Transform Domain Study of Some Families of Codes

A Thesis
Submitted for the Degree of

Doctor of Philosophy

in the Faculty of Engineering

by
Bikash Kumar Dey

Department of Electrical Communication Engineering
Indian Institute of Science
Bangalore 560012

August 2002

Abstract

Discrete Fourier transform (DFT) is the most widely used tool in any field of electrical engineering. In the name of Mattson-Solomon polynomials, the DFT was used in the context of linear cyclic codes in the early history of coding theory. From then on, it has become a very useful tool for investigating structural properties of many different families of codes over different alphabets.

Codes with rich algebraic structure are of strong interest to coding theorists due to the ease of design and decoding. Classical families of linear cyclic codes like BCH codes and Reed-Muller codes were the center of attraction for a long time. Though rich algebraic structures like linearity and cyclicity make design and decoding easier, they restrict the freedom of choice of long good codes. No asymptotically good family of cyclic code is found and it is known that BCH codes are not asymptotically good. So, successful attempts have been made to slacken the restrictions of linearity and cyclicity to look for good codes. However, to keep the problem of designing and decoding tractable, neither of the structural restrictions is completely given away.

Compromising linearity gives codes which are linear over some subfield F_q of the alphabet field F_{q^m} but not necessarily linear over F_{q^m}. Different good classes of F_q-linear cyclic codes (F_qLC) over F_{q^m} like twisted BCH codes and subspace subcodes of Reed-Solomon (SSRS) codes are found by different authors [1, 2]. A part of this thesis characterizes the F_q-linear cyclic codes over F_{q^m} in DFT domain when length is relatively prime to q. With respect to any given F_q-basis of F_{q^m}, every n-length F_q-linear cyclic codes over F_{q^m} can be considered as a linear m-quasi-cyclic code of length mn over F_q. A way is given to derive a lower bound on the minimum Hamming distance of the corresponding quasi-cyclic code using the DFT domain characterization of an F_qLC code.

Slackening the cyclicity gives the quasi-cyclic codes. For a length n code, it is called an l-quasi-cyclic code (where l divides n) if it is closed under the l-times cyclic shifts. So, cyclic codes are nothing but 1-quasi-cyclic codes. Refining the works of Chen, Peterson and Weldon [3], Kasami [4] proved that 2-quasi-cyclic codes asymptotically meet a slightly loose version of Gilbert-Varshamov bound. Many quasi-cyclic codes were found, which are best known codes of their lengths. The structural properties and enumeration of quasi-cyclic codes were discussed using different approaches in [5–7]. The algebraic structure of the l-quasi-cyclic codes of length n is investigated in this thesis with the help

of conventional DFT of length n. A way is given to derive a lower bound on the minimum Hamming distance of a quasi-cyclic code Using the DFT domain characterization of the code. Since DFT is defined only when the length n is relatively prime to the characteristic of the field, the scope of this treatment is restricted to the same case. Under the action of the co-ordinate permutation 'l-times cyclic shift', there are l equal length cycles of the co-ordinate positions. A parallel work by Ling and Solé [8] effectively takes the DFT cycle-wise and investigates the structure of quasi-cyclic codes. Their approach is restricted to the case: $(\frac{n}{l}, q) = 1$, a weaker restriction than that $((n, q) = 1)$ needed in the approach presented here.

The classes of codes like cyclic codes, abelian codes, quasi-cyclic codes [9] and abelian codes are defined by certain restrictions on their permutation groups. Cyclic codes of length n are those codes, whose permutation groups contain a transitive cyclic subgroup. Similarly, l-quasi-cyclic codes of length n are those, which are closed under a fixed point free (for $l \neq n$) permutation with equal cycle lengths or equivalently which are closed under the action of a permutation group generated by such a permutation. All these classes of codes are defined to be with their permutation group containing a certain type of abelian subgroup. So, it could be interesting to find a general common way of treating these codes. Precisely that is done in a part of this thesis. Given any abelian subgroup G of the permutation group of the co-ordinates such that the exponent is relatively prime to q, G-invariant codes are investigated with the help of a suitably defined DFT. Duals of G-invariant codes and self-dual G-invariant codes are characterized in transform domain. A general formula of enumeration of self-dual G-invariant codes is found using this characterization. A way to derive a lower bound on the minimum Hamming distance of a G-invariant code is outlined. Karlin's decoding algorithm for a systematic quasi-cyclic code with single row of circulants in the generator matrix is extended to the case of systematic quasi-abelian codes. In particular, this can be used to decode systematic quasi-cyclic codes with columns of parity circulants in the generator matrix. Note that the part of the work mentioned in the last paragraph does not follow as corollary to this part, since a conventional DFT of length n is used in the previous case. Here, the DFT is defined so as to 'fit' the group G and it's restriction to the case of quasi-cyclic codes will result in a DFT as used by Ling and Solé [8]. As a result, the enumeration formula for self-dual G-invariant codes gives all their existence and enumeration results on self-dual quasi-cyclic codes as corollaries.

For the next part of the works of this thesis, the field structure of the alphabet is compromised and more general structures namely Galois rings are taken as alphabet. Though coding theorists have for a long time had theoretical interest on codes over integer residue rings [10, 11], codes over integer residue rings and more generally over Galois rings have received serious attention [12–18] after it was shown [19] that some important families of nonlinear binary codes can be obtained by Gray map from linear codes over $\mathbb{Z}_4$. A part of this thesis generalizes the transform domain study of G-invariant codes (G is as in the previous paragraph).

The automorphism/permutation groups of codes over finite fields are known to be useful for decoding (see [20–26] for examples) Recently, Blackford and Ray-Chaudhury [27] used transform domain techniques to permutation groups of cyclic codes over Galois rings. Here, their technique is extended to permutation groups of abelian codes over Galois rings.

A code is called affine invariant if it is invariant under the affine permutations. Often it is comparatively easier to determine the full permutation groups of affine invariant codes [28–32]. The conditions for extended cyclic codes over finite fields and integer residue rings to be affine-invariant were derived by respectively Kasami, Lin and Peterson [33] Abdukhalikov [34]. Blackford and Ray-Chaudhuri [27] used transform domain approach to characterize affine invariant extended cyclic codes of length 2^m over subrings of $GR(4, m)$ and using this characterization, they found new classes of affine invariant codes over Galois rings from BCH codes. Their approach is extended to extended cyclic codes of length 2^m over any subring of $GR(2^e, m)$ for $m \geq e - 1$ and also to extended cyclic codes of length p^m over $GR(p^2, m)$ (where $m \geq 1$) for arbitrary prime p. New classes of affine invariant codes are found using these results.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Cyclic Codes in Transform Domain

Discrete Fourier transform (DFT) is the most widely used tool in any field of electrical engineering. In the name of Mattson-Solomon polynomials, the DFT was used in the context of linear cyclic codes in the early history of coding theory. From then on, it has become a very useful tool for investigating structural properties of many different families of codes over different alphabets. Some classical works in this context is due to Mattson and Solomon [35] and Blahut [36]. A lot more work has been done and [37–41] are but to mention a very few.

In this section, the most widely studied family of codes, namely cyclic codes, is discussed with discrete Fourier transform as a groundwork for the next chapters. A detailed treatment on cyclic codes is available in any standard book on coding theory (e.g. [20, 42–46]).

A cyclic code $\mathcal{C}$ of length n over F_q is such that cyclic shift of any codeword is also a codeword. That is, if $\mathbf{a} = (a_0, a_1, \cdots, a_{n-1}) \in F_q^n$, then $(a_1, a_2, \cdots, a_{n-1}, a_0) \in F_q^n$. The vector $(a_0, a_1, \cdots, a_{n-1}) \in F_q^n$ is also represented by the polynomial

$$a(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_{n-1} X^{n-1}.$$

In polynomial form, the cyclic shift is equivalent to multiplication (modulo $(X^n - 1)$) by X. So, a linear cyclic code can be considered as a subset of all polynomials of degree at most $n-1$ which is closed under multiplication (modulo $(X^n - 1)$) by any polynomial. In other words, a cyclic code is an ideal of the ring $\frac{F_q[X]}{(X^n-1)}$. Since $\frac{F_q[X]}{(X^n-1)}$ is a principal ideal ring, any cyclic code has a generator polynomial $g(X)$ of minimum degree and it is easy to see that $g(X)$ divides $X^n - 1$. So, the set of roots (in appropriate extension field) of $g(X)$ is a subset of the roots of $X^n - 1$ with multiplicities, less than or equal to that in $X^n - 1$ and the code is fully and uniquely determined by the this set of roots of $g(X)$ with their multiplicities. When n is relatively prime to q, $X^n - 1$ does not have any multiple root and we'll be interested only in this case. When n is not relatively prime to q, the cyclic codes of length n are referred to as repeated root cyclic codes [47–50]. For the rest of the section, n is assumed to be relatively prime to q.

Let r be the smallest positive integer such that $n|(q^r - 1)$. Then All the roots of $X^n - 1$ are in F_{q^r}. Let $\alpha \in F_{q^r}$ be an element of order n. The DFT of the vector $\mathbf{a} = (a_0, a_1, \cdots, a_{n-1}) \in F_q^n$ is defined to be $\mathbf{A} = (A_0, A_1, \cdots, A_{n-1}) \in F_{q^r}^n$, where

$$A_j = \sum_{i=0}^{n-1} \alpha^{ij} a_i \quad \text{for } j = 0, 1, \cdots, n-1 \tag{1.1}$$

and the inverse transform is given by

$$a_i = n^{-1} \sum_{j=0}^{n-1} \alpha^{-ij} A_j \quad \text{for } i = 0, 1, \cdots, n-1. \tag{1.2}$$

For any $j \in [0, n-1]$, the *q-cyclotomic coset modulo n* of j, denoted by $[j]_n^q$, is defined as

$$[j]_n^q = \{i \in [0, n-1] | j \equiv iq^t \bmod n \text{ for some nonnegative integer } t\}.$$

The superscript $[j]_n^q$ will sometimes be omitted when it is obvious.

Example 1.1.1. Table 1.1 shows cyclotomic cosets modulo 15 and 63 for different q.

Table 1.1: Cyclotomic Cosets modulo 15 and 63

(a) Cyclotomic Cosets modulo 15

$2/2^3$-cyclotomic cosets	$\{0\}$	$\{1,2,4,8\}$				$\{3,6,9,12\}$				$\{5,10\}$		$\{7,13,11,14\}$			
cardinality	1	4				4				2		4			
2^2-cyclotomic cosets	$\{0\}$	$\{1,4\}$		$\{2,8\}$		$\{3,12\}$		$\{6,9\}$		$\{5\}$	$\{10\}$	$\{7,13\}$		$\{14,11\}$	
cardinality	1	2		2		2		2		2		2		2	
2^4-cyclotomic cosets	$\{0\}$	$\{1\}$	$\{2\}$	$\{4\}$	$\{8\}$	$\{3\}$	$\{6\}$	$\{9\}$	$\{12\}$	$\{5\}$	$\{10\}$	$\{7\}$	$\{13\}$	$\{11\}$	$\{14\}$
cardinality	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

(b) Cyclotomic Cosets modulo 63

$2/2^5$-cyclotomic cosets	$\{0\}$	$\{1,2,4,8,16,32\}$						$\{3,6,12,24,48,33\}$						$\{5,10,20,40,17,34\}$						$\{9,18,36\}$		
cardinality	1	6						6						6						3		
		$\{7,14,28,56,49,35\}$						$\{11,22,44,25,50,37\}$						$\{13,26,52,41,19,38\}$						$\{27,54,45\}$		
		6						6						6						3		
		$\{15,30,60,57,51,39\}$						$\{23,46,29,58,53,43\}$						$\{31,62,61,59,55,47\}$						$\{21,42\}$		
		6						6						6						2		
$2^2/2^4$-cyclotomic cosets	$\{0\}$	$\{1,4,16\}$			$\{2,8,32\}$			$\{3,12,48\}$			$\{6,24,33\}$			$\{5,20,17\}$			$\{10,40,34\}$			$\{9,18,36\}$		
cardinality	1	3			3			3			3			3			3			3		
		$\{7,28,49\}$			$\{14,56,35\}$			$\{11,44,50\}$			$\{22,25,37\}$			$\{13,52,19\}$			$\{26,41,38\}$			$\{27,54,45\}$		
		3			3			3			3			3			3			3		
		$\{15,60,51\}$			$\{30,57,39\}$			$\{23,29,53\}$			$\{46,58,43\}$			$\{31,61,55\}$			$\{62,59,47\}$			$\{21\}$	$\{42\}$	
		3			3			3			3			3			3			1	1	
2^3-cyclotomic cosets	$\{0\}$	$\{1,8\}$		$\{2,16\}$		$\{4,32\}$		$\{3,24\}$		$\{6,48\}$		$\{12,33\}$		$\{5,40\}$		$\{10,17\}$		$\{20,34\}$		$\{9\}$	$\{18\}$	$\{36\}$
cardinality	1	2		2		2		2		2		2		2		2		2		1	1	1
		$\{7,56\}$		$\{14,49\}$		$\{28,35\}$		$\{11,25\}$		$\{22,50\}$		$\{44,37\}$		$\{13,41\}$		$\{26,19\}$		$\{52,38\}$		$\{27\}$	$\{54\}$	$\{45\}$
		2		2		2		2		2		2		2		2		2		1	1	1
		$\{15,57\}$		$\{30,51\}$		$\{60,39\}$		$\{23,58\}$		$\{46,53\}$		$\{29,43\}$		$\{31,59\}$		$\{62,55\}$		$\{61,47\}$		$\{21,42\}$		
		2		2		2		2		2		2		2		2		2		2		
2^6-cyclotomic cosets	$\{0\}$	$\{1\}$	$\{8\}$	$\{2\}$	$\{16\}$	$\{4\}$	$\{32\}$	$\{3\}$	$\{24\}$	$\{6\}$	$\{48\}$	$\{12\}$	$\{33\}$	$\{5\}$	$\{40\}$	$\{10\}$	$\{17\}$	$\{20\}$	$\{34\}$	$\{9\}$	$\{18\}$	$\{36\}$
cardinality	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
		$\{7\}$	$\{56\}$	$\{14\}$	$\{49\}$	$\{28\}$	$\{35\}$	$\{11\}$	$\{25\}$	$\{22\}$	$\{50\}$	$\{44\}$	$\{37\}$	$\{13\}$	$\{41\}$	$\{26\}$	$\{19\}$	$\{52\}$	$\{38\}$	$\{27\}$	$\{54\}$	$\{45\}$
		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
		$\{15\}$	$\{57\}$	$\{30\}$	$\{51\}$	$\{60\}$	$\{39\}$	$\{23\}$	$\{58\}$	$\{46\}$	$\{53\}$	$\{29\}$	$\{43\}$	$\{31\}$	$\{59\}$	$\{62\}$	$\{55\}$	$\{61\}$	$\{47\}$	$\{21\}$	$\{42\}$	
		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

The DFT defined by (1.1) is a F_q-linear map satisfying the following two properties:

Conjugacy Constraint : $\mathbf{A} \in F_{q^r}^n$ is DFT of some vector $\mathbf{a} \in F_q^n$ if and only if $A_{jq} = A_j^q$ for all $j \in [0, n-1]$. Clearly, this constraint restricts A_j to be in the subfield $F_{q^{r_j}}$, where r_j is the length of $[j]_n$. Note that a specific value for A_j uniquely specifies the value of all the transform components $A_{j'}$ for $j' \in [j]_n$.

Cyclic Shift Property : If $\mathbf{A} = DFT(\mathbf{a})$, $\mathbf{b} \in F_q^n$ such that $b_i = a_{i-1}$, and $\mathbf{B} = DFT(\mathbf{b})$, then $B_j = \alpha^j A_j$.

The roots of $X^n - 1$ are $\{\alpha^j | j \in [0, n-1]\}$. It is clear from the definition of DFT that α^j is a root of $g(X)$ if and only if $A_j = 0$ for all codewords $\mathbf{a} \in \mathcal{C}$. So, the set $T = \{j \in [0, n-1] | A_j = 0 \text{for all} \mathbf{a} \in \mathcal{C}\}$ is called the defining set of $\mathcal{C}$. Due to conjugacy constraint, T is union of some q-cyclotomic cosets modulo n.

The following bound on the minimum Hamming distance of a cyclic code is the most important property of cyclic code.

BCH Bound: The minimum Hamming distance of a cyclic code $\mathcal{C}$ is more than the length of the longest cyclically consecutive sequence of numbers in T.

So, to obtain a code with minimum distance at least $\delta+1$, one needs to take a δ -length sequence S in $[0, n-1]$ and $T = [S]_n^q$. The resulting codes are called BCH codes. When $n = q-1$, $[S]_n^q = S$ and the cyclic codes with defining sets of the form $T = \{1, 2, \cdots, \delta\}$ are called Reed-Solomon codes and are famous as a class of MDS (maximum distance separable) codes [20] and for the ease of decoding. Other popular cyclic codes include Reed-Muller codes and quadratic residue codes.

1.2 Quasi-cyclic Codes and F_qLC codes

Though rich algebraic structures like linearity and cyclicity make design and decoding easier, they restrict the freedom of choice of long good codes. No asymptotically good family of cyclic code is found and it is known that BCH codes are not asymptotically good, that is, keeping the normalized rate fixed, as the length increases the normalized minimum Hamming distance goes towards zero. So, successful attempts have been made to slacken the restrictions of linearity and cyclicity to look for good codes. However, to keep the problem of designing and decoding tractable, neither of the structural restrictions is completely given away.

Compromising linearity gives codes which are linear over some subfield F_q of the alphabet field F_{q^m} but not necessarily linear over F_{q^m}. Different good classes of F_q-linear cyclic codes (F_qLC) over F_{q^m} like twisted BCH codes and subspace subcodes of Reed-Solomon (SSRS) codes are found by different authors [1, 2]. A part of this thesis investigates the algebraic structure of the F_q-linear cyclic codes over F_{q^m} in DFT domain when length is relatively prime to q. With respect to any given F_q-basis of F_{q^m}, every n-length F_q-linear cyclic codes over F_{q^m} can be considered as a linear m-quasi-cyclic code of length mn over F_q. The minimum distance of the corresponding quasi-cyclic code is investigated.

Slackening the cyclicity gives the quasi-cyclic codes. For a length n code, it is called an l-quasi-cyclic code (where l divides n) if it is closed under the l-times cyclic shifts. So an l-quasi-cyclic code can be viewed as a submodule of the l dimensional free module $(F_q C_{\frac{n}{l}})^l$ or $\left(\frac{F_q[X}{(X^{\frac{n}{l}}-1)}\right)^l$. Cyclic codes are nothing but 1-quasi-cyclic codes. Refining the works of Chen, Peterson and Weldon [3], Kasami [4] proved that 2-quasi-cyclic codes asymptotically meet a slightly loose version of Gilbert-Varshamov bound. Many quasi-cyclic codes are found, which are best known for their lengths [51–57]. The structural properties and enumeration of quasi-cyclic codes were discussed using different approaches in [5–7]. The algebraic structure of the l-quasi-cyclic codes of length n is investigated in this thesis with the help of conventional DFT of length n.

1.3 Codes over Galois Rings

Though coding theorists have for a long time had theoretical interest on codes over integer residue rings [10, 11, 58–61], codes over integer residue rings and more generally over Galois rings have received serious attention [12–18] after it was shown [19] that some important families of nonlinear binary codes can be obtained by Gray map from linear codes over $\mathbb{Z}_4$. Transform technique was used for cyclic and abelian codes over $\mathbb{Z}_m$ in [27, 62, 63]. A part of this thesis generalizes the transform domain study (in Chapter 4) of G-invariant codes when G is any abelian group of permutations G for codes over Galois rings.

