 1995.

[35] J. H. van Lint and R. M. Wilson, "On the minimum distance of cyclic codes," *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 23-40, 1986.

[36] F. J. MacWilliams, "Binary codes which are ideals in the group algebra of an abelian group," *BSTJ*, vol. 49, pp. 987-1011, 1970.

[37] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. New York: North-Holland, 1977.

[38] J. L. Massey, *Threshold Decoding*. Cambridge, MA: MIT Press, 1963.

[39] _____, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 122-127, 1969.

[40] J. L. Massey and T. Schaub, "Linear complexity in coding theory," in *Coding Theory and Applications* (Lecture Notes in Computer Science, vol. 311). New York: Springer-Verlag, 1988.

[41] O. Moreno and V. Kumar, "Minimum distance bounds for cyclic codes and Deligne's theorem," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1524-1534, 1993.

[42] O. Moreno, V. Zinoviev, and V. Kumar, "The exact minimum distance of some cyclic codes," in *Proc. AGCT4'94* (Novgorod, Russia).

[43] D. J. Muder, "Minimal trellises for block codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1049-1053, 1988.

[44] W. W. Peterson and E.J. Weldon, *Error Correcting Codes*, 2nd ed. Cambridge, MA: MIT Press, 1972.

[45] J. M. Pollard, "The Fast Fourier Transform in a Finite Field," *Math. Computat.*, no. 25, pp. 365-374, 1971.

[46] I. S. Reed, T. K. Truong, X. Chen, and X. Yin, "The algebraic decoding of the (41,21,9) quadratic residue codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 974-986, 1992.

[47] C. Roos, "A new lower bound for the minimum distance of a cyclic code," *IEEE Trans. Inform. Theory*, vol. IT-29, no 3, 1983.

[48] T. Schaub, "A linear complexity approach to cyclic codes,"

dissertation, Swiss Federal Institute of Technology, Zuerich, 1988.

[49] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol.27, pp. 379-423 and pp. 623-656, 1948.

[50] B. -Z. Shen and K. K. Tzeng, "Generation of matrices for determining minimum distance and decoding of algebraic-geometric codes," in *Proc. 1994 IEEE Int. Workshop on Information Theory* (Moscow, Russia, July 3-8, 1994), pp.89-90. Also, *IEEE Trans. Inform. Theory* (Special Issue on Algebraic-Geometric Codes), vol. 41, pp. 1703-1708, 1995.

[51] K. K. Shen, C. Wang, K. K. Tzeng, and B.-Z. Shen, "Table of matrices for determining minimum distance and decoding of cyclic codes," Tech. Rep., Dept. Elec. Eng. and Comput. Sci., Lehigh Univ., Bethlehem, PA, Sept. 1994.

[52] _____, "Generation of matrices for determining minimum distance and decoding of cyclic codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 653-657, 1996.

[53] G. Solomon and J. J. Stiffler, "Algebraically punctured cyclic codes," *Inform. Contr.*, no. 8, pp. 170-179, 1965.

[54] P. Stevens, "Extension of the BCH decoding algorithm to decode binary cyclic codes up to their maximum error-correction capabilities." *IEEE Trans. Inform. Theory*, vol. 34, pp. 1332-1340, 1988.

[55] K. K. Tzeng and C. R. P. Hartmann, "On the minimum distance of certain reversible cyclic codes," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 644-646, 1970.

[56] A. J. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm." *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 260-269, 1967.

[57] J. C. Willems, "Models for dynamics," in *Dynamics Reported*, vol. 2. New York: Wiley, 1989, pp.171-269.

[58] J. Wolfmann, "New bounds on cyclic codes from algebraic curves," in *Lecture Notes in Computer Science*, vol.388. New

York: Springer-Verlag, 1989, pp. 47-62.

[59] J. M. Wozencraft and B. Reiffen, *Sequential Decoding*. New York: Wiley, 1961.