1.4 Permutation Group of Codes and Affine Invariant Codes

Let $\mathcal{C}$ be an $[n, k]$ over F_q linear code and G a permutation group of degree n. Then G acts on $\mathcal{C}$ in the following way: for a codeword $\mathbf{a}$ of $\mathcal{C}$ and a permutation x of G, the image of $\mathbf{a}$ under x is obtained from $\mathbf{a}$ by permuting the coordinate positions of $\mathbf{a}$ according to x. This action is called the permutation action of G on $\mathcal{C}$. The set (which forms a subgroup) of permutations in the symmetry group of degree n under which a code $\mathcal{C}$ is closed/invariant is called the permutation group of $\mathcal{C}$. More generally, the set of monomial automorphisms of F_q^n, under which a code $\mathcal{C}$ is closed/invariant is called the monomial automorphism group of $\mathcal{C}$.

The automorphism/permutation groups of codes over finite fields are known to be useful for decoding (see [20–26] for examples) Recently, Blackford and Ray-Chaudhury [27] used transform domain techniques to permutation groups of cyclic codes over Galois rings. Here, their technique is extended to permutation groups of abelian codes over Galois rings.

Permutations of F_{p^m} (where p is a prime) of the form $x \mapsto ax + b$, where $a, b \in F_{p^m}$, $a \neq 0$, are called the affine permutations. These permutations form a subgroup of the symmetric group of order p^m and is denoted as $AGL(1, p^m)$. A code of length p^m with components indexed by elements of F_{p^m} is said to be affine invariant if it is invariant under the affine permutations. Clearly, affine invariant codes, after the 0'th component deleted, are cyclic codes. Kasami, Lin and Peterson [33] found a necessary and sufficient condition on the defining set of any cyclic code, under which the extended cyclic code is affine invariant. As corollaries, they showed that the famous extended BCH and generalized Reed-Muller codes are affine invariant. Often it is comparatively easier to determine the full permutation groups of affine invariant codes [28–32]. The conditions for extended cyclic codes over integer residue rings to be affine-invariant were derived by Abdukhalikov [34]. Blackford and Ray-Chaudhuri [27] used transform domain approach to characterize affine invariant extended cyclic codes of length 2^m over subrings of $GR(4, m)$ and using this characterization, they found new classes of affine invariant codes over Galois rings from BCH codes.

1.5 Contribution and Organization of the Thesis

In Chapter 2 of this thesis, the algebraic structure of the F_q-linear cyclic codes over F_{q^m} is investigated in DFT domain when length is relatively prime to q. With respect to any given F_q-basis of F_{q^m}, every n-length F_q-linear cyclic codes over F_{q^m} can be considered as a linear m-quasi-cyclic code of length mn over F_q. The minimum distance of the corresponding quasi-cyclic code is investigated.

In Chapter 3, the linear quasi-cyclic codes are studied in conventional DFT domain. A way is given to derive a lower bound on the minimum Hamming distance of a quasi-cyclic code Using the DFT domain characterization of the code.

In Chapter 4, the algebraic structure of codes closed under any arbitrary abelian subgroup G of S_n (group of permutations of n elements) is investigated in a suitable transform domain. These codes are precisely those which have G as a subgroup of their permutation groups. When special types of G are taken, G-invariant codes coincide with the class of quasi-abelian codes and thus with the classes of quasi-cyclic codes and abelian codes. Tanner's approach for getting a bound on the minimum distance from a set of parity check equations over an extension field is extended and how it can be used to get a minimum distance bound for G-invariant codes is outlined. Karlin [64] showed a way to decode a class of one-generator quasi-cyclic codes. Heijnen and van Tilborg [65] proposed another decoding technique for the class of one-generator quasi-cyclic codes, which uses the same basic idea but achieves some computational advantages by better usage of the quasi-cyclic property of the code. Karlin's approach is extended to a class of quasi-cyclic codes, not necessarily one-generator. When restricted to one-generator quasi-cyclic codes, this method reduces to Karlin's method. Moreover, our method also applies to a class of quasi-abelian codes specified in subsection 4.8.1. Chapter 5 extends the results of Chapter 4 to codes over Galois rings and Blackford and Ray-Chaudhury's transform technique to [27] permutation groups of cyclic codes over Galois rings is extended to permutation groups of abelian codes over Galois rings.

The conditions for extended cyclic codes over integer residue rings to be affine-invariant were derived by Abdukhalikov [34]. Blackford and Ray-Chaudhuri [27] used transform domain approach to characterize affine invariant extended cyclic codes of length 2^m over subrings of $GR(4, m)$ and using this characterization, they found new classes of affine invariant codes over Galois rings from BCH codes. In chapter 6, their approach is extended to cyclic codes of length 2^m over any subring of $GR(2^e, m)$ for $m \geq e-1$ and also to extended cyclic codes of length p^m over $GR(p^2, m)$ (where $m \geq 1$) for arbitrary prime p. Classes of affine invariant BCH codes and GRM codes over $\mathbb{Z}_{2^e}$ and over $\mathbb{Z}_{p^2}$ are found using these conditions.

Chapter 7 concludes the thesis with some possible further directions of research.

Chapter 2

F_q-Linear Cyclic Codes over F_{q^m}

2.1 Introduction

A linear code over F_{q^m}, (q is a power of a prime p) is closed under addition, and multiplication with elements from F_{q^m}. In this chapter, the class of nonlinear codes over F_{q^m} that are closed under addition, and multiplication with elements from F_q is considered and are called F_q-linear codes. Such codes have found practical applications in deep-space communication [2] and computer memory systems [66–70]. Among the F_q-linear codes, we restrict ourselves to cyclic codes. This class of codes are referred as F_q-linear cyclic codes. Henceforth F_q-linear codes over F_{q^m} and F_q-linear cyclic codes over F_{q^m} will be written as F_qL and F_qLC codes. The class of F_qLC codes includes the following classes of codes as special cases:

1. **Group cyclic codes over elementary abelian groups:** When $q = p$ the class of F_pLC codes coincides with the class of group cyclic codes defined over an elementary abelian group C_p^m (a direct product of m cyclic groups of order p). A length n group code over a group G is a subgroup of G^n under component-wise operation. Group codes constitute an important ingredient in the construction of geometrically uniform codes [71]. Hamming distance properties of group codes over abelian groups are closely connected to the Hamming distance properties of codes over subgroups that are elementary abelian [72]. Group cyclic codes over C_p^m constructed using nonsingular circulant matrices over F_{p^m} have been studied and applied to block coded modulation schemes with phase shift keying [73]. It is known [74, 75] that the class of group cyclic codes over C_p^m contains MDS codes that are not linear over

F_{p^m}.

2. **SSRS codes:** Given a Reed-Solomon code of length $n = q^m - 1$ over F_{q^m}, the subcode obtained by taking all the codewords with components from an F_q-subspace of F_{q^m} is called a subspace subcode of the Reed-Solomon (SSRS) code. These codes are also F_qLC codes and were discussed by Hattori, McEliece and Solomon in [2]. The authors derived dimension formula for this class of codes and codes with larger number of codewords than any previously known code with the same length and minimum distance have been reported. The class of SSRS codes is a subclass of subgroup subcodes, discussed in [76].

3. **Linear cyclic codes over finite fields:** Obviously, with $m = 1$, the class of F_qLC codes coincides with the extensively studied class of linear cyclic codes over finite fields [38, 77].

4. **Twisted BCH codes:** Consider a code obtained by taking the coordinate-wise image of a BCH code over F_{q^r} under an F_q-linear map $\phi : F_{q^r} \longrightarrow F_q^m$ for some $m \leq r$. Twisted BCH codes, constructed as F_q dual (see Section 4) of such codes, were introduced in [1] and is a subclass of F_qLC codes. Large number of good codes were constructed in [1, 78, 79] as twisted BCH codes and as combinations of twisted BCH codes with other codes.

A code is m-quasi-cyclic (m-QC) if the cyclic shift of components of every codeword by m positions gives another codeword [20]. Structural properties of quasi-cyclic codes were investigated in [5–7]. There is a 1-1 correspondence between the class of F_qLC codes of length n over F_{q^m} and the class of m-QC codes of length mn over F_q. If $\{\beta_0, \beta_1, \cdots, \beta_{m-1}\}$ is an F_q-basis of F_{q^m}, then any vector $(a_0, a_1, \cdots, a_{n-1}) \in F_{q^m}^n$ can be seen with respect to this basis as $(a_{0,0}, a_{0,1}, \cdots, a_{0,m-1}, \cdots, a_{n-1,0}, a_{n-1,1}, \cdots, a_{n-1,m-1}) \in F_q^{mn}$, where $a_i = \sum_{j=0}^{m-1} a_{i,j}\beta_j$. When seen this way, any F_qLC code of length n over F_{q^m} corresponds to an m-QC code of length nm over F_q.

In this chapter,

- the DFT domain characterization of F_qLC codes over F_{q^m} is obtained.
- transform domain condition for two vectors to be F_q-dual of each other is given. This is used to prove nonexistence of certain self dual F_qLC codes and equivalently

nonexistence of the corresponding self dual QC codes. These results for self dual QC codes are also available in [8] and also follows from the results in Chapter 4.

- the transform domain characterization of F_qLC codes is used to derive minimum distance bound for the corresponding QC codes.

The content of this chapter is organized as follows : In Section 2.2, some new terminologies are introduced and linear cyclic codes over a finite field are described in DFT domain using these terminologies. In Section 2.3, the main result of this chapter, i.e., the DFT domain description of F_qLC codes is given. The characterization is in terms of any decomposition of the code into subcodes, for which each nonzero transform component's values are from certain minimal invariant subspaces of the extension field. In Section 2.4, transform domain condition for two vectors to be F_q-dual of each other w. r. t. a self dual basis of F_{q^m} is derived and used to prove the nonexistence of self dual F_qLC codes and self dual QC codes of certain parameters. In Section 2.5, it is shown how one can obtain a set of parity check equations over an extension field for the corresponding QC code and thus can get a bound on it's minimum distance using an approach similar to Tanner's [80]. Several directions for further research and concluding remarks constitute Section 2.6.

2.2 Preliminaries

q-cyclotomic coset modulo n was defined in Section 1.1. In this chapter, q^m-cyclotomic cosets modulo n are also needed which are defined in the similar way.

Clearly, a q-cyclotomic coset modulo $\frac{n}{m}$ is union of some q-cyclotomic cosets modulo n. If $J \subseteq [0, n-1]$, it's cyclotomic cosets are defined as $[J]_n = \cup_{j\in J}[j]_n$ and $[J]_{\frac{n}{m}} = \cup_{j\in J}[j]_{\frac{n}{m}}$

In the following, for a subset $I = \{i_1, i_2, \cdots, i_k\} \subseteq I_n$, $(A_i)_{i\in I}$ denotes the ordered tuple $(A_{i_1}, A_{i_2}, \cdots, A_{i_k})$ where an arbitrary fixed order in I is assumed. For some ordered tuples $T_1 = (t_{11}, \cdots, t_{1,j_1}), \cdots, T_l = (t_{l,1}, \cdots, t_{l,j_l})$ the concatenated tuple $(t_{11}, \cdots, t_{1,j_1}, \cdots, t_{l,1}, \cdots, t_{l,j_l})$ is denoted as $(T_1, \cdots, T_l)$.

Definition 1. Let $I_1, I_2, \cdots, I_l$ be some disjoint subsets of I_n and suppose $R_{I_j} = \{(A_i)_{i\in I_j} | \mathbf{a} \in \mathcal{C}\}$ for $j = 1, 2, \cdots, l$. The sets of transform components $\{A_i | i \in I_j\}$; $1 \leq j \leq l$ are called

unrelated for $\mathcal{C}$ if $\left\{\left((A_i)_{i\in I_1}, (A_i)_{i\in I_2}, \cdots, (A_i)_{i\in I_l}\right) | \mathbf{a} \in \mathcal{C}\right\} = R_{I_1} \times R_{I_2} \times \cdots \times R_{I_l}$. They are called **related** if they are not unrelated.

Now, the extensively studied linear cyclic codes over F_{q^m} can be characterized as follows:

- A cyclic code is the set of inverse DFT vectors of all the vectors of an F_{q^m}-subspace of $DFT(F_{q^m}^n) \subset F_{q^{mr}}^n$, in which transform components in $[j]_n^{q^m}$, $j \in I_n$, take either only the zero value or all the values of $F_{q^{mr_j}}$, and transform components in disjoint $[J_1]_n^{q^m}$ and $[J_2]_n^{q^m}$ are unrelated.

From the above characterization, it is clear that to specify a cyclic code, it is sufficient to specify the set $[J]_n^{q^m}$ in which the transform components of all the codewords is zero. It is important to note that the transform components A_j and A_k are not related by the conjugacy constraint of the DFT unless $[j]_n^{q^m} = [k]_n^{q^m}$. One of the results of this chapter is that in an F_qLC code, transform components take values from appropriate invariant subspaces (introduced in the following subsection). Moreover, the transform components from different q^m-cyclotomic cosets within a q-cyclotomic coset modulo n can be related for F_qLC codes by appropriate F_q-homomorphism (discussed in the next section) and all F_qLC codes are describable in terms of these relations along with the appropriate invariant subspaces.

2.2.1 Invariant subspaces of F_{q^l}

In this subsection the notion of invariant subspaces required for the characterization of F_qLC codes in transform domain is introduced. For any element s in a finite field F_{q^l}, the set $[s]^q = \{s, s^q, s^{q^2}, \cdots, s^{q^{e-1}}\}$, where e is the smallest positive integer such that $s^{q^e} = s$, is called the q-conjugacy class of s. Note that, if $\alpha \in F_{q^l}$ is of order n and $s = \alpha^j$, then there is a 1-1 correspondence between $[j]_n^q$ and $[s]^q$, namely $jq^t \mapsto s^{q^t}$. So, $|[s]^q| = |[j]_n^q| = e_j$.

Definition 2. For any element $s \in F_{q^l}$, a subset U of F_{q^l} is called **s-invariant** if $sU = U$. In addition, if U is an F_q-subspace, then it is called an **s-invariant F_q- subspace**. For brevity, "$[s,q]$-subspace" will be written instead of "s-invariant F_q-subspace". An $[s,q]$-subspace of F_{q^l} is called minimal if it contains no proper $[s,q]$-subspace.

If U and V are two $[s,q]$-subspaces of F_{q^l}, then so are $U \cap V$ and $U+V$. If s and s' are in the same q-conjugacy class, then $s' = s^{q^i}$ and $s = (s')^{q^j}$ for some i and j. So, $[s,q]$-subspaces and $[s',q]$-subspaces are the same.

Example 2.2.1. Consider $q = 2$, $m = 2$, $n = 15$ and $r = 2$. Let α be a primitive element of F_{16}. Since $[\alpha^5]^2 = [\alpha^{10}]^2$, we have $[\alpha^5, 2]$-subspaces to be the same as $[\alpha^{10}, 2]$-subspaces. The minimal $[\alpha^5, 2]$ subspaces of F_{2^4} are $V_1 = \{0, 1, \alpha^5, \alpha^{10}\}$, $V_2 = \{0, \alpha, \alpha^6, \alpha^{11}\}$, $V_3 = \{0, \alpha^2, \alpha^7, \alpha^{12}\}$, $V_4 = \{0, \alpha^3, \alpha^8, \alpha^{13}\}$, and $V_5 = \{0, \alpha^4, \alpha^9, \alpha^{14}\}$. These are also minimal $[\alpha^{10}, 4]$-subspaces. The $[\alpha^k, 2]$-subspaces, for $k \neq 0, 5, 10$ are $\{0\}$ and F_{16}. Every subset consisting of two elements $\{0, x\}; x \in F_{16}^*$ is a minimal $[\alpha^0, 2]$-subspace and none of these is an $[\alpha^0, 4]$-subspace. Observe that $\{1, \alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ is an α^3-invariant subset and not an $[\alpha^3, 2]$-subspace. The corresponding $[\alpha^3, 2]$-subspace, obtained as F_2-span of the set is F_{16}.

One can also talk about $[s, q^\lambda]$-subspaces of F_{q^l} when $\lambda | l$. The $[s, q^\lambda]$-subspaces are useful when one considers F_{q^λ}-linear codes over F_{q^m}. However, in such cases one can take q^λ to be q' and treat them as $F_{q'}$-linear codes over $F_{q'^{\frac{m}{\lambda}}}$. So, we'll be concerned with only $[s,q]$-subspaces throughout the chapter.

Let s be an element of order t in F_{q^l}. Then, it is well known that $Span_{F_q}\{s^i | i = 0, 1, \cdots, t-1\} \simeq F_{q^e}$, where e is the exponent of $[s]^q$. So, $[s,q]$-subspaces are nothing but the F_{q^e}-subspaces of F_{q^l} and the minimal $[s,q]$-subspaces are the one dimensional F_{q^e}-subspaces of F_{q^l}.

2.3 Transform Domain Characterization of $FqLC$ Codes

Throughout, length n codes over F_{q^m} are considered, where n and q are relatively prime and α will denote the n^{th} root of unity, used as the DFT kernel.

From the cyclic shift property it follows that in an F_qLC code $\mathcal{C}$, the set of j^{th} transform components constitutes an $[\alpha^j, q]$-subspace of $F_{q^{mr}}$. However, a code need not be an F_qLC code even if each DFT component A_j takes values from an $[\alpha^j, q]$-subspace.

Example 2.3.1. Consider length 15, F_2L codes over $F_{16} = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{14}\}$. We have $q = 2, m = 4$ and $r = 1$. In Table 2.1, the code $\mathcal{C}_3$ is not cyclic, though each transform component takes values from appropriate invariant subspaces. Other five codes in the same table are F_2LC codes. We have chosen α with the minimal polynomial X^2+X+1.

Table 2.1: Few Length 15 F_2-Linear Codes over F_{16}
[Only nonzero transform components are shown. The nonzero elements of F_{16} are represented by the corresponding power of the primitive element and 0 is represented by -1.]

	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	A_5	A_{10}
	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
$\mathcal{C}_0$	0	2	8	0	2	8	0	2	8	0	2	8	0	2	8	1	4
	8	0	2	8	0	2	8	0	2	8	0	2	8	0	2	6	14
	2	8	0	2	8	0	2	8	0	2	8	0	2	8	0	11	9
	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
$\mathcal{C}_1$	4	9	14	4	9	14	4	9	14	4	9	14	4	9	14	-1	4
	14	4	9	14	4	9	14	4	9	14	4	9	14	4	9	-1	14
	9	14	4	9	14	4	9	14	4	9	14	4	9	14	4	-1	9
	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
	4	9	14	4	9	14	4	9	14	4	9	14	4	9	14	-1	4
	14	4	9	14	4	9	14	4	9	14	4	9	14	4	9	-1	14
	9	14	4	9	14	4	9	14	4	9	14	4	9	14	4	-1	9
	0	2	8	0	2	8	0	2	8	0	2	8	0	2	8	1	4
$\mathcal{C}_4$	1	11	6	1	11	6	1	11	6	1	11	6	1	11	6	1	-1
=	3	10	12	3	10	12	3	10	12	3	10	12	3	10	12	1	9
$\mathcal{C}_0$	7	13	5	7	13	5	7	13	5	7	13	5	7	13	5	1	14
+	8	0	2	8	0	2	8	0	2	8	0	2	8	0	2	6	14
$\mathcal{C}_1$	5	7	13	5	7	13	5	7	13	5	7	13	5	7	13	6	9
	6	1	11	6	1	11	6	1	11	6	1	11	6	1	11	6	-1
	12	3	10	12	3	10	12	3	10	12	3	10	12	3	10	6	4
	2	8	0	2	8	0	2	8	0	2	8	0	2	8	0	11	9
	10	12	3	10	12	3	10	12	3	10	12	3	10	12	3	11	14
	13	5	7	13	5	7	13	5	7	13	5	7	13	5	7	11	4
	11	6	1	11	6	1	11	6	1	11	6	1	11	6	1	11	-1
	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
$\mathcal{C}_6$	0	10	5	0	10	5	0	10	5	0	10	5	0	10	5	0	-1
	5	0	10	5	0	10	5	0	10	5	0	10	5	0	10	5	-1
	10	5	0	10	5	0	10	5	0	10	5	0	10	5	0	10	-1

	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	A_5	A_{10}
	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
$\mathcal{C}_2$	4	3	7	4	3	7	4	3	7	4	3	7	4	3	7	1	0
	7	4	3	7	4	3	7	4	3	7	4	3	7	4	3	6	10
	3	7	4	3	7	4	3	7	4	3	7	4	3	7	4	11	5
	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
$\mathcal{C}_3$	0	2	8	0	2	8	0	2	8	0	2	8	0	2	8	1	4
	5	7	13	5	7	13	5	7	13	5	7	13	5	7	13	6	9
	10	12	3	10	12	3	10	12	3	10	12	3	10	12	3	11	14
	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
	4	3	7	4	3	7	4	3	7	4	3	7	4	3	7	1	0
	7	4	3	7	4	3	7	4	3	7	4	3	7	4	3	6	10
	3	7	4	3	7	4	3	7	4	3	7	4	3	7	4	11	5
	0	2	8	0	2	8	0	2	8	0	2	8	0	2	8	1	4
$\mathcal{C}_5$	1	6	11	1	6	11	1	6	11	1	6	11	1	6	11	-1	1
=	9	10	13	9	10	13	9	10	13	9	10	13	9	10	13	11	2
$\mathcal{C}_0$	14	12	5	14	12	5	14	12	5	14	12	5	14	12	5	6	8
+	8	0	2	8	0	2	8	0	2	8	0	2	8	0	2	6	14
$\mathcal{C}_2$	5	14	12	5	14	12	5	14	12	5	14	12	5	14	12	11	3
	11	1	6	11	1	6	11	1	6	11	1	6	11	1	6	-1	11
	13	9	10	13	9	10	13	9	10	13	9	10	13	9	10	1	12
	2	8	0	2	8	0	2	8	0	2	8	0	2	8	0	11	9
	10	13	9	10	13	9	10	13	9	10	13	9	10	13	9	6	7
	12	5	14	12	5	14	12	5	14	12	5	14	12	5	14	1	13
	6	11	1	6	11	1	6	11	1	6	11	1	6	11	1	-1	6

The code $\mathcal{C}_3$ in Table 2.1 is not cyclic, since A_5 and A_{10} are related by an isomorphism which does not *correspond to cyclicity* in the time-domain. In the rest of this section all the possible relations that correspond to cyclicity in the time domain are identified, leading to a characterization of F_qLC codes in the transform domain. The characterization is in terms of the component codes of a decomposition of the code under consideration. In the following subsection, the decomposition of F_qLC codes is discussed.

2.3.1 Decomposition of F_qLC Codes

Suppose A_j takes values from $V \subset F_{q^{mr}}$, $V \neq \{0\}$ for an F_qL code $\mathcal{C}$. Let V_1 be an F_q-subspace of $F_{q^{mr}}$. Let us call $\mathcal{C}' = \{\mathbf{a} | \mathbf{a} \in \mathcal{C}, A_j \in V_1\}$ as the F_qL subcode obtained by restricting A_j in V_1. For example, the subcode $\mathcal{C}_1$ of Table 2.1 can be obtained from $\mathcal{C}_4$ by restricting A_5 to $\{0\}$. If $\mathcal{C}''$ is a complement of $\mathcal{C}'$ in $\mathcal{C}$ and A_j takes values from V_2 in $\mathcal{C}''$, then V_2 is a complement of $V \bigcap V_1$ in V. Clearly, if $\mathcal{C}$ is cyclic and V_1 is an $[\alpha^j, q]$-subspace, then $\mathcal{C}'$ is also cyclic. If $S \subseteq I_n$, then the subcode obtained by restricting the transform components A_j; $j \notin S$ to 0 will be called the S-subcode of $\mathcal{C}$ and will be denoted as $\mathcal{C}_S$.

Lemma 2.3.1. *Suppose in an F_qL code $\mathcal{C}$, A_j takes values from a subspace $V \subseteq F_{q^{mr}}$. Let $V_1, V_2 \subseteq V$ be two subspaces of V such that $V = V_1 + V_2$. (i) If $\mathcal{C}_1$ and $\mathcal{C}_2$ are the subcodes of $\mathcal{C}$, obtained by restricting A_j in V_1 and V_2 respectively, then $\mathcal{C} = \mathcal{C}_1 + \mathcal{C}_2$. (ii) If V_1 and V_2 are $[\alpha^j, q]$-subspaces, then $\mathcal{C}$ is cyclic if and only if $\mathcal{C}_1$ and $\mathcal{C}_2$ are cyclic.*

Proof: Let us prove (i), then (ii) is obvious. It is sufficient to show that $\mathcal{C} \subset \mathcal{C}_1 + \mathcal{C}_2$. Consider a codeword $c_3 \in \mathcal{C}$. Suppose $A_j = v_3 \in V$ for c_3. Since $V = V_1 + V_2$, $\exists v_1 \in V_1$ and $v_2 \in V_2$ such that $v_3 = v_1 + v_2$. Let $c_1 \in \mathcal{C}_1$ such that $A_j = v_1$ for c_1. Now, for the codeword $c_2 = c_3 - c_1$, $A_j = v_3 - v_1 = v_2 \in V_2$. So, $c_2 \in \mathcal{C}_2$ and thus $c_3 = c_1 + c_2 \in \mathcal{C}_1 + \mathcal{C}_2$. ■

Notice that $\mathcal{C}_2$ need not be a complement of $\mathcal{C}_1$ in $\mathcal{C}$ even if V_2 is a complement of V_1 since the intersection of $\mathcal{C}_1$ and $\mathcal{C}_2$ in that case is precisely the subcode obtained from $\mathcal{C}$ by restricting A_j to $\{0\}$.

Suppose in an F_qL code $\mathcal{C}$, a nonzero transform component A_j takes values from a nonzero F_q-subspace V of $F_{q^{mr}}$, and V intersects with more than one minimal $[\alpha^j, q]$-subspaces. Then, we have $t > 1$ minimal $[\alpha^j, q]$-subspaces $V_1, V_2, \cdots, V_t$ such that $V \subseteq \oplus_{i=1}^{t} V_i$ and $V \cap V_i \neq \phi$ for $i = 1, 2, \cdots, t$. Then, we can decompose the code as the sum of t smaller codes $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_t$ obtained by restricting A_j to $V_1, V_2, \cdots, V_t$, i.e., $\mathcal{C} = \mathcal{C}_1 + \mathcal{C}_2 + \cdots + \mathcal{C}_t$. So by successively doing this for each j, $\mathcal{C}$ can be decomposed into a set of subcodes, in each of which, for any $j \in I_n$, transform component A_j takes values from an F_q-subspace of a minimal $[\alpha^j, q]$-subspaces. In particular, if the original code was an F_qLC code, each of the subcodes obtained this way will have A_j from a minimal $[\alpha^j, q]$-subspaces or zero. The following are immediate consequences of this observation and Lemma 2.3.1.

1. In a minimal F_qLC code, any nonzero transform component A_j takes values from a minimal $[\alpha^j, q]$-subspace of $F_{q^{mr}}$. For example, the codes $\mathcal{C}_1$ and $\mathcal{C}_2$ in Table 2.1 are minimal F_2LC codes and the nonzero transform components A_5 and A_{10} take values from minimal $[\alpha^5, 2]$-subspaces.

2. A code is F_qLC if and only if all the subcodes obtained by restricting any nonzero

transform component A_j in minimal $[\alpha^j, q]$-subspace of $F_{q^{mr}}$ are F_qLC. The statement is also true without the word 'minimal'.

Codes with Spectral Base

Definition 3. Suppose in an F_qL code $\mathcal{C}$, transform components $A_j,\ j \in I_n$ take values from F_q-subspaces V_j of $F_{q^{mr}}$. A set of transform components $\{A_l | l \in L \subseteq I_n\}$ is called a **spectral base** if they are nonzero and unrelated for $\mathcal{C}$ and any other transform component $A_k,\ k \notin L$ can be expressed as $A_k = \sum_{l \in L} \sigma_{kl} A_l$ such that σ_{kl} is an F_q-homomorphism of V_l into V_k.

A code may not have a spectral base, since though we can always find a maximal subset of transform components which are unrelated, values of other components may not be determined by the values of those transform components. As example, consider the code $\mathcal{C} = \mathcal{C}_5 + \mathcal{C}_6$ where $\mathcal{C}_5$ and $\mathcal{C}_6$ are from Table 2.1. Clearly, $\mathcal{C}_5$ and $\mathcal{C}_6$ have F_2-dimensions 4 and 2 respectively and $\mathcal{C}$ has dimension 6. In $\mathcal{C}$, both A_5 and A_{10} take values from F_{16}. So, $\{A_5, A_{10}\}$ is not a spectral base for $\mathcal{C}$ and neither of A_5 or A_{10} alone constitutes a spectral base. So, This code does not have a spectral base.

If a code has a spectral base, then it will be called a **code with spectral base**.

If some sets of transform components are unrelated in two codes $\mathcal{C}'$ and $\mathcal{C}''$, then it is unrelated in the code $\mathcal{C}' + \mathcal{C}''$. However, the converse is not true. For instance, consider the two F_2LC codes $\mathcal{C}_0$ and $\mathcal{C}_1$ and their sum $\mathcal{C}_4$ shown in Table 2.1. Clearly in $\mathcal{C}_0$ and $\mathcal{C}_1$, A_5 and A_{10} are related. But they are unrelated in $\mathcal{C}_4$.

Theorem 2.3.2. *If $\mathcal{C}$ is an F_qLC code over F_{q^m} where any nonzero transform component A_j takes values from a minimal $[\alpha^j, q]$-subspace V_j of $F_{q^{mr}}$, then there is a spectral base $\{A_l | l \in L \subseteq I_n\}$ for $\mathcal{C}$*

Proof: L is constructed iteratively as follows. First assign $L = \phi$, $L_1 = \{j \in I_n | A_j = 0 \text{ in } \mathcal{C}\}$ and do the following repeatedly until $L \cup L_1 = I_n$.

- Take any $j \in I_n \setminus (L \cup L_1)$. Consider the subcode $\mathcal{C}_1$ of $\mathcal{C}$ obtained by restricting $\{A_l | l \in L\}$ to zero. Clearly, in that subcode $\mathcal{C}_1$, either $A_j = 0$ or A_j takes values from V_j. If $A_j = 0$ in $\mathcal{C}_1$, then in $\mathcal{C}$, A_j can be expressed as $A_j = \sum_{l \in L} \sigma_l A_l$ for some

F_q-homomorphisms $\sigma_l : V_l \longmapsto V_j$ and thus put j in L'. Otherwise, $\{A_l | l \in L \cup \{j\}\}$ is a set of unrelated components in $\mathcal{C}$. So, put j in L.

Clearly, after all the iterations are over, the set L will be the indexes of a spectral base. Observe that the spectral base is not unique. ∎

Clearly, for a code $\mathcal{C}$ as described in Theorem 2.3.2, if $l \in L$, the subcode $\mathcal{C}_l$ obtained by restricting all the transform components $\{A_j | j \in L, j \neq l\}$ to zero is a minimal F_qLC code. Moreover, $\mathcal{C}$ can be decomposed as $\mathcal{C} = \oplus_{l\in L}\mathcal{C}_l$. We have already seen that, any code can be decomposed as a sum of subcodes with nonzero transform components taking values from minimal invariant subspaces. Each of those subcodes can now be further decomposed as direct sum of minimal subcodes. So we have,

Theorem 2.3.3. *Any F_qLC code of length n, $(n,p) = 1$ over F_{q^m} can be decomposed as direct sum of minimal F_qLC codes.*

This theorem implies that, any m-QC code of length nm over F_q can be decomposed as direct sum of minimal m-QC codes, if $(n,q) = 1$. This was first proved in [5].

2.3.2 Linearized Polynomials and Induced Maps

Unlike linear cyclic codes, transform components in different q^m-cyclotomic cosets may be related in an F_qLC code as will be shown in next subsection. In particular, transform components may be related by F_q-homomorphisms. But two transform components can not be related by some arbitrary homomorphism. The allowed homomorphisms will be characterized in the next subsection in terms of linearized polynomials. In this subsection, linearized polynomials and their induced maps are discussed as a preparation to the next subsection.

Definition 4. [81] A polynomial of the form $f(X) = \sum_{i=0}^{t} c_i X^{q^i} \in F_{q^l}[X]$ is called a q-polynomial or a linearized polynomial over F_{q^l}.

Each q-polynomial of degree less than q^l induces a distinct F_q-linear map of F_{q^l}. So, considering the identical cardinalities, we have

$$End_{F_q}(F_{q^l}) \;=\; \{\sigma_f : x \mapsto f(x) | f(X) = \sum_{i=0}^{l-1} c_i X^{q^i} \in F_{q^l}[X]\}. \tag{2.1}$$

For any $y \in F_{q^l} \setminus \{0\}$, the map $x \mapsto yx$ induced by the polynomial $f(X) = yX$ is an F_q-automorphism of F_{q^l} and will be denoted from now onwards by σ_y. The subset $\{\sigma_y | y \in F_{q^l} \setminus \{0\}\}$ forms a cyclic subgroup of $Aut_{F_q}(F_{q^l})$, generated by $\sigma_{\beta_{q^l}}$, where $\beta_{q^l} \in F_{q^l}$ is a primitive element of F_{q^l}. In this subgroup, $\sigma_y^i = \sigma_{y^i}$. This subgroup will be denoted as $S_{q,l}$ and $S_{q,l} \cup \{0\}$ as $\mathbf{S}_{q,l}$, where 0 denotes the zero map. Clearly, $\mathbf{S}_{q,l}$ forms a field isomorphic to F_{q^l}.

The map $\sigma_{X^q} : y \mapsto y^q$ of F_{q^l} onto F_{q^l}, induced by the polynomial $f(X) = X^q$ will be denoted as $\theta_{q,l}$. Clearly, $\theta_{q,l}\sigma_x = \sigma_x^q \theta_{q,l}$ i.e., $\theta_{q,l}\sigma_x\theta_{q,l}^{-1} = \sigma_x^q$ for all $x \in F_{q^l}$. The map induced by the polynomial $f(X) = X^{q^i}$ is $\theta_{q,l}^i$. So, for any $f(X) = \sum_{i=0}^{l-1} c_i X^{q^i}$, $\sigma_f = \sum_{i=0}^{l-1} \sigma_{c_i}\theta_{q,l}^i$. So we have

$$End_{F_q}(F_{q^l}) \quad = \quad \oplus_{i=0}^{l-1} \mathbf{S}_{q,l}\theta_{q,l}^i. \tag{2.2}$$

That is, any endomorphism $\sigma \in End_{F_q}(F_{q^l})$ can be decomposed uniquely as $\sigma = \sum_{i=0}^{l-1} \sigma_{(i)}$ where $\sigma_{(i)} \in \mathbf{S}_{q,l}\theta_{q,l}^i$. This decomposition will be called as canonical decomposition of σ.

2.3.3 Transform Domain Characterization

The following theorem gives the basic condition that a homomorphism should satisfy to qualify for a possible relating homomorphism.

Theorem 2.3.4. *Suppose, in an F_qLC code, A_j and A_k take values from the $[\alpha^j, q]$-subspace V_1 and $[\alpha^k, q]$-subspace V_2 respectively. Suppose A_k is related to A_j by an F_q homomorphism $\sigma : V_1 \mapsto V_2$ i.e. $A_k = \sigma(A_j)$. Then σ satisfies*

$$\sigma(\alpha^j v) = \alpha^k \sigma(v) \qquad \forall \quad v \in V_1. \tag{2.3}$$

Proof: Consider any $v \in V_1$. There is a codeword with transform pair $(A_k, A_j) = (\sigma(v), v)$. Since the code is cyclic, the cyclic shift of this vector with transform pair $(A_k, A_j) = (\alpha^k\sigma(v), \alpha^j v)$ is also a codeword. But, since $A_k = \sigma(A_j)$ holds for any codeword, $\alpha^k\sigma(v) = \sigma(\alpha^j v)$. ■

Clearly, kernel of such a homomorphism is an $[\alpha^j, q]$ subspace. However, for an F_qLC code, two related transform components may not be related by a homomorphism. But when each nonzero transform component A_j takes values from a minimal $[\alpha^j, q]$-subspace, then relations are by isomorphisms. To see that, let $\mathcal{C}$ be such an F_qLC code where each nonzero transform component A_j takes values from a minimal $[\alpha^j, q]$-subspace V_j of $F_{q^{mr}}$ and let $\{A_l | l \in L \subseteq I_n\}$ for $\mathcal{C}$ be a spectral base of $\mathcal{C}$. For any $k \notin L$, $A_k = \sum_{j \in L} \sigma_{kj} A_j$, where σ_{kj} is an F_q-homomorphism of V_j into V_k satisfying

$$\sigma_{kj}(\alpha^j v) \;=\; \alpha^k \sigma_{kj}(v) \;\; \forall v \in V_j. \tag{2.4}$$

Without loss of generality, we can assume that, $A_{[k]_n^{q^m}}$ and $A_{[j]_n^{q^m}}$ are the only nonzero components in the code. Now, consider the cyclic subcode $\mathcal{C}_1$ obtained by restricting $A_k = 0$ in $\mathcal{C}$. In $\mathcal{C}_1$, A_j takes values from $V_3 = Ker\{\sigma_{kj}\}$, an α^j -invariant subspace. V_3 can not be same as V_j since then $V_k = Im\,(\sigma_{kj}) = \{0\}$. So, $V_3 = \{0\}$ and thus σ_{kj} is an isomorphism.

In what follows, a sequence of results is presented in terms of lemmas and theorems which leads to the transform domain characterization (Theorem 2.3.11).

Lemma 2.3.5. *Suppose $x_1, x_2 \in F_{q^l}$. Then, $[x_1]^q = [x_2]^q$ if and only if there exists $\sigma \in Aut_{F_q}(F_{q^l})$ such that $\sigma(x_1 x) = x_2 \sigma(x)$ $\forall x \in F_{q^l}$.*

Proof: ($\Rightarrow$): $[x_1]^q = [x_2]^q \Leftrightarrow x_2 \in [x_1]^q \Leftrightarrow \exists i$ s. t. $x_2 = x_1^{q^i}$. Now, clearly $\sigma = \theta_{q,l}^i \in Aut_{F_q}(F_{q^l})$ satisfies the condition $\sigma(x_1 x) = x_2 \sigma(x)$ $\forall x \in F_{q^l}$.

($\Leftarrow$): The given condition is equivalent to $\sigma\sigma_{x_1} = \sigma_{x_2}\sigma$. Let $\sigma = \sum_{i=0}^{l-1} \sigma_{(i)}$ be the canonical decomposition of σ. Then,

$$\begin{aligned}
& \sum_{i=0}^{l-1} \sigma_{(i)}\sigma_{x_1} = \sum_{i=0}^{l-1} \sigma_{x_2}\sigma_{(i)} \\
\Rightarrow \;\; & \sigma_{(i)}\sigma_{x_1} = \sigma_{x_2}\sigma_{(i)} \quad \text{for} \quad 0 \le i \le l-1 \\
\Rightarrow \;\; & \sigma_{x_1^{q^i}}\sigma_{(i)} = \sigma_{x_2}\sigma_{(i)} \quad \text{for} \quad 0 \le i \le l-1 \\
\Rightarrow \;\; & x_1^{q^i} = x_2 \;\text{ or }\; \sigma_{(i)} = \mathbf{0} \quad \text{for} \quad 0 \le i \le l-1.
\end{aligned}$$

At least for one i, $\sigma_{(i)} \neq \mathbf{0}$ since $\sigma \neq \mathbf{0}$ and thus x_2 is in the q-conjugacy class of x_1. ∎

Lemma 2.3.6. *Let $V_1 \subseteq F_{q^l}$ be a minimal $[x_1, q]$-subspace and $\sigma : V_1 \longrightarrow F_{q^l}$ be a nonzero homomorphism satisfying*

$$\sigma(x_1 v) = x_2 \sigma(v) \quad \forall \;\; v \in V_1. \tag{2.5}$$

Then $[x_1]^q = [x_2]^q$.

Proof: Since $Ker(\sigma) \subseteq V_1$ is an $[x_1, q]$ subspace, V_1 is a minimal $[x_1, q]$-subspace and σ is nonzero, $Ker(\sigma) = \{0\}$. Let $Im(\sigma) = V_2$. Then, σ is an isomorphism of V_1 onto V_2 satisfying

$$\sigma(x_1 v) = x_2 \sigma(v) \quad \forall \;\; v \in V_1. \tag{2.6}$$

V_2 is an x_2-invariant subspace, since for any $v = \sigma(v_1) \in V_2$, $x_2 v = x_2\sigma(v_1) = \sigma(x_1 v_1) \in V_2$. Clearly, σ^{-1} satisfies

$$\sigma^{-1}(x_2 v) = x_1 \sigma^{-1}(v) \quad \forall \;\; v \in V_2. \tag{2.7}$$

If V_2 is not a minimal x_2-invariant subspace, then it can be decomposed as direct sum of some minimal x_2-invariant subspaces and restriction of σ^{-1} to at least one of the minimal x_2-invariant subspaces (say V_3) is nonzero. Then $\sigma^{-1}(V_3) \neq V_1$ is a proper x_1-invariant subspace of V_1: contradiction to minimality of V_1. So, V_2 is a minimal x_2 - invariant subspace. So, the size of the minimal x_1 - invariant subspaces and minimal x_2 - invariant subspaces are same i.e., $e_{x_1} = |[x_1]^q| = |[x_2]^q|$ and x_1-invariant subspaces and x_2 - invariant subspaces are same. Suppose $V_2 = y_1 F_{q^{e_{x_1}}}$ and $V_1 = y_2 F_{q^{e_{x_1}}}$. Then, define the map $\sigma_1 : F_{q^{e_{x_1}}} \longrightarrow F_{q^{e_{x_1}}}$ by $y \mapsto y_1^{-1}\sigma(y_2 y)$. Clearly, σ_1 is an F_q-automorphism and it satisfies $\sigma_1(x_1 v) = x_2 \sigma_1(v) \quad \forall \;\; v \in F_{q^{e_{x_1}}}$. So, by Lemma 2.3.5, $[x_1]^q = [x_2]^q$. ■

The fact that, the codes under consideration are F_qLC, does not allow any arbitrary sets of transform components to be related. The following theorem tells which components can be related in an F_qLC codes.

Theorem 2.3.7. *In an F_qLC code, the transform components of different q-cyclotomic cosets are unrelated.*

Proof: By Theorem 2.3.3, it is sufficient to show that the statement is true for minimal F_qLC codes. Suppose in one such subcode, A_j and A_k are related as $A_j = \sigma_{kj} A_k$ where σ_{lj} is nonzero and it satisfies eqn. (2.4). So, by Lemma 2.3.6, $[\alpha^j]^q = [\alpha^k]^q \Rightarrow [j]_n^q = [k]_n^q$. That is, j and k are in the same q-cyclotomic coset modulo n. ■

Corollary 2.3.8. *(i) Any minimal F_qLC code has nonzero transform components only in one q-cyclotomic coset. (ii)Any minimal F_qLC code which has nonzero transform* *components in $[j]_n^q$ with exponent e has size q^e. (iii)Let $J_1, J_2, \cdots, J_t$ be the distinct q-cyclotomic cosets of $[0, n-1]$. Then any F_qLC code $\mathcal{C}$ can be decomposed as $\mathcal{C} = \oplus_{i=1}^t \mathcal{C}_{J_i}$, where the direct sum is over F_q.*

For a given F_qLC code, when the corresponding m-quasi-cyclic codes are considered, $\mathcal{C}_{J_i}$, $i = 1, \cdots, t$, give the primary components [7] or irreducible components [5] of the code. But these primary components are not uniquely decomposable into minimal quasi-cyclic codes (or cyclic irreducible submodules, as is called in [5, 7]). If $\mathbf{a} \in F_{q^m}^n$, then the intersection of all the F_qLC codes containing $\mathbf{a}$ is called the F_qLC code generated by $\mathbf{a}$. Such F_qLC codes are refered as one-generator F_qLC codes, whereas the corresponding quasi-cyclic codes are known as one-generator quasi-cyclic codes. For a one-generator F_qLC code $\mathcal{C}$, each component $\mathcal{C}_{J_i}$ is minimal, since otherwise, suppose $\mathcal{C}_{J_k}$ is not minimal and $\mathbf{b} \in \mathcal{C}_{J_k}$ such that $B_j = A_j \; \forall j \in J_k$ and $B_j = 0 \; \forall j \notin J_k$ (by definition of $\mathcal{C}_{J_k}$, such a $\mathbf{b}$ exists). Since $\mathcal{C}_{J_k}$ is not minimal, we can decompose $\mathcal{C}_{J_k}$ as $\mathcal{C}_{J_k} = \mathcal{C}_1 \oplus \mathcal{C}_2$, such that $\mathbf{b} \in \mathcal{C}_1$ and $\mathcal{C}_2 \neq \{\mathbf{0}\}$. Then clearly, $\mathcal{C}' = \mathcal{C}_1 \oplus_{i \neq k} \mathcal{C}_{J_i}$ contains $\mathbf{a}$: a contradiction, since $\mathcal{C}'$ is a proper subcode of $\mathcal{C}$. So, $\mathcal{C}_{J_i}$; $i = 1, \cdots, t$, are minimal for any one-generator code $\mathcal{C}$. Moreover, if for an F_qLC code $\mathcal{C}$, $\mathcal{C}_{J_i}$ is direct sum of t_i minimal F_qLC codes, then the code is generated by $max_{1 \leq i \leq t} t_i$ vectors and the F_q-dimension of the code is $\sum_{i=1}^t t_i |J_i|$.

Once we know which components can be related, we would like to know in what ways they can be related. The following lemma specifies all possible homomorphisms by which a transform component A_{jq^t} can be related to A_j, when A_j takes values from a minimal α^j-invariant subspace. As example, for a minimal F_qLC code, any nonzero transform component is a spectral base and it takes values from a minimal invariant subspace. The other transform components will be related by homomorphisms, specified by Lemma (2.3.9). For 1-generator F_qLC code, a set containing one nonzero transform component from each nonzero q-cyclotomic coset of transform components forms a spectral base and each transform component in the spectral base takes values from minimal invariant subspace. So, Lemma (2.3.9) gives the relations for 1-generator F_qLC codes also. In fact, any F_qLC code, where nonzero transform components takes values from minimal invariant subspaces, the relations of the other transform components with those in a spectral base are given by this lemma.

Lemma 2.3.9. *For some fixed $y \in F_{q^l}$, a homomorphism $\sigma : x_1 F_{q^{e_y}} \to x_2 F_{q^{e_y}}$ satisfies $\sigma(yx) = y^{q^t} \sigma(x) \; \forall x \in x_1 F_{q^{e_y}}$ iff σ is induced by a polynomial $f(X) = cX^{q^t}$ for some* *unique constant* $c \in x_2 x_1^{-q^t} F_{q^{e_y}}$.

Proof: Backward implication is trivial. For the forward implication, clearly σ satisfies the above condition if and only if $\sigma' : F_{q^{e_y}} \to F_{q^{e_y}}$; $x \mapsto x_2^{-1}\sigma(x_1 x)$ satisfies $\sigma'(yx) = y^{q^t}\sigma'(x)$ $\forall x \in F_{q^{e_y}}$. Suppose, $f_1(X) = \sum_{i=0}^{e_y-1} c_i' X^{q^i}$ induces the map σ'. Then, for any $x \in F_{q^{e_y}}$,

$$
\begin{aligned}
& \sigma'(yx) = y^{q^t}\sigma'(x) \\
\Leftrightarrow\ & \sum_{i=0}^{e_y-1} c_i' y^{q^i} x^{q^i} = y^{q^t} \sum_{i=0}^{e_y-1} c_i' x^{q^i} \ \ \forall x \in F_{q^{e_y}} \\
\Leftrightarrow\ & c_i' y^{q^i} x^{q^i} = y^{q^t} c_i' x^{q^i} \ \ \forall x \in F_{q^{e_y}} \ \ \text{for } i = 0, \cdots, e_y - 1 \\
\Leftrightarrow\ & y^{q^i} x^{q^i} = y^{q^t} x^{q^i} \ \ \forall x \in F_{q^{e_y}} \ \ \text{whenever } c_i' \neq 0 \\
\Leftrightarrow\ & i = t \ \ \text{whenever } c_i' \neq 0.
\end{aligned}
$$

So, there is at most one nonzero term $c' X^{q^l}$ in $f_1(X)$ where $c' \in F_{q^{e_y}}$. So, the map σ is induced by the polynomial $f(X) = x_2 f_1(x_1^{-1}X) = x_2 c' x_1^{-q^t} X^{q^t} = cX^{q^t}$ where $c = x_2 c' x_1^{-q^t} \in x_2 x_1^{-q^t} F_{q^{e_y}}$. ■

For $y = \alpha^j$, this theorem specifies all possible homomorphisms by which A_{jq^t} can be related to A_j for an F_qLC code when A_j takes values from a minimal α^j-invariant subspace.

Example 2.3.2. Clearly, in the minimal F_qLC codes $\mathcal{C}_0$ and $\mathcal{C}_2$ in Table 2.1, A_5 is related to A_{10} by homomorphisms. Suppose $A_5 = \sigma_f(A_{10})$ where $f(X)$ is a q-polynomial over F_{2^4}.

For $\mathcal{C}_0$, $f(X) = \alpha^8 X^2$.

For $\mathcal{C}_2$, $f(X) = \alpha X^2$.

Example 2.3.3. Consider an F_qLC code with same parameters as in Table 2.1, where A_1, A_8, A_5 take values freely from $F_{16}, F_{16},$ and $\alpha^3 F_4$ respectively and other nonzero transform components $A_2, A_4,$ and A_{10} are related to them as $A_2 = \alpha^2 A_1^2 + \alpha^5 A_8^4$, $A_4 = \alpha A_1^4 + \alpha^7 A_8^8$, and $A_{10} = \alpha^2 A_5^2$. This code is F_qLC but neither minimal nor 1-generator. But here the spectral base $\{A_1, A_8, A_5\}$ take values from minimal invariant subspaces and thus the other transform components relations with them are dictated by Lemma (2.3.9).

Even if a transform component does not take values from some minimal invariant subspace, another transform component may be related to it by homomorphism. The following theorem specifies all such homomorphisms. In particular, for a code with spectral base, the other transform components are related to those in the spectral base by homomorphisms, even though the transform components in the spectral base do not take values from minimal invariant subspaces. For codes with spectral base, the invariant subspaces of the components in a spectral base and the polynomials inducing the relating homomorphisms for other components specify the code completely.

Theorem 2.3.10. *Suppose $V \subseteq F_{q^l}$ is a y-invariant subspace and $V = \oplus_{j=0}^{t-1} V_j$ where V_j are minimal y-invariant subspaces. Then, for any $\sigma \in Hom_{F_q}(V, F_{q^l})$ satisfying $\sigma(yx) = y^{q^i}\sigma(x)\ \forall x \in V$, there is a unique polynomial of the form $f(X) = \sum_{j=0}^{t-1} a_j X^{q^{jey+i}}$; $a_j \in F_{q^l}$ such that $\sigma = \sigma_f$.*

Proof: By Lemma 2.3.9, there exists a unique $f_j(X) = b_j X^{q^i}$, $b_j \in F_{q^l}$, which induces $\sigma|_{V_j}$ i.e., $\sigma|_{V_j} = \sigma_{f_j}|_{V_j}$.

Let us consider any polynomial $f(X) = \sum_{j=0}^{t-1} a_j X^{q^{jey+i}}$ where $a_j \in F_{q^l}$. Now, $\sigma = \sigma_f \Leftrightarrow \sigma|_{V_j} = \sigma_{f_j}|_{V_j}\ \forall j$.

Suppose $V_j = x_j F_{q^{ey}}$; $x_j \neq 0$, for $j = 0, 1, \cdots, t-1$. For any $v \in V_j$, $v = x_j s$ for some $s \in F_{q^{ey}}$. So,

$$\begin{aligned} \sigma_f|_{V_k} = \sigma_{f_k}|_{V_k} &\Leftrightarrow f(x_k s) = f_k(x_k s)\ \forall s \in F_{q^{ey}} \\ &\Leftrightarrow \left(\sum_{j=0}^{t-1} a_j x_k^{q^{jey+i}}\right) s^{q^i} = b_k x_k^{q^i} s^{q^i}\ \forall s \in F_{q^{ey}} \\ &\Leftrightarrow \sum_{j=0}^{t-1} a_j x_k^{q^{jey+i}} = b_k x_k^{q^i} \end{aligned}$$

So,

$$\sigma = \sigma_f \Leftrightarrow M \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} b_0 x_0^{q^i} \\ b_1 x_1^{q^i} \\ \vdots \\ b_{t-1} x_{t-1}^{q^i} \end{pmatrix} \tag{2.8}$$

where

$$M = \begin{pmatrix} x_0^{q^i} & x_0^{q^{ey+i}} & x_0^{q^{2ey+i}} & \cdots & x_0^{q^{(t-1)ey+i}} \\ x_1^{q^i} & x_1^{q^{ey+i}} & x_1^{q^{2ey+i}} & \cdots & x_1^{q^{(t-1)ey+i}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{t-1}^{q^i} & x_{t-1}^{q^{ey+i}} & x_{t-1}^{q^{2ey+i}} & \cdots & x_{t-1}^{q^{(t-1)ey+i}} \end{pmatrix}$$

Now, $\{x_0, x_1, \cdots, x_{t-1}\}$ are linearly independent over $F_{q^{e_y}}$ since V is the direct sum of $x_0 F_{q^{e_y}}, x_1 F_{q^{e_y}}, \cdots, x_{t-1} F_{q^{e_y}}$. So, $\{x_0^{q^i}, x_1^{q^i}, \cdots, x_{t-1}^{q^i}\}$ are linearly independent over $F_{q^{e_y}} \Rightarrow$ M is nonsingular [81] $\Rightarrow$ there exists unique solution of (2.8) for $a_0, a_1, \cdots, a_{t-1}$. ■

If A_j takes values from an α^j-invariant subspace $V = \oplus_{l=0}^{t-1} V_l$ and A_{jq^i} is related to A_j by homomorphism, then the relation can be expressed as $A_k = \sum_{l=0}^{t-1} c_j A_j^{q^{le_j+i}}$ for some constants $c_j \in F_{q^l}$. If $j_1, \cdots, j_w \in [k]_n^q$ and A_k is related to $A_{j_1}, \cdots, A_{j_w}$ by homomorphisms i.e., if $A_k = \sigma_1(A_{j_1}) + \cdots + \sigma_w(A_{j_w})$, where $\sigma_1, \cdots, \sigma_w$ are homomorphisms, then the relation can be expressed as $A_k = \sum_{h_1=0}^{l_1-1} c_{1,h_1} A_{j_1}^{q^{h_1 e_k + t_1}} + \cdots + \sum_{h_w=0}^{l_w-1} c_{w,h_w} A_{j_w}^{q^{h_w e_k + t_w}}$, where $k \equiv j_i^{q^{t_i}} \bmod n$ for $i = 1, \cdots, w$.

Example 2.3.4. In the code $\mathcal{C}_5$ in Table 2.1, A_5 is related to A_{10} by a homomorphism induced by the polynomial $f(X) = \alpha^{14}X^2 + \alpha^8 X^8$.

Example 2.3.5. Consider a code with the same parameters as in Table 2.1, where A_{14}, A_{13} and A_{10} take values freely from F_{16} which is not a minimal α^{10}-invariant subspace. Suppose the other nonzero transform components are related to these as $A_{11} = \alpha^6 A_{14}^4 + \alpha^4 A_{13}^2$, $A_7 = \alpha^7 A_{14}^8 + \alpha^{11} A_{13}^4$, and $A_5 = \alpha^7 A_{10}^2 + \alpha^{13} A_{10}^8$. It can be checked that the code constructed this way is an F_qLC code. $\{A_{14}, A_{13}, A_{10}\}$ is a spectral base of the code and so the other transform components are related to them by the homomorphisms as specified by Theorem 2.3.10.

In general, an F_qLC code may not have a spectral base and thus the relations between the transform components are not given by Theorem 2.3.10. For such codes, transform domain characterization can be given in terms of a decomposition of the code into F_qLC codes with spectral base. One such way of decomposing is by restricting the transform components to minimal invariant subspaces. From Theorem 2.3.2, Theorem 2.3.7 and Lemma 2.3.9, transform domain characterization of F_qLC codes can be stated as follows:

Theorem 2.3.11 (Transform Domain Characterization). *$\mathcal{C}$ is an F_qLC-code iff for any $j \in I_n$, the transform components in $[j]_n^q$ and $I_n \setminus [j]_n^q$ are unrelated and for each $[j]_n^q$-subcode $\mathcal{C}_{[j]_n^q}$ the subcodes obtained by restricting the nonzero transform components to minimal α^j-invariant subspaces satisfy*

- *A_j is zero or takes values from a minimal α^j-invariant subspace.*
- *There is a maximal set L of unrelated components such that*
  $A_j = \sum_{l \in L} c_{jl} A_l^{q^t}$ for any nonzero A_j, where $c_{jl} \in F_{q^{r_j}}$ and $j \equiv lq^t \bmod n$.

2.3.4 Special Cases

In this subsection several special cases arising out of restrictions on the values of n, q and m are discussed.

1. **No related components:** Recall that for a given n, the exponents of $[j]_n^q$ and $[j]_n^{q^m}$ are denoted by, respectively, e_j and r_j. If $e_j = r_j$ for $0 \leq j \leq (n-1)$, then no two q^m-cyclotomic coset modulo n can be within one q-cyclotomic cosets modulo n, since every q-cyclotomic coset modulo n is also a q^m-cyclotomic coset modulo n. In this case, no two or more transform components with indexes from different q^m-cyclotomic cosets can be related. In such cases, the F_qLC codes are completely specified by the invariant subspaces from which the nonzero transform components take values. Two such cases are $n = 15, q = 2$ and $m = 3$ and $n = 63, q = 2$ and $m = 5$.

   This special case is obtained if e_1 is a prime then for all values of m. For example $n = 31$ and $q = 2$.

2. **m=1:** When $m = 1$, the codes under consideration are conventional linear cyclic codes over F_q. This case is also the special case of the previous one i.e., the case for which no related components are possible.

2.4 Dual Codes of F_qLC Codes

In this section, the equivalent condition in transform domain for two codes being dual of each other is derived, and nonexistence of self dual F_qLC codes for certain cases is proved. Unlike linear codes, dual of an F_qLC code has been defined as F_q-dual w. r. t. an F_q-basis of F_{q^m} [1]. That is, if $\{\gamma_1, \gamma_2, \cdots, \gamma_m\}$ is an F_q-basis of F_{q^m}, then two vectors $\mathbf{a}, \mathbf{b} \in F_{q^m}^n$ are called orthogonal to each other, if $\sum_{i=0}^{n-1} \sum_{j=1}^{m} a_{ij} b_{ij} = 0$, where a_{ij} and b_{ij} denote the j-th components of $\mathbf{a}$ and $\mathbf{b}$ respectively. Henceforth, 'tr' will always denote the F_{q^m}/F_q-trace.

Definition 5. [81] An F_q-basis $\{\gamma_1, \gamma_2, \cdots, \gamma_m\}$ of F_{q^m} is called a **self dual basis** if

$$\begin{aligned} tr(\gamma_i \gamma_j) &= 1 \quad \text{if } i = j \\ &= 0 \quad \text{if } i \neq j. \end{aligned}$$

Clearly, the j-th component of $\mathbf{x} \in F_{q^m}$ w. r. t. a self dual basis is given by $tr(\gamma_j x)$. It is known [82] that a self dual basis exists if and only if q is even or q and m are both odd.

We consider only the cases where a self dual basis of F_{q^m} exists and in which case define F_q duality with respect to such a basis. The following theorem gives the transform domain condition for two vectors to be F_q dual of each other.

Lemma 2.4.1. *For any* $\mathbf{a}, \mathbf{b} \in F_{q^m}^n$, $\mathbf{a} \perp \mathbf{b}$ *if and only if*

$$tr\left(\sum_{k=0}^{n-1} A_{-k} B_k\right) = 0. \tag{2.9}$$

Proof: Suppose $\{\gamma_1, \gamma_2, \cdots, \gamma_m\}$ is a self dual basis of F_{q^m}.

$$\begin{aligned}
\mathbf{a} \perp \mathbf{b} \;&\Leftrightarrow\; \sum_{i=0}^{n-1}\sum_{j=1}^{m} a_{ij} tr(\gamma_j b_i) = 0 \\
&\Leftrightarrow\; tr\left(\sum_{i=0}^{n-1}\sum_{j=1}^{m} a_{ij}\gamma_j b_i\right) = 0 \\
&\Leftrightarrow\; tr\left(\sum_{i=0}^{n-1}\sum_{j=1}^{m} a_{ij}\gamma_j \sum_{k=0}^{n-1} \alpha^{-ik} B_k\right) = 0 \\
&\Leftrightarrow\; tr\left(\sum_{k=0}^{n-1} B_k \sum_{i=0}^{n-1} \alpha^{-ik} \sum_{j=0}^{m} a_{ij}\gamma_j\right) = 0 \\
&\Leftrightarrow\; tr\left(\sum_{k=0}^{n-1} B_k \sum_{i=0}^{n-1} \alpha^{-ik} a_i\right) = 0 \\
&\Leftrightarrow\; tr\left(\sum_{k=0}^{n-1} B_k A_{-k}\right) = 0.
\end{aligned}$$

■

Theorem 2.4.1 specializes to the case of $m = 1$ as: $\mathbf{a} \perp \mathbf{b}$ iff $\sum_{k=0}^{n-1} A_{-k} B_k = 0$.

Since for an $F_q LC$ code $\mathcal{C}$, transform components in different q-cyclotomic cosets are unrelated, using Theorem 2.4.1, we can write $\mathcal{C}^\perp$ as (note that $J_1, J_2, \cdots, J_t$ are the distinct q-cyclotomic cosets of I_n):

$$\mathcal{C}^\perp = \left\{ \mathbf{b} \in F_{q^m}^n \middle| tr\left(\sum_{k \in J_i} B_k A_{-k}\right) = 0 \text{ for } i = 1, \cdots, t \text{ and } \forall \mathbf{a} \in \mathcal{C} \right\}$$

and the J_i-subcode of $\mathcal{C}^\perp$ obtained by restricting A_j; $j \notin J_i$ to zero can be written as

$$\begin{aligned}\left(\mathcal{C}^\perp\right)_{J_i} &= \left\{\mathbf{b} \in F_{q^m}^n | tr\left(\sum_{k \in J_i} B_k A_{-k}\right) = 0 \text{ and } B_k = 0 \text{ for } k \notin J_i\ \forall \mathbf{a} \in \mathcal{C}\right\} \\ &= \left\{\mathbf{b} \in F_{q^m}^n | tr\left(\sum_{k \in J_i} B_k A_{-k}\right) = 0 \text{ and } B_k = 0 \text{ for } k \notin J_i\ \forall \mathbf{a} \in \mathcal{C}_{-J_i}\right\} \quad (2.10)\end{aligned}$$

So, $\left(\mathcal{C}^\perp\right)_{J_i}$ is the biggest code with zero transform components outside $-J_i = \{-j \bmod n | j \in J_i\}$ which is orthogonal to $\mathcal{C}_{-J_i}$.

Using Theorem 2.4.1, the following nonexistence result for self dual F_qLC codes is obtained.

Theorem 2.4.2. *There is no self dual F_qLC code over F_{q^m} when $(n, q) = 1$ and m is odd.*

Proof: For the cases under consideration, there is always a self dual basis $\{\gamma_1, \gamma_2, \cdots, \gamma_m\}$ of F_{q^m}. Suppose, in the F_qLC codes $\mathcal{C}$ and it's dual $\mathcal{C}^\perp$, A_0 takes values from the F_q-subspaces $V \subseteq F_{q^m}$ and $V_1 \subseteq F_{q^m}$ respectively. Since A_0 is not related to other transform components, for any $v \in V$, there is a codeword in $\mathcal{C}$ with $A_0 = v$ and all other transform components zero. So according to Theorem (2.4.1), $V_1 = \{v_1 \in F_{q^m} | tr(vv_1) = 0\ \forall v \in V\} = V^\perp$. Where $V^\perp$ is the trace dual subspace of V. If $\mathcal{C}$ is a self dual code, then $V = V^\perp \Rightarrow dim_{F_q}(V) = m - dim_{F_q}(V)$ which is impossible since m is odd. ■

Note that the theorem is independent of the choice of the basis, though a self dual basis is used to prove it. If a self dual code exists w. r. t. any basis of F_{q^m}, then by change of basis one can get another code which is self dual w. r. t. a self dual basis.

Corollary 2.4.3. *There is no self dual m-QC code over F_q of length mn if m is odd and $(n, q) = 1$.*

Suppose q and m are even, n is odd and q-cyclotomic cosets modulo n are all singletons. Then, by equation (2.10), A_0 should take values from one self dual subspace of F_{q^m} i.e., a subspace V such that

$$V = \{v \in F_{q^m} | tr(vu) = 0 \text{ for each } u \in V\}. \quad (2.11)$$

With respect to a self dual basis of F_{q^m}, such a subspace is image of a self dual code of length m over F_q. Since number of self dual codes of length m over F_q is $\prod_{i=1}^{\frac{m}{2}-1}(q^i + 1)$

(see [20]), V can be chosen in $\prod_{i=1}^{\frac{m}{2}-1}(q^i+1)$ ways. For any other $k \in I_n$, A_k can be chosen to take values from any subspace V_k of F_{q^m} and A_{-k} should take values from it's dual subspace. So, the number of ways in which subspaces for A_k and A_{-k} can be chosen is $N(m,q)$= number of distinct subspaces of F_{q^m}. So, the total number of self dual quasi-cyclic codes with these parameters is $N(m,q)^{\frac{n-1}{2}} \prod_{i=1}^{\frac{m}{2}-1}(q^i+1)$.

Remark: Cor. 2.4.3 and the above expression for the total number of quasi-cyclic self dual codes is also available in [8] and also follows from the results in Chapter 4 as corollary.

2.5 Parity Check Matrix and Minimum Distance of Quasicyclic Codes

For linear codes, Tanner [80] used parity check equations over an extension field to derive minimum distance bound in terms of minimum distance of certain cyclic codes. Given a binary parity check matrix of a binary QC code, Tanner used block-wise DFT or block-wise linearized polynomial transform or Kronecker product of the two to get a set of parity check equations over an extension field of F_2.

An n-length F_qLC code over F_{q^m} can be considered as an m-QC code of length nm over F_q by expanding each component as F_q-linear combination of an F_q-basis of F_{q^m}. Similarly, any nm-length m-QC code can be considered as an n-length F_qLC code over F_{q^m}. Here it is described how in some cases one can directly get a set of parity check equations of a QC code over an extension field of F_q from the transform domain structure of the corresponding F_qLC code. Before doing so, we first give a theorem (Theorem 2.5.1) for the distance bound. This is in a slightly different form from Tanner's related theorems [80, Theorems 6,8 and 10] and the proof is also similar. Power of a vector will mean component-wise power.

Theorem 2.5.1. *Suppose, the components of the vector* $\mathbf{v} \in F_{q^r}^n$ *are nonzero and distinct. If for each* $k = k_0, k_1, \cdots, k_{\delta-2}$, *the vectors* $\mathbf{v}^k$ *are in the span of a set of parity check equations over* F_{q^r}, *then the minimum distance of the code is at least that of the cyclic code of length* q^r-1 *with roots* β^k, $k = k_0, k_1, \cdots, k_{\delta-2}$ *where* β *is a primitive element of* F_{q^r}.

Proof: Let $\mathcal{C}$ be the code, which has $\mathbf{v}^k$, $k = k_0, k_1, \cdots, k_{\delta-2}$ in the span of it's' parity check equations. Let the corresponding cyclic code be $\mathcal{C}_c$.

Suppose $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ with $v_i = \beta^{\lambda_i}$, where λ_i's are distinct.

For any $\mathbf{a} \in \mathcal{C}$ with weight $\omega_H(\mathbf{a}) = d$, we'll show that $\exists \mathbf{a}' \in \mathcal{C}_c$, s. t. $\omega_H(\mathbf{a}') = d$.

We construct $\mathbf{a}'$ as

$$a'_{\lambda_i} = a_i \text{ for } i \in [0, n-1]$$
$$a'_j = 0 \text{ when } j \neq \lambda_i \ \forall i \in [0, n-1]$$

Clearly, $\omega_H(\mathbf{a}') = d$.

Now,

$$\begin{aligned}
\mathbf{a} \in \mathcal{C} \ &\Rightarrow \ \sum_{i=0}^{n-1} a_i v_i^k = 0 \ \ for \ \ k = k_0, k_1, \cdots, k_{\delta-2} \\
&\Rightarrow \ \sum_{i=0}^{n-1} a'_{\lambda_i} \beta^{\lambda_i k} = 0 \ \ for \ \ k = k_0, k_1, \cdots, k_{\delta-2} \\
&\Rightarrow \ \sum_{j=0}^{q^r-2} a'_j \beta^{jk} = 0 \ \ for \ \ k = k_0, k_1, \cdots, k_{\delta-2} \\
&\Rightarrow \ \mathbf{a}' \in \mathcal{C}_c.
\end{aligned}$$

■

The idea behind this theorem is that, if a code has certain powers of $\mathbf{v}$ as parity check vectors, then the code can be seen as a shortened code (that is, the code obtained by taking the codewords with certain positions zeros and then deleting those positions)[20] of a cyclic code of length $q^r - 1$. Not only is the minimum distance of the code guaranteed to be at least that of the cyclic code, the decoding algorithm for the cyclic code can also be used to decode the shortened code. The decoder only have to pad zeros in the truncated positions and decode from the resulting $q^r - 1$ length vector.

If $k_i = k_0 + i$ in Theorem 2.5.2, by the BCH bound one can conclude that the minimum distance of the n length code is at least δ.

Here is a natural generalization of the results using which some minimum distance can be guaranteed by viewing the code as a shortened code of an abelian code.

For s vectors $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_s$ over F_{q^r} of lengths $n_1, n_2, \cdots, n_s$ respectively, let $\mathbf{v}_1 \boxtimes \mathbf{v}_2 \boxtimes \cdots, \boxtimes \mathbf{v}_s$ denote the $n_1 \times n_2 \times \cdots \times n_s$ array with $(i_1, i_2, \cdots, i_s)$-th element $v_{1,i_1} v_{2,i_2} \cdots v_{s,i_s}$.

Theorem 2.5.2. *Let r be an arbitrary positive integer and the components of each of the vectors $\mathbf{v}_l$; $l = 1, \cdots, s$ of lengths $n_1, n_2, \cdots, n_s$ respectively be nonzero and distinct. If the* *components of the code can be arranged in an $n_1 \times n_2 \times \cdots \times n_s$ array, such that for each $k_l = k_{l,0}, k_{l,1}, \cdots, k_{l,\delta_l-2}$ for $l = 1, \cdots, s$, the arrays $\mathbf{v}_1^{k_1} \boxtimes \mathbf{v}_2^{k_2} \boxtimes \cdots \boxtimes \mathbf{v}_s^{k_s}$ are in the span of a set of parity check equations over F_{q^r}, then the minimum distance of the code is at least that of the s-dimensional cyclic code of length $(q^r-1)^s$ with roots $(\beta^{k_1}, \beta^{k_2}, \cdots, \beta^{k_s})$, where β is a primitive element of F_{q^r}.*

Proof: Let $\mathcal{C}$ be a code having $\mathbf{v}_1^{k_1} \boxtimes \mathbf{v}_2^{k_2} \boxtimes \cdots \boxtimes \mathbf{v}_s^{k_s}$ in the span of it's' parity check equations for $k_l = k_{l,0}, k_{l,1}, \cdots, k_{l,\delta_l-2}$ for $l = 1, \cdots, s$. Let the corresponding s-dimensional cyclic code be $\mathcal{C}_a$.

Suppose $\mathbf{v}_l = (v_{l,0}, v_{l,1}, \cdots, v_{l,n_l-1})$ with $v_{l,i} = \beta^{\lambda_{l,i}}$, where $\lambda_{l,i} \neq \lambda_{l,j}$ for $i \neq j$; $\forall l$.

For any $\mathbf{a} \in \mathcal{C}$ with weight $\omega_H(\mathbf{a}) = d$, we'll show that $\exists \mathbf{a}' \in \mathcal{C}_c$, s. t. $\omega_H(\mathbf{a}') = d$.

We construct $\mathbf{a}'$ as

$$\begin{aligned} a'_{\lambda_{1,i_1},\cdots,\lambda_{s,i_s}} &= a_{i_1,\cdots,i_s} \text{ for } (i_1, \cdots, i_s) \in I_{n_1 \times n_2, \times \cdots, \times n_s} \\ a_{j_1,\cdots,j_s} &= 0 \text{ when } (j_1, \cdots, j_s) \neq (\lambda_{1,i_1}, \cdots, \lambda_{s,i_s}) \;\; \forall (i_1, \cdots, i_s) \in I_{n_1 \times n_2, \times \cdots, \times n_s} \end{aligned}$$

Clearly, $\omega_H(\mathbf{a}') = d$.

Now,

$$\begin{aligned} \mathbf{a} \in \mathcal{C} \;\; &\Rightarrow \sum_{i_1=0}^{n_1-1} \cdots \sum_{i_s=0}^{n_s-1} a_{i_1,\cdots,i_s} v_{1,i_1}^{k_1} \cdots v_{s,i_s}^{k_s} = 0 \;\; for \;\; k_1 = k_{1,0}, k_{1,1}, \cdots, k_{1,\delta_1-2}, \;\cdots \;, \\ & \qquad\qquad\qquad\qquad\qquad\qquad k_s = k_{s,0}, k_{s,1}, \cdots, k_{s,\delta_s-2} \\ &\Rightarrow \sum_{i_1=0}^{n_1-1} \cdots \sum_{i_s=0}^{n_s-1} a'_{\lambda_{1,i_1},\cdots,\lambda_{s,i_s}} \beta^{\lambda_{1,i_1} k_1} \cdots \beta^{\lambda_{s,i_s} k_s} = 0 \qquad '' \\ &\Rightarrow \sum_{j_1=0}^{q^r-1} \cdots \sum_{j_s=0}^{q^r-1} a'_{j_1,\cdots,j_s} \beta^{j_1 k_1} \cdots \beta^{i_s k_s} = 0 \qquad '' \\ &\Rightarrow \mathbf{a}' \in \mathcal{C}_a \end{aligned}$$

■

Though Theorem 2.5.2 gives a way to get minimum distance bound of any linear code, for which a set of parity check equations over an extension field is known, it is very difficult to know which arrangement of the code components in how many dimensions with what choice of $\mathbf{v}_l$'s will give the maximum bound on the minimum distance. Even for the one-dimensional ($s = 1$) case, it is very difficult to choose the best $\mathbf{v}_1$ and arrangement of code components because of the huge possibility of choices.

Recall that the correspondence between F_qLC codes over F_{q^m} and m-QC codes over F_q is with respect to an F_q-basis of F_{q^m}. Let us take a basis $\{\beta_0, \beta_1, \cdots, \beta_{m-1}\}$. By our characterization of F_qLC codes in DFT domain, we know that for any $j \in [0, n-1]$, A_j can take values from any α^j-invariant subspace of $F_{q^{mr_j}}$. In particular, A_j can take values from subspaces of the form $c^{-1}F_{q^l}$ where $e_j|l$ and $l|mr_j$. Such a DFT domain restriction gives a parity check equation of the corresponding QC code over $F_{q^{mr}}$ as follows.

$$
\begin{aligned}
A_j \in c^{-1}F_{q^l} \quad & \Leftrightarrow cA_j \in F_{q^l} \\
& \Leftrightarrow (cA_j)^{q^l} = cA_j \\
& \Leftrightarrow \left(c\sum_{i=0}^{n-1}\alpha^{ij}a_i\right)^{q^l} = c\sum_{i=0}^{n-1}\alpha^{ij}a_i \\
& \Leftrightarrow \left(c\sum_{i=0}^{n-1}\alpha^{ij}\sum_{x=0}^{m-1}a_{ix}\beta_x\right)^{q^l} = c\sum_{i=0}^{n-1}\alpha^{ij}\sum_{x=0}^{m-1}a_{ix}\beta_x \\
& \Leftrightarrow c^{q^l}\sum_{i=0}^{n-1}\sum_{x=0}^{m-1}a_{ix}\alpha^{ijq^l}\beta_x^{q^l} = c\sum_{i=0}^{n-1}\sum_{x=0}^{m-1}a_{ix}\alpha^{ij}\beta_x \\
& \Leftrightarrow \sum_{i=0}^{n-1}\sum_{x=0}^{m-1}a_{ix}\left(c^{q^l}\alpha^{ijq^l}\beta_x^{q^l} - c\alpha^{ij}\beta_x\right) = 0.
\end{aligned}
$$

This gives a parity check vector $\mathbf{h} = (h_{0,0}, h_{0,1}, \cdots, h_{0,m-1}, \cdots, h_{n-1,0}, \cdots, h_{n-1,m-1})$ with $h_{i,x} = \left(c^{q^l}\alpha^{ijq^l}\beta_x^{q^l} - c\alpha^{ij}\beta_x\right)$. If $A_j = 0$, it gives a parity check vector $\mathbf{h}$ with $h_{i,x} = \alpha^{ij}\beta_x$.

Now, for an F_qLC code, A_k can be related to several other transform components $A_{j_1}, A_{j_2}, \cdots, A_{j_w}$ by homomorphisms, where $j_1, \cdots, j_w \in [k]_n^q$. Then, for some constants $c_{i,h_i} \in F_{q^{mr}}$,

$$
\begin{aligned}
A_k \quad & = \sum_{h_1=0}^{l_1-1} c_{1,h_1} A_{j_1}^{q^{h_1 e_k + t_1}} + \cdots \\
& \qquad + \sum_{h_w=0}^{l_w-1} c_{w,h_w} A_{j_w}^{q^{h_w e_k + t_w}} \\
\Leftrightarrow \quad \sum_{i=0}^{n-1} a_i\alpha^{ik} \quad & = \sum_{h_1=0}^{l_1-1} c_{1,h_1}\left(\sum_{i=0}^{n-1} a_i\alpha^{ij_1}\right)^{q^{h_1 e_k + t_1}} + \cdots \\
& \qquad + \sum_{h_w=0}^{l_w-1} c_{w,h_w}\left(\sum_{i=0}^{n-1} a_i\alpha^{ij_w}\right)^{q^{h_w e_k + t_w}}
\end{aligned}
$$

$$\Leftrightarrow \quad \sum_{i=0}^{n-1} a_i\alpha^{ik} = \sum_{h_1=0}^{l_1-1} c_{1,h_1} \sum_{i=0}^{n-1} a_i^{q^{h_1e_k+t_1}} \alpha^{ij_1q^{h_1e_k+t_1}} + \cdots + \sum_{h_w=0}^{l_w-1} c_{w,h_w} \sum_{i=0}^{n-1} a_i^{q^{h_we_k+t_w}} \alpha^{ij_wq^{h_we_k+t_w}}$$

$$\Leftrightarrow \quad \sum_{i=0}^{n-1}\sum_{x=0}^{m-1} a_{ix}\beta_x\alpha^{ik} = \sum_{i=0}^{n-1}\sum_{x=0}^{m-1} a_{ix} \sum_{h_1=0}^{l_1-1} c_{1,h_1} \beta_x^{q^{h_1e_k+t_1}} \alpha^{ij_1q^{h_1e_k+t_1}} + \cdots + \sum_{i=0}^{n-1}\sum_{x=0}^{m-1} a_{ix} \sum_{h_w=0}^{l_w-1} c_{w,h_w} \beta_x^{q^{h_we_k+t_w}} \alpha^{ij_wq^{h_we_k+t_w}}$$

$$\Leftrightarrow \quad \sum_{i=0}^{n-1}\sum_{x=0}^{m-1} a_{ix}\left(\beta_x\alpha^{ik} - \sum_{h_1=0}^{l_1-1} c_{1,h_1} \beta_x^{q^{h_1e_k+t_1}} \alpha^{ij_1q^{h_1e_k+t_1}} - \cdots - \sum_{h_w=0}^{l_w-1} c_{w,h_w} \beta_x^{q^{h_we_k+t_w}} \alpha^{ij_wq^{h_we_k+t_w}}\right) = 0.$$

This gives a parity check vector $\mathbf{h}$ with $h_{i,x} = \left(\beta_x\alpha^{ik} - \sum_{h_1=0}^{l_1-1} c_{1,h_1} \beta_x^{q^{h_1e_k+t_1}} \alpha^{ij_1q^{h_1e_k+t_1}} - \cdots - \sum_{h_w=0}^{l_w-1} c_{w,h_w} \beta_x^{q^{h_we_k+t_w}} \alpha^{ij_wq^{h_we_k+t_w}}\right)$.

The component wise conjugate vectors of the parity check vectors obtained in these ways and the vectors in their span are also parity check vectors of the code. However, in general for any F_qLC code, the components may not be related simply by homomorphisms or components may not take values from the subspaces of the form $c^{-1}F_{q^l}$. In those cases, the parity check vectors obtained in the above ways may not specify the code completely. But still those equations can be used for estimating a minimum distance bound by Theorem 2.5.1 or Theorem 2.5.2.

Since the DFT components in different q-cyclotomic cosets modulo n are unrelated, the set of parity check equations over F_{q^r} are union of the check equations corresponding to each q-cyclotomic coset modulo n. In a minimal code, any nonzero DFT component A_j takes values from a minimal α^j-invariant subspace and all other nonzero components (which are in the same q-cyclotomic coset modulo n) are related to A_j by an isomorphism. So, for any minimal code, a set of parity check vectors completely specifying the code can be obtained. Since for any one-generator code, $[j]_n^q$-subcode is minimal or zero for each j, a set of parity check vectors completely specifying the code can be obtained for one-generator codes also. There are however other codes for which complete set of parity check vectors can be derived. In fact, codes can be constructed by imposing simple transform domain restrictions and thus allowing derivations of a complete set of parity check equations over $F_{q^{mr}}$. We illustrate this with the following two examples.

If β is a primitive element of $F_{q^{mr}}$, then $\alpha = \beta^{\frac{q^{mr}-1}{n}}$ is used as the DFT kernel and $\{1, \beta, \beta^2, \cdots, \beta^{m-1}\}$ is taken as the basis.

Example 2.5.1. We consider the F_2LC code of length $n = 3$ over F_{2^4} given by the transform domain restrictions $A_0 = 0$ and $A_2 = \beta^4 A_1^2 + \beta^{10} A_1^8$. With the chosen basis, these two restrictions give the parity check vectors of the corresponding 4-QC code

$$\begin{aligned} \mathbf{h}_{(1)} &= \left(1, \beta, \beta^2, \beta^3, 1, \beta, \beta^2, \beta^3, 1, \beta, \beta^2, \beta^3\right) \\ \text{and } \mathbf{h}_{(2)} &= \left(\beta^8, \beta^5, \beta^{12}, \beta^6, \beta^3, 1, \beta^7, \beta, \beta^{13}, \beta^{10}, \beta^2, \beta^{11}\right) \end{aligned}$$

respectively. Component-wise conjugates of these vectors are also parity check vectors. Moreover,
${\mathbf{h}_{(2)}}^3 = (\beta^9, 1, \beta^6, \beta^3, \beta^9, 1, \beta^6, \beta^3, \beta^9, 1, \beta^6, \beta^3) = \beta \mathbf{h}_{(1)} + \beta^8 {\mathbf{h}_{(1)}}^2 + \beta^6 {\mathbf{h}_{(1)}}^4 + {\mathbf{h}_{(1)}}^8$ and ${\mathbf{h}_{(2)}}^0 = (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) = \beta^{11} \mathbf{h}_{(1)} + \beta^7 {\mathbf{h}_{(1)}}^2 + \beta^{15} {\mathbf{h}_{(1)}}^4 + \beta^{13} {\mathbf{h}_{(1)}}^8$. So, five consecutive powers of $\mathbf{h}_{(2)}$ are parity check vectors of the corresponding QC code. Clearly, the dimension of the code is 4 since $A_1 \in F_{2^4}$. So, the corresponding QC code is a $[12, 4, 6]$ code.

Example 2.5.2. Consider the F_qLC code of length $n = 3$ over F_{2^3} given by the transform domain restriction $A_1 \in \beta^{62} F_{2^2}$, where the DFT is taken over F_{2^6}. With the chosen basis, this restriction in DFT domain gives the parity check vector of the corresponding 3-QC code of length 9 :

$$\mathbf{h} = \left(\beta^{54}, \beta^{14}, \beta^{35}, \beta^{55}, \beta^{15}, \beta^{36}, \beta^{56}, \beta^{16}, \beta^{37}\right).$$

The components of this vector are nonzero and distinct. Since $\mathbf{h}$ and it's conjugate $\mathbf{h}^2$ are both parity check equations of the QC code, this gives a minimum distance lower bound of 3. If the vector $\mathbf{h}^0 = (1, 1, \cdots, 1)$ is included as a parity check vector, a minimum distance bound of 4 is obtained.

2.6 Discussion

The class of F_q-linear cyclic (F_qLC) codes over F_{q^m} have been characterized using the DFT defined over an extension field of F_{q^m}. The characterization is used to get minimum distance bound for m-quasi-cyclic codes of length mn. The characterization is also used to prove a nonexistence result for self dual quasi-cyclic codes. Some interesting special cases have been identified and discussed.

Chapter 3

Quasi-cyclic Codes

3.1 Introduction

A code is called l-quasi-cyclic if cyclic shift of every codeword by l positions gives another codeword [20]. The class of quasi-cyclic codes is a generalization of cyclic codes (l=1) and has been studied by several authors in various context. The connection between quasi-cyclic codes and convolutional codes have been studied in [83] and [84]. The class of quasi-cyclic codes contain good codes in the sense of meeting a version of the Gilbert-Varshamov bound [4]. With restrictions on the parameters, quasi-cyclic codes have been investigated in [51–56, 77, 85–88]. Some of the early works on quasi-cyclic codes are done using the properties of circulant matrices by Karlin [64, 89].

There has been renewed interest in quasi-cyclic codes due to their close relationship with tail-biting representation of general block codes [90]. For instance, motivated by the 64-state quasi-cyclic representation of the $(24, 12, 8)$ Golay code, reported in [83], theory of tail-biting representation of block codes is initiated in [90] and minimal tail-biting trellises for several codes including the Golay code are reported.

For studying l-quasi-cyclic codes, quite often [4, 6, 7, 51–56, 80, 83–87] co-ordinates of a codeword $\mathbf{a} = (a_0, a_1, \cdots, a_{n-1})$ are permuted and blocked as $((a_0, a_l, a_{2l}, \cdots, a_{(\frac{n}{l}-1)l}),$ $(a_1, a_{l+1}, a_{2l+1}, \cdots, a_{(\frac{n}{l}-1)l+1}), \cdots, (a_{l-1}, a_{2l-1}, a_{3l-1}, \cdots, a_{n-1}))$. With this co-ordinate ordering, generator and parity check matrices (with possibly some redundant rows) can be written as matrices with $\frac{n}{l} \times \frac{n}{l}$ circulant matrices as elements. It specializes to cyclic codes with $l = 1$ resulting in only one block in the codewords and circulant matrices as generator and parity check matrices. In the recent literature [7], Lally and Fitzpatrick consider the codewords in the blocked polynomial form as $(a^{(0)}(X), a^{(1)}(X), a^{(2)}(X), \cdots, a^{(l-1)}(X))$ where $a^{(i)}(X) = a_i + a_{i+l}X + a_{i+2l}X^2 + \cdots + a_{i+(\frac{n}{l}-1)l}X^{\frac{n}{l}-1})$ and view a quasi-cyclic code as a submodule of $\left(\frac{F_q[X]}{(X^{\frac{n}{l}}-1)}\right)^l$. The authors then investigate the structural properties of quasi-cyclic codes with the help of Groebner bases of modules over $F_q[X]$. Essentially the same module structure was imposed by Conan and Seguin in [5, 6] in unblocked form of codewords. They imposed an $F_q[X]$-module structure on the code by defining $f(X).\mathbf{a} = f(T^l)(\mathbf{a})$, where T is the cyclic shift operator. Since $(X^{\frac{n}{l}} - 1) \subseteq F_q[X]$ annihilates the code, the code can be seen as an $\frac{F_q[X]}{(X^{\frac{n}{l}}-1)}$ module. Unblocked polynomial form of a codeword can be obtained from the blocked polynomial form of a codeword as $a(X) = a^{(0)}(X^l) + Xa^{(1)}(X^l) + X^2a^{(2)}(X^l) + \cdots + X^{l-1}a^{(l-1)}(X^l))$.

Tanner in [80] gives ways to transform block circulant binary parity check matrix into a parity check matrix over an extension field by block wise DFT or linearized polynomial transform. He gives an interesting way to estimate minimum Hamming distance bound from such parity check matrix. For using block wise DFT, one need the condition $(\frac{n}{l}, 2) = 1$, whereas linearized polynomial transform does not need any such condition to be satisfied. Using block wise DFT, Ling and Solé [8] showed that in some cases quasi-cyclic codes can be constructed by well known construction methods from lower length codes.

In this chapter the structural properties of quasi-cyclic codes are investigated in transform domain using n-length DFT of the unblocked codewords. This needs $(n, q) = 1$, an even stronger condition than $(\frac{n}{l}, q) = 1$. In a similar way as in [80], our approach is shown to give useful minimum Hamming distance bound.

The content of this chapter is organized as follows: In the next section, quasi-cyclic codes are characterized in DFT domain. Construction of parity check equations over an extension field from transform domain structure of quasi-cyclic codes is studied in Section 3.3. How such parity check equations can give minimum distance bounds are also discussed in this section. Finally in Section 3.4, the chapter is concluded with some possible directions of further investigation.

3.2 Quasi-Cyclic Codes in Transform Domain

Let F_q denote the finite field of cardinality q. Linear codes over F_q of length n are considered where $(n, q) = 1$. Let l be a positive integer dividing n. A code is called *l-quasi-cyclic* if the code is closed under cyclic shift by l symbols. Obviously, l=1 gives cyclic codes. Throughout the chapter only linear quasi-cyclic codes are discussed.

Let r be the smallest positive integer such that $n|(q^r - 1)$ and $\alpha \in F_{q^r}$ be an element of order n. Then DFT and inverse DFT of n-length vectors are defined in usual manner.

For any $j \in [0, n-1]$, the *residue class modulo $\frac{n}{l}$* of j, denoted by $(j)_{n,l}$, is defined as

$$(j)_{n,l} = \{i \in [0, n-1] | j \equiv i \bmod \tfrac{n}{l}\}.$$

Cardinality of $(j)_{n,l}$ is l for all $j \in [0, n-1]$. If a vector is cyclically shifted l times, every transform component in a residue class modulo $\frac{n}{l}$ is multiplied by same scalar.

Like q-cyclotomic coset modulo n, on the same set $[0, n-1]$, let us define *q-cyclotomic coset modulo $\frac{n}{l}$* of j, denoted by $[j]_{\frac{n}{l}}$, as

$$[j]_{\frac{n}{l}} = \{i \in [0, n-1] | j \equiv iq^t \bmod \tfrac{n}{l} \text{ for some non-negative integer } t\}.$$

Let us define the *length of* $[j]_{\frac{n}{l}}$ as the number of elements in it that are less than $\frac{n}{l}$. The length of $[j]_n$ is same as it's size and will be denoted by r_j. Note that the length of $[j]_{\frac{n}{l}}$ is the same as the length of $[jl]_n$ and hence is denoted by r_{lj}. Clearly, $r_{lj} = r_{lk}$ if $[j]_{\frac{n}{l}} = [k]_{\frac{n}{l}}$ and $r_j = r_k$ if $[j]_n = [k]_n$. Each cyclotomic coset modulo $\frac{n}{l}$ of $[0, n-1]$ corresponds to a cyclotomic coset modulo $\frac{n}{l}$ of $[0, \frac{n}{l} - 1]$. Suppose $S = [j]_{\frac{n}{l}} \cap [0, \frac{n}{l} - 1]$. Then clearly $[j]_{\frac{n}{l}} = S \cup (S + \frac{n}{l}) \cup \cdots \cup (S + (l-1)\frac{n}{l})$. So, $|[j]_{\frac{n}{l}}| = l|S| = lr_{lj}$.

Clearly, a q-cyclotomic coset modulo $\frac{n}{l}$ is union of some q-cyclotomic cosets modulo n. If $J \subseteq [0, n-1]$, we write $[J]_n = \cup_{j \in J} [j]_n$ and $[J]_{\frac{n}{l}} = \cup_{j \in J} [j]_{\frac{n}{l}}$

Example 3.2.1. In $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, the cyclotomic cosets modulo 9 and modulo $\frac{9}{3} = 3$ are

$$[0]_9 = \{0\}; [1]_9 = \{1, 2, 4, 5, 7, 8\}; [3]_9 = \{3, 6\}$$

and

$$[0]_3 = \{0, 3, 6\}; [1]_3 = \{1, 2, 4, 5, 7, 8\} .$$

The length of the cyclotomic cosets modulo 9 are same as the size of these sets, whereas the length of $[0]_3$ is 1 and not same as it's size. Similarly, the length of $[1]_3$ is 2 whereas it's size is 6.

Let $\mathcal{C}$ be a linear l-quasi-cyclic code and $\mathcal{C}_D = \{DFT(\mathbf{a})|\mathbf{a} \in \mathcal{C}\}$. From the definition of linear quasi-cyclic codes and the cyclic shift property, it follows that $\mathcal{C}_D$ should satisfy the following two properties:

1. $\mathcal{C}_D$ is a vector space over F_q.
2. If $\mathbf{A} \in \mathcal{C}_D$ and $\mathbf{B} \in F_{q^r}^n$ such that $B_j = \alpha^{lj} A_j$ for $j = 0, 1, \cdots, n-1$, then $\mathbf{B} \in \mathcal{C}_D$.

The second property above leads to

Theorem 3.2.1. *Let $J = \{j_1, j_2, \cdots, j_l\} \subseteq I_n$ be a residue class modulo $\frac{n}{l}$ with $j_1 < j_2 < \cdots < j_l$. The set of ordered tuples of transform components A_J of all the codewords of a linear l-quasi-cyclic code is an $F_{q^{r_{lj_1}}}$-subspace of $F_{q^{r_{j_1}}} \times F_{q^{r_{j_2}}} \times \cdots \times F_{q^{r_{j_l}}}$.*

However A_J can not take values from arbitrary $F_{q^{r_{lj_1}}}$-subspace. The subspace should conform with the conjugacy constraints on the components. As an example, consider binary 3-quasi-cyclic codes of length 9. The set $\{0, 3, 6\}$ is a residue class modulo 3. The 3-tuple (A_0, A_3, A_6) should take values from an F_2-subspace V of $F_2 \times F_4 \times F_4$ such that any vector $x = (x_1, x_2, x_3) \in F_2 \times F_4 \times F_4$ satisfies $x_3 = x_2^2$.

If $\mathcal{C}$ is m-quasi-cyclic and $S \subset F_{q^r}$ is α^{lj}-invariant, then clearly the subcode obtained by restricting the j^{th} transform component to S is also m-quasi-cyclic. If the nonzero transform components can be partitioned into two mutually unrelated and disjoint subsets, then clearly, the code is the direct sum of the two subcodes obtained by restricting each subset of transform components to zero. In particular, for two mutually unrelated subsets of the form S and S^c where $S^c = [0, n-1] \setminus S$, we have $\mathcal{C} = \mathcal{C}_S \bigoplus \mathcal{C}_{S^c}$. A quasi-cyclic code is called *minimal* if it does not contain any proper nonzero quasi-cyclic subcode.

Note that when specialized to l=1, Theorem 3.1 reduces to the well known fact for cyclic codes: the set of values taken by A_j is either $\{0\}$ or $F_{q^{r_j}}$. In the case of cyclic codes components of transform vectors from two different $[j_1]_n$ and $[j_2]_n$ can never be related to each other. Whereas for l-quasi-cyclic codes they can be related provided $[j_1]_n$ and $[j_2]_n$ are in the same cyclotomic coset modulo $\frac{n}{l}$ [Theorem 3.2.4]. Notice that when m=1, the set of cyclotomic cosets modulo n and modulo $\frac{n}{m}$ are identical and there is no room to relate transform components of different cyclotomic cosets.

In the following subsection minimal quasi-cyclic codes are discussed and the general case is discussed in the next subsection.

3.2.1 Minimal Quasi-Cyclic Codes

In a minimal quasi-cyclic code, for any $j \in [0, n-1]$, A_j should take values from a minimal α^{lj}-invariant subspace, since otherwise, A_j can be restricted to a minimal α^{lj}-invariant subspace to get a proper quasi-cyclic subcode.

Now, consider any $j, k \in [0, n-1]$ such that none of A_j and A_k are zero for all the codewords of a minimal l-quasi-cyclic code $\mathcal{C}$. Suppose A_j and A_k take values from the minimal α^{lj}-invariant and α^{lk}-invariant subspaces V_{lj} and V_{lk} respectively. Since the code is minimal, if A_j is restricted to $\{0\}$, then the subcode obtained is the zero code. Since the code is linear, for any other element β in V_{lj}, there is only one codeword in $\mathcal{C}$ with $A_j = \beta$. This is true for any nonzero transform component in $\mathcal{C}$. So, A_j and A_k are related by a linear invertible map of V_{lj} onto V_{lk}. But because the code is quasi-cyclic, arbitrary linear invertible map can not relate two nonzero transform components.

The following two lemmas will help to identify the possible linear invertible maps, connecting two nonzero transform components in a minimal quasi-cyclic code.

Lemma 3.2.2. *Let $\sigma : F_{q^t} \rightarrow F_{q^t}$ be an F_q-linear invertible map and β and β' two elements of F_{q^t} with cardinality of their conjugacy classes t. If $\sigma(\beta a) = \beta' \sigma(a)$ $\forall a \in F_{q^t}$, then, $\beta' = \beta^{q^t}$ for some $t < t$ and $\sigma : a \longmapsto c a^{q^t}$ $\forall a \in F_{q^t}$ for some unique $c \in F_{q^t}$.*

Proof: Any map of F_{q^t} into F_{q^t} is induced by a unique polynomial over F_{q^t} of degree at most $q^t - 1$ [81]. Let the polynomial $f_\sigma(X) = \sum_{i=0}^{q^t-1} c_i X^i \in F_{q^t}[X]$ be such that $\sigma(a) = f_\sigma(a)$ $\forall a \in F_{q^t}$. In this case, $c_0 = 0$ since $f_\sigma(0) = \sigma(0) = 0$.

For any $s \in F_{q^t}$, define the permutation $\lambda_s : F_{q^t} \longrightarrow F_{q^t}$ as $\lambda_s : a \longmapsto sa$.

By hypotheses,

$$\sigma \lambda_\beta = \lambda_{\beta'} \sigma \tag{3.1}$$

Clearly,

$$f_{\sigma\lambda_\beta}(X) = \sum_{i=1}^{q^t-1} c_i \beta^i X^i$$

and

$$f_{\lambda_{\beta'}\sigma}(X) = \sum_{i=1}^{q^t-1} c_i \beta' X^i$$

Equation (3.1) implies

$$\begin{aligned} c_i\beta^i &= c_i\beta' \text{ for } i = 1, 2, \cdots, q^t - 1 \\ \Rightarrow \beta^i &= \beta' \text{ whenever } c_i \neq 0 \end{aligned}$$

If, for some $i_1 \leq q^t - 1$, we have $c_{i_1} \neq 0$, then $f_\sigma(X) = c_{i_1}X^{i_1} + \cdots$.

Since σ is F_q-linear, we have

$$\begin{aligned} & \sigma(sa) = s\sigma(a) \ \ \forall s \in F_q \text{ and } \forall a \in F_{q^t} \\ \Rightarrow \quad & \sigma\lambda_s = \lambda_s\sigma \ \ \forall s \in F_q \\ \Rightarrow \quad & c_{i_1}s^{i_1} = sc_{i_1} \ \ \forall s \in F_q \\ \Rightarrow \quad & s = s^{i_1} \ \ \forall s \in F_q \\ \Rightarrow \quad & i_1 = q^{t_1} \text{ for some } t_1 < t. \end{aligned}$$

Suppose, $\exists\, i_1 = q^{t_1}$, $i_2 = q^{t_2}$, $t_1, t_2 < t$, such that $c_{i_1}, c_{i_2} \neq 0$. Then,

$$\begin{aligned} \beta' &= \beta^{q^{t_1}} = \beta^{q^{t_2}} \\ &\Rightarrow t|(t_2 - t_1) \\ &\Rightarrow t_2 = t_1 \end{aligned}$$

So, there is only one nonzero term in $f_\sigma(X)$ and that is of degree $q^{t'}$ for some positive integer $t' < t$ and thus the lemma follows. ∎

Lemma 3.2.3. *Let β and β' be two elements of F_{q^r} such that lengths of their conjugacy classes are both t, and sF_{q^t} and $s'F_{q^t}$ be two β and β'-invariant subspaces in F_{q^r}. Suppose $\sigma : sF_{q^t} \longrightarrow s'F_{q^t}$ is an F_q linear invertible map. Then σ satisfies $\sigma(\beta a) = \beta'\sigma(a)$ if and only if $\beta' = \beta^{q^{t'}}$ and $f_\sigma(X) = cX^{q^{t'}}$ for some unique $c \in s's^{-q^{t'}}F_{q^t}$ and $t' < t$.*

Proof: The reverse implication is trivial. So only the forward implication is proved here.

Let us define a map $\sigma' : F_{q^t} \longrightarrow F_{q^t}$ as $\sigma' : a \longmapsto (s')^{-1}\sigma(sa)$. Clearly, σ' is an F_q-linear map and

$$\begin{aligned} \sigma'(\beta a) &= (s')^{-1}\sigma(s\beta a) \\ &= (s')^{-1}\beta'\sigma(sa) \\ &= \beta'\sigma'(a) \end{aligned}$$

So by lemma 3.2.2, $\beta' = \beta^{q^{t'}}$ for some $t' < t$ and $f_{\sigma'}(X) = c'X^{q^{t'}}$ for some $c' \in F_{q^t}$.

By definition of σ', $\sigma(a) = s'\sigma'(s^{-1}a)$; $\quad \forall a \in sF_{q^t}$ and so, $f_\sigma(X) = s'f_{\sigma'}(s^{-1}X) = s's^{-q^{t'}}c'X^{q^{t'}} = cX^{q^{t'}}$ where $c = s's^{-q^{t'}}c'$. ■

The following theorem identifies the relations between transform components of different cyclotomic cosets modulo n that give minimal l-quasi-cyclic codes.

Theorem 3.2.4. *In an n-length minimal l-quasi-cyclic code, transform components in only one cyclotomic coset modulo $\frac{n}{l}$, say $[j]_{\frac{n}{l}}$, is nonzero and any two nonzero transform components A_{j_1} and A_{j_2}, where $j_1, j_2 \in [j]_{\frac{n}{l}}$ and $[j_1]_n \neq [j_2]_n$, are related by an isomorphism σ with $f_\sigma(X) = cX^{q^t}$ for some unique $c \in F_{q^r}$, where t is such that $j_2 \equiv j_1 q^t$ mod $\frac{n}{l}$. If A_{j_1} and A_{j_2} take values from $sF_{q^{r_{lj}}}$ and $s'F_{q^{r_{lj}}}$ respectively, then c is from $s's^{-q^t}F_{q^{r_{lj}}}$.*

Proof: In a minimal quasi-cyclic code, if A_{j_1} and A_{j_2} are nonzero, then A_{j_1} and A_{j_2} take values from minimal α^{lj_1} and α^{lj_2}-invariant subspaces of $F_{q^{r_{j_1}}}$ and $F_{q^{r_{j_2}}}$ respectively, and A_{j_2} is dependent on A_{j_1} by an F_q-linear invertible map σ, i.e., $A_{j_2} = \sigma A_{j_1}$. Since the code is l-quasi-cyclic, σ should satisfy $\sigma(\alpha^{lj_1}a) = \alpha^{lj_2}\sigma(a)$. So, by using Lemma (3.2.3) with $\beta = \alpha^{lj_1}$ and $\beta' = \alpha^{lj_2}$, we see that $lj_2 \equiv lj_1 q^t$ mod n for some $t < r_{lj_1}$, i.e., lj_2 and lj_1 are in same cyclotomic coset modulo n or equivalently, j_2 and j_1 are in same cyclotomic coset modulo $\frac{n}{l}$. So, in a minimal quasi-cyclic code, transform components are nonzero only in one cyclotomic coset modulo $\frac{n}{l}$. Moreover, again by Lemma (3.2.3), if $j_2 \equiv j_1 q^t$ mod $\frac{n}{l}$, then the isomorphism σ is given by $f_\sigma(X) = cX^{q^t}$ for some $c \in F_{q^r}$. ■

Example 3.2.2. Consider length n=9, binary (q=2), 3-quasi-cyclic codes($l = 3$). The cyclotomic cosets modulo n are $\{0\}, \{3, 6\}$ and $\{1, 2, 4, 5, 7, 8\}$ and the cyclotomic cosets modulo $\frac{n}{l} = 3$ are $\{0, 3, 6\}$ and $\{1, 2, 4, 5, 7, 8\}$. The number of minimal α^{lj}-invariant subspaces in $F_{q^{r_j}}$ is given by $\frac{q^{r_j}-1}{q^{r_{lj}}-1}$. For the example under consideration these values are tabulated in Table 1 for all cyclotomic cosets. (The double vertical lines demarcate cyclotomic cosets modulo $\frac{n}{l}$ and the single vertical lines further demarcates cyclotomic cosets modulo n in the cyclotomic cosets modulo $\frac{n}{l}$.) The minimal codes with non-zeros only in the cyclotomic coset $\{1, 2, 4, 5, 7, 8\}$ can not be connected to any other cyclotomic cosets and there are 21 such codes each corresponding to one α^3-invariant subspace in F_{2^6}. Table 3.3 in page 50 shows all other minimal 3-quasi-cyclic codes possible. There is one minimal 3-quasi-cyclic code ($\mathcal{C}_1$ in Table 3.3) with DFT coefficients taking nonzero values only in the cyclotomic coset $\{0\}$ modulo 9, and there are three ($\mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4$ in Table 3.3 with DFT coefficients taking nonzero values only in $\{3, 6\}$. There are three minimal 3-quasi-cyclic codes in which DFT coefficients in $\{0\}$ and $\{3, 6\}$ are nonzero and related. These are $\mathcal{C}_5, \mathcal{C}_6, \mathcal{C}_7$ in Table 3.3, and the relations are given by $A_3 = cA_0^{2^t}$ where $t = 0$ and the value of c are respectively 1, α^{21} and α^{42}. For comparison the total number of minimal cyclic codes (l=1) is given at the bottom of the table.

Table 3.1: Details pertaining to Examples 3.2.2 and 3.2.3

Cyclotomic Cosets modulo $\frac{n}{m}$	$\{0,3,6\}$		$\{1,2,4,8,7,5\}$	$\{0,5,10\}$		$\{1,2,3,4,6,7,8,9,11,12,13,14\}$			$\{0,3,6,9,12\}$		$\{1,2,4,5,7,8,10,11,13,14\}$		
Length of $[j]_{3j}$ $= r_{3j}$	1		2	1		4			1		2		
Cyclotomic Cosets modulo n	$\{0\}$	$\{3,6\}$	$\{1,2,4,8,7,5\}$	$\{0\}$	$\{5,10\}$	$\{1,2,4,8\}$	$\{3,6,12,9\}$	$\{7,14,13,11\}$	$\{0\}$	$\{3,6,12,9\}$	$\{1,2,4,8\}$	$\{7,14,13,11\}$	$\{5,10\}$
Length of $[j]_9$ ne $= r_j$	1	2	6	1	2	4	4	4	1	4	4	4	2
Number of min. α^{3j}-invariant subspaces in $F_{q^{r_j}} = \frac{q^{r_j}-1}{q^{r_{3j}}-1}$	1	3	21	1	3	1	1	1	1	15	5	5	1
# of min. quasicyclic codes with unrelated transform components	1	3	21	1	3	1	1	1	1	15	5	5	1
# of min. quasicyclic codes with related transform components	3		0	3		270			15		330		
Total# of min. quasicyclic codes	28			280					372				
Total# of min. cyclic codes	3			5					5				

The relations in the above example for codes with related transform components turn out to be simple and straightforward. To exemplify more than two cyclotomic cosets modulo n being related the following example is given.

Example 3.2.3. Consider binary codes of length 15. We have l-quasi-cyclic codes for l=3 and l=5. For both these values the cyclotomic cosets and possible minimal quasi-cyclic codes are classified in Table 1. In Table 3.4 in page 50, the codewords and their transform vectors for four minimal 5-quasi-cyclic codes with different cyclotomic cosets modulo n related are listed. For the code $\mathcal{C}_1$, the cyclotomic cosets $\{7, 11, 13, 14\}$ and $\{1, 2, 4, 8\}$ are related and the relation is $A_7 = \alpha^7 A_1$, that is $t = 0$ and $c = \alpha^7$. The relations for the codes $\mathcal{C}_2$ and $\mathcal{C}_3$ are respectively $A_5 = \alpha^6 A_1^2$ and $A_7 = \alpha^3 A_5^2$. The code $\mathcal{C}_4$ has been obtained by relating the three cyclotomic cosets $\{1, 2, 4, 8\}$, $\{5, 10\}$ and $\{7, 11, 13, 14\}$. The relations are $A_5 = \alpha^{11} A_1^2$ and $A_7 = \alpha^3 A_1$.

Clearly, any nonzero vector is contained in a minimal quasi-cyclic code if and only if DFT of the vector is nonzero only in one cyclotomic coset modulo $\frac{n}{l}$. That minimal quasi-cyclic code is spanned by the l-shifts of the vector.

3.2.2 Arbitrary Quasi-Cyclic Codes

Let $\mathcal{C}$ be an arbitrary quasi-cyclic code and suppose A_j is nonzero for $\mathcal{C}$ and takes values from an α^{lj}-invariant subspace V of $F_{q^{r_j}}$. Let V_1 and V_2 be two α^{lj}-invariant subspaces of V such that $V = V_1 + V_2$. If $\mathcal{C}_1$ and $\mathcal{C}_2$ are the quasi-cyclic subcodes obtained by restricting A_j in the subspaces V_1 and V_2 respectively, then clearly, $\mathcal{C} = \mathcal{C}_1 + \mathcal{C}_2$. (However if $V = V_1 \oplus V_2$, then $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2$ need not be true. In fact, $\mathcal{C}_1 \cap \mathcal{C}_2$ is the subcode of $\mathcal{C}$ obtained by restricting the transform component A_j to $\{0\}$.) By successively doing this, we can decompose the code as sum of a family of subcodes, each of which has any nonzero transform component A_j taking values from some minimal α^{lj}-invariant subspace. Now, let us consider one such code (which is a subcode of the original code). Let $\{j_1, j_2, \cdots, j_t\}$ be a set of representatives of different cyclotomic cosets modulo n, where transform components are nonzero in the code. We construct a subset L of $\{j_1, j_2, \cdots, j_t\}$ as follows. First assign $L = \{j_1\}$. Suppose A_{j_l} takes values from the minimal α^{lj_l}-invariant subspace V_{j_l}. In the subcode obtained by restricting A_{j_1} to 0, A_{j_2} will take values from either V_{j_2} or 0. If it takes values from 0, then clearly, A_{j_2} is related to A_{j_1} by an isomorphism. Otherwise, A_{j_1} and A_{j_2} take values independently and in that case keep j_2 in L. Next

Table 3.3: Minimal 3-quasi-cyclic codes of Example 3.2.2

	Codewords									DFT								
	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
$\mathcal{C}_1$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
$\mathcal{C}_2$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	1	1	0	1	1	0	1	1	0	0	0	1	0	0	1	0	0
$\mathcal{C}_3$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	1	0	1	1	0	1	1	0	0	0	0	α^{21}	0	0	α^{42}	0	0
$\mathcal{C}_4$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	1	1	0	1	1	0	1	0	0	0	α^{42}	0	0	α^{21}	0	0
$\mathcal{C}_5$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0
$\mathcal{C}_6$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	1	0	0	1	0	0	1	1	0	0	α^{21}	0	0	α^{42}	0	0
$\mathcal{C}_7$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	1	0	0	1	0	0	1	0	1	0	0	α^{42}	0	0	α^{21}	0	0

Table 3.4: Codes of Example 3.2.3

	Codewords															DFT														
	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	A_{14}
$\mathcal{C}_1$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	1	1	0	1	1	1	1	0	1	1	0	0	0	α	α^2	0	α^4	0	0	α^8	α^8	0	0	α^4	0	α^2	α
	0	1	1	1	1	0	1	1	0	0	0	0	0	1	1	0	α^6	α^{12}	0	α^9	0	0	α^{13}	α^3	0	0	α^{14}	0	α^7	α^{11}
	0	1	1	0	0	0	0	0	1	1	0	1	1	1	1	0	α^{11}	α^7	0	α^{14}	0	0	α^3	α^{13}	0	0	α^9	0	α^{12}	α^6
$\mathcal{C}_2$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	1	1	1	1	0	1	1	1	0	1	0	0	0	1	0	α^2	α^4	0	α^8	α^{10}	0	0	α	0	α^5	0	0	0	0
	0	1	1	1	0	1	0	0	0	1	1	1	1	1	1	0	α^7	α^{14}	0	α^{13}	α^5	0	0	α^{11}	0	α^{10}	0	0	0	0
	1	0	0	0	1	1	1	1	1	1	0	1	1	1	0	0	α^{12}	α^9	0	α^3	1	0	0	α^6	0	1	0	0	0	0
$\mathcal{C}_3$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	1	1	1	1	1	0	0	0	1	0	1	1	1	0	0	0	0	0	0	1	0	α^3	0	0	1	α^9	0	α^{12}	α^6
	0	1	1	1	0	1	1	1	1	1	1	0	0	0	1	0	0	0	0	0	α^5	0	α^{13}	0	0	α^{10}	α^{14}	0	α^7	α^{11}
	1	0	0	0	1	0	1	1	1	0	1	1	1	1	1	0	0	0	0	0	α^{10}	0	α^8	0	0	α^5	α^4	0	α^2	α
$\mathcal{C}_4$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	1	1	1	1	0	0	1	1	1	0	1	0	0	0	0	α^2	α^4	0	α^8	1	0	α^5	α	0	1	α^{10}	0	α^5	α^{10}
	0	1	0	0	0	0	1	1	1	1	0	0	1	1	1	0	α^{12}	α^9	0	α^3	α^5	0	1	α^6	0	α^{10}	1	0	1	1
	0	0	1	1	1	0	1	0	0	0	0	1	1	1	1	0	α^7	α^{14}	0	α^{13}	α^{10}	0	α^{10}	α^{11}	0	α^5	α^5	0	α^{10}	α^5

restrict all the transform components indexed by elements of L to 0 and check a transform component A_{j_l} not yet considered. If its values vary over V_{j_l}, then put j_l in L. Continuing this way, we'll get a set L such that all the transform components indexed by its elements takes values independently and values of all other transform components are determined by them.

Note that in the process of construction of L, the minimality of V_{j_l}'s are used and consequently such a subset L may not exist when V_{j_l}'s are not minimal α^{lj_l}-invariant subspaces. Now, we can decompose the subcode as direct sum of $|L|$ codes, each one of which is obtained by restricting all but one transform components indexed by L to zero. Clearly, each subcode thus obtained is a minimal code. So, any quasi-cyclic code can be decomposed as sum of some minimal quasi-cyclic codes. Just taking a minimal family of such minimal subcodes such that their sum is the original code, we can express the code as direct sum of some minimal quasi-cyclic codes. So we have,

Theorem 3.2.5. *Any quasi-cyclic code can be decomposed as direct sum of some minimal quasi-cyclic codes.*

Theorem 3.2.5 was first proved in [5]. Note that decomposition of a quasi-cyclic code in terms of some minimal quasi-cyclic codes is not unique, though for l=1, that is for cyclic codes such a decomposition is unique.

For a minimal l-quasi-cyclic code, transform components in different cyclotomic classes modulo $\frac{n}{l}$ are unrelated. So, by Theorem 3.2.5 it is also true for any l-quasi-cyclic code. This gives the following characterization of l-quasi-cyclic codes in transform domain.

Theorem 3.2.6. *A code $\mathcal{C}$ is l-quasi-cyclic iff*

- *Transform components in different cyclotomic cosets modulo $\frac{n}{l}$ are mutually unrelated.*
- *For any $j \in [0, \frac{n}{l}-1]$, $A_{(j)_{n,l}}$ takes values from an $F_{q^{r_{lj}}}$-subspace of $F_{q^{r_j}} \times F_{q^{r_{j+\frac{n}{l}}}} \times \cdots \times F_{q^{r_{j+(l-1)\frac{n}{l}}}}$.*

Though the decomposition of an l-quasi-cyclic code is not unique in general, by first part of Theorem 3.2.6, any G-invariant code can be decomposed uniquely as direct sum of some l-quasi-cyclic codes, each having nonzero transform components only in some distinct cyclotomic class modulo $\frac{n}{l}$. So we have,

Theorem 3.2.7. *Let Λ_i, $i = 1, 2, \cdots, t$ be the distinct cyclotomic cosets modulo $\frac{n}{l}$ of $[0, n-1]$. Then,*

$$\mathcal{C} = \bigoplus_{i=1}^{t} \mathcal{C}_{\Lambda_i} \tag{3.2}$$

The unique subcodes $\mathcal{C}_{\Lambda_i}$'s in (3.2), obtained by considering each cyclotomic coset modulo $\frac{n}{l}$ are actually the primary components [7] or irreducible components [5] of the code. In [7], primary components of $\mathcal{C}$ were obtained as $\frac{X^{\frac{n}{l}}-1}{f_i(X)}.\mathcal{C}$, where $f_i(X)$ are the irreducible factors of $X^{\frac{n}{l}}-1$. To see the bridge, note that $\frac{n}{l}$-length DFT of $\frac{X^{\frac{n}{l}}-1}{f_i(X)}$ is nonzero in exactly one cyclotomic coset modulo $\frac{n}{l}$, say $[0, \frac{n}{l}] \cap [j]_{\frac{n}{l}}$. So, n-length DFT of $\frac{X^n-1}{f_i(X^l)}$ is nonzero in exactly one cyclotomic coset modulo $\frac{n}{l}$, namely $[j]_{\frac{n}{l}}$, because if $k \equiv lq^t \bmod \frac{n}{l}$, then k-th component of n-length DFT of $\frac{X^n-1}{f_i(X^l)}$ is $\frac{\alpha^{kn}-1}{f_i(\alpha^{kl})} = \frac{\alpha^{lq^t n}-1}{f_i(\alpha^{lq^t l})} = \frac{(\alpha^l)^{lq^t \frac{n}{l}}-1}{f_i\left((\alpha^l)^{lq^t}\right)} = lq^t$-th component of $\frac{n}{l}$-length DFT of $\frac{X^{\frac{n}{l}}-1}{f_i(X)}$. So, multiplying $\frac{X^{\frac{n}{l}}-1}{f_i(X)}$ to $\mathcal{C}$, which is same as multiplying $\frac{X^n-1}{f_i(X^l)}$ to $\mathcal{C}$ in unblocked form, is equivalent to 'zeroing out' the transform components in all but one cyclotomic coset modulo $\frac{n}{l}$, that is $[j]_{\frac{n}{l}}$. Thus $\mathcal{C}_{\Lambda_i}$'s are the primary components of the code.

Let us consider one subcode $\mathcal{C}_{\Lambda_i}$. Let $j_{i,1}, j_{i,2}, \cdots, j_{i,k_i}$ be the representatives of the different cyclotomic cosets modulo n in Λ_i. Now, in any quasi-cyclic code, this set of representatives can be uniquely partitioned into some subsets such that transform components corresponding to these subsets are mutually unrelated and any subset can not further be partitioned in the same way. Let $\{j_{i,1}, j_{i,2}, \cdots, j_{i,k_i}\} = \cup_{l=1}^{s_i} \Lambda_{i,l}$ be the partition. Then the code $\mathcal{C}_{\Lambda_i}$ can further be decomposed as direct sum of s_i subcodes $\mathcal{C}_{\Lambda_{i,1}}, \mathcal{C}_{\Lambda_{i,2}}, \cdots, \mathcal{C}_{\Lambda_{i,s_i}}$, where $\mathcal{C}_{\Lambda_{i,l}}$ is obtained by restricting all the transform components of $\mathcal{C}_{\Lambda_i}$ except those indexed by elements of $[\Lambda_{i,l}]_n$ to zero. Then, we have the unique decomposition

$$\mathcal{C} = \bigoplus_{i=1}^{t} \bigoplus_{l=1}^{s_i} \mathcal{C}_{\Lambda_{i,l}} \tag{3.3}$$

Notice that in the unique decomposition of $\mathcal{C}$ in (3.3), the subcodes $\mathcal{C}_{\Lambda_{i,l}}$ are not necessarily minimal and moreover these are not necessarily uniquely decomposable into minimal quasi-cyclic codes. For example, consider the three length 9 binary 3-quasi-cyclic codes $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_5$ listed in Table 2. Direct sum of any two of these three give the same code, which has nonzero transform components in one cyclotomic coset modulo $\frac{n}{l}$ and is decomposable in three different ways. In [7], the authors give a systematic way to get a decomposition of the subcodes $\mathcal{C}_{\Lambda_i}$ using Groebner bases.

Given any subset $S \subseteq F_q^n$, the intersection of all the quasi-cyclic codes containing S is called the quasi-cyclic code generated by S. A code generated by a single vector is called a one-generator quasi-cyclic code [7, 54, 55]. Note that for a one generator quasi-cyclic code, each component $\mathcal{C}_{\Lambda_i}$ (see equation (3.2)) is either zero or minimal, since it is generated by the vector whose DFT components in the corresponding cyclotomic coset modulo $\frac{n}{l}$ are same as that of $\mathbf{a}$ and all other DFT components are zero.

If a minimal quasi-cyclic code takes nonzero DFT values in $[j]_{\frac{n}{l}}$, then it's dimension is r_{lj}. Suppose there are t cyclotomic cosets modulo $\frac{n}{l}$. If j is in the i-th cyclotomic coset modulo $\frac{n}{l}$, then let us denote r_{lj} as t_i. Considering the dimension, $\mathcal{C}_{\Lambda_i}$ can be direct sum of at most l minimal quasi-cyclic codes (or cyclic irreducible codes as is called in [5, 7]). The number of ways $\mathcal{C}_{\Lambda_i}$ of dimension $l_i t_i$ can be chosen is thus given by $\prod_{h=0}^{l_i-1} \frac{q^{lt_i}-q^{ht_i}}{q^{l_it_i}-q^{ht_i}}$, where empty product is assumed to be 1. So, the total number of distinct l-quasi-cyclic codes of length n is given by $\sum_{l_0=0}^{l} \sum_{l_1=0}^{l} \cdots \sum_{l_t=0}^{l} \prod_{i=1}^{t} \left(\prod_{h=0}^{l_i-1} \frac{q^{lt_i}-q^{ht_i}}{q^{l_it_i}-q^{ht_i}} \right)$. This formula was originally derived in [5]. From the values of l_i's for a code, lot of structural informations can be known. As example, if $\max_i l_i = l$, then one needs at least l generators to generate the code. So, for one-generated code, $l_i = 1$ or 0 and at least one l_i is 1. A one-generated code is minimal iff the generator has nonzero transform components in exactly one cyclotomic coset modulo $\frac{n}{l}$. Dimension of a one generated code is given by $\sum t_i$ where the summation is over the cyclotomic cosets modulo $\frac{n}{l}$ where DFT components of the generator are not all zeros, that is, where corresponding primary components of the code is nonzero. In [6, 7], the dimension of the quasi-cyclic code generated by the single generator in blocked polynomial form $(g^{(0)}(X), g^{(1)}(X), \cdots, g^{(l-1)}(X))$ is derived to be $\frac{n}{l} - deg(gcd(g^{(0)}(X), g^{(1)}(X), \cdots, g^{(l-1)}(X), X^{\frac{n}{l}} - 1))$. The fact that both the formulas are actually same can be realized just by noting that t_i's are actually degrees of the irreducible factors of $X^{\frac{n}{l}} - 1$.

3.3 Parity Check Matrix and Minimum Distance Bound

As discussed in the previous two chapter, a lower bound on the minimum Hamming distance of a code can be obtained from a set of parity check equations over an extension field. In the following, it is shown how one can get a set of parity check equations over an extension field from the transform domain description of a quasi-cyclic code.

For an arbitrary $j \in I_{\frac{n}{l}}$, suppose $A_{(j)_{n,l}}$ takes values from an $F_{q^{r_{lj}}}$-subspace V of $F_{q^{r_j}} \times F_{q^{r_{j+\frac{n}{l}}}} \times \cdots \times F_{q^{r_{j+(l-1)\frac{n}{l}}}}$. Then V is the null space of a system of $F_{q^{r_{lj}}}$-linear equations of the form

$$\sum_{i=0}^{l-1} Tr_i \left(c_i A_{j+i\frac{n}{l}}\right) = 0 \tag{3.4}$$

where Tr_i is the $F_{q^{r_{j+i\frac{n}{l}}}}/F_{q^{r_{lj}}}$-trace:

$$\begin{array}{rccc} Tr_i: & F_{q^{r_{j+i\frac{n}{l}}}} & \longrightarrow & F_{q^{r_{lj}}} \\ & x \mapsto & & x + x^q + \cdots + x^{q^{l_i}} \end{array}$$

where $l_i = \frac{r_{j+i\frac{n}{l}}}{r_{lj}}$. Now equation (3.4) can be rewritten as

$$\begin{aligned} & \sum_{i=0}^{l-1} \sum_{k=0}^{l_i-1} \left(c_i A_{j+i\frac{n}{l}}\right)^{q^k} = 0 \\ \Rightarrow & \sum_{i=0}^{l-1} \sum_{k=0}^{l_i-1} c_i^{q^k} \sum_{t=0}^{n-1} \alpha^{t(j+i\frac{n}{l})q^k} a_t = 0 \\ \Rightarrow & \sum_{t=0}^{n-1} \left(\sum_{k=0}^{l_i-1} \left(\sum_{i=0}^{l-1} c_i \alpha^{t(j+i\frac{n}{l})} \right)^{q^k} \right) a_t = 0 \end{aligned}$$

This gives a parity check equation over F_{q^r} for the code.

The component wise conjugate vectors of the parity check vectors obtained in these ways and the vectors in their span are also parity check vectors of the code.

Example 3.3.1. Consider an $l = 3$-quasi-cyclic code of length $n = 9$ over F_2 given by the frequency domain restriction $A_1 \in \beta^{-3} F_4$, where $\beta = X$ is a primitive element (F_{64} is constructed as $F[X]/(X^6 + X + 1)$ and the DFT is defined over F_{64} with the DFT kernel $\alpha = \beta^7$). Note that conjugacy constraints allow A_1 to take any value from F_{64}. But in this particular quasi-cyclic code, A_1 takes values from a minimal α^3-invariant subspace. The restriction $A_1 \in \beta^{-3} F_4$ gives the parity check vector:

$$\begin{aligned} \mathbf{h} &= \left(\left(\beta^3 \alpha^i\right)^4 - \beta^3 \alpha^i \right)_{i=0 \ to \ 8} \\ &= \left(\beta^{48}, \beta^{56}, \beta^7, \beta^6, \beta^{14}, \beta^{28}, \beta^{27}, \beta^{35}, \beta^{50}\right) \end{aligned}$$

Components of $\mathbf{h}$ are distinct and nonzero and $\mathbf{h}^2$, being a component wise conjugate of $\mathbf{h}$, is also a parity check vector of the code. So, Theorem 2.5.1 guarantees a minimum

Hamming distance at least 3 for the code. So, it is a $[9, 5, \geq 3]$ code. If we impose the further condition $A_0 = 0$, then we get another parity check vector $\mathbf{h}^0 = (1, 1, \cdots, 1)$ and as a result we get a $[9, 4, \geq 4]$ code.

3.4 Discussion

In this chapter, a generalization of the well known DFT domain characterization of cyclic codes over finite fields is obtained. It is shown that for minimal l-quasi-cyclic length n codes, transform components in different cyclotomic cosets modulo n are related (not possible for cyclic codes) provided they are in the same cyclotomic cosets modulo $\frac{n}{l}$, and have identified all possible relations. For non-minimal quasi-cyclic codes the decomposition in terms of minimal quasi-cyclic codes is discussed. A way to get minimum distance bound for quasi-cyclic codes in terms of the minimum distance of a BCH code is shown. Decoding algorithm for a corresponding BCH code can be used to decode the quasi-cyclic code upto that minimum distance. However, this technique is difficult to apply for long codes.

Chapter 4

Codes Closed under Arbitrary Abelian Group of Permutations

4.1 Introduction

Codes with rich algebraic structure are of strong interest to coding theorists due to the ease of design and decoding. Classical families of cyclic codes like BCH codes and Reed-Muller codes were the center of attraction for a long time. For a cyclic code, the code's permutation group contains a cyclic subgroup generated by the cyclic permutation. A linear cyclic code can also be viewed as an ideal of the group algebra on the cyclic group of order n (length of the code). More generally, ideals of group algebras on abelian groups are known as abelian codes. Alternatively, the abelian codes on an abelian group G can be considered as the linear codes closed under the action of a transitive abelian group of permutations, which is isomorphic to G. Abelian codes were studied using DFT in [37, 91].

A different direction of generalization gives another class of codes: quasi-cyclic codes. A code of length n is said to be l-quasi-cyclic for some $l|n$ if every l times cyclic shift of a codeword is also a codeword. The permutation group of an l-quasi-cyclic code contains a cyclic group (of order $\frac{n}{l}$) of permutations generated by 'l times cyclic shift'. For any vector $(a_0, a_1, \cdots, a_{n-1})$, if every l-th position is blocked together to rearrange the symbols as $\Big((a_0, a_l, \cdots, a_{(\frac{n}{l}-1)l}), (a_1, a_{l+1}, \cdots, a_{(\frac{n}{l}-1)l+1}), \cdots, (a_{l-1}, a_{2l-1}, \cdots, a_{n-1})\Big)$, then the code is l-quasi-cyclic if block-wise cyclically shifted version $((a_l, a_{2l}, \cdots, a_0), (a_{l+1}, a_{2l+1}, \cdots, a_1), \cdots, (a_{2l-1}, a_{3l-1}, \cdots, a_{l-1}))$ of every codeword $((a_0, a_l, \cdots, a_{(\frac{n}{l}-1)l}), (a_1, a_{l+1}, \cdots, a_{(\frac{n}{l}-1)l+1}), \cdots, (a_{l-1}, a_{2l-1}, \cdots, a_{n-1}))$ is also a codeword. So an l-quasi-cyclic code can be viewed as

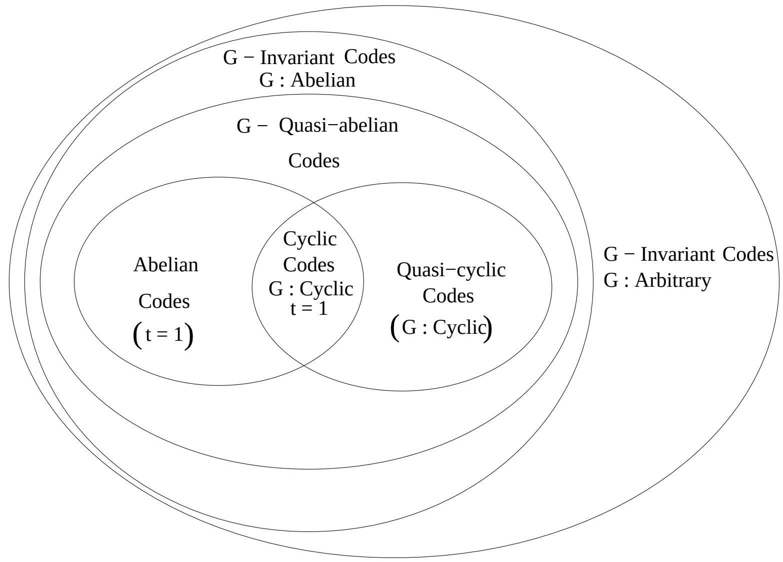

Figure 4.1: Different families of codes and their defining groups of permutations

a submodule of the l dimensional free module $(F_qC_{\frac{n}{l}})^l$ over the group algebra $F_qC_{\frac{n}{l}}$ where $C_{\frac{n}{l}}$ is a cyclic group of order $\frac{n}{l}$. Clearly, if an l-quasi-cyclic code has the additional structure that it is also closed under the cyclic shift of the blocks, i.e. $((a_1, a_{l+1}, \cdots, a_{(\frac{n}{l}-1)l+1}), (a_2, a_{l+2}, \cdots, a_{(\frac{n}{l}-1)l+2}), \cdots, (a_0, a_l, \cdots, a_{(\frac{n}{l}-1)l}))$ is also a codeword for every codeword $((a_0, a_l, \cdots, a_{(\frac{n}{l}-1)l}), (a_1, a_{l+1}, \cdots, a_{(\frac{n}{l}-1)l+1}), \cdots, (a_{l-1}, a_{2l-1}, \cdots, a_{n-1}))$, then the code is an abelian code on the abelian group $C_l \times C_{\frac{n}{l}}$.

A more general but not so popular class of codes is the class of quasi-abelian codes [9]. For an abelian group G and it's subgroup H, a subspace of the group algebra F_qG which is closed under the action of elements of H, i.e. which is an F_qH module, is called a quasi-abelian code. In fact, for an abelian group H and any positive integer t, any submodule of $(F_qH)^t$ can be considered as a quasi-abelian codes. In that case, any abelian $G \supseteq H$ with $|G| = t|H|$ can be used to define quasi-abelian code as in [9]. So, we'll call such codes as H-quasi-abelian codes. When $t = 1$, this class specializes to abelian codes and when H is a cyclic group, it specializes to quasi-cyclic codes.

In this chapter, the algebraic structure of codes closed under any arbitrary abelian subgroup G of S_n (group of permutations of n elements) is investigated. We call this class as G-invariant codes. These codes are precisely those which have G as a subgroup of their permutation groups. When special types of G are taken, G-invariant codes coincide with the class of quasi-abelian codes and thus with the classes of quasi-cyclic codes and

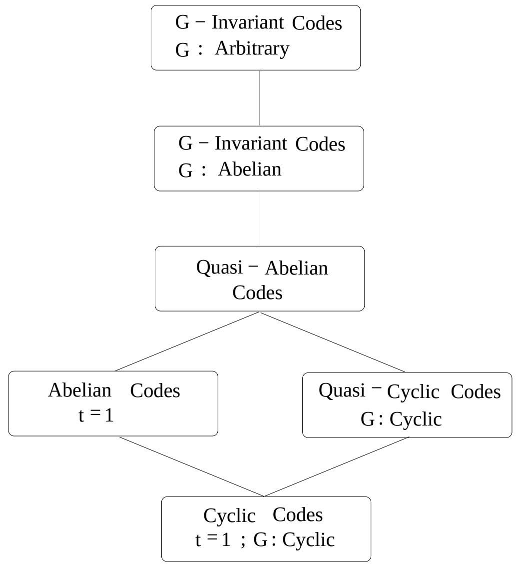

Figure 4.2: Different families of codes and their defining groups of permutations

abelian codes. Figure 4.1 and Figure 4.2 show the relations between different types of codes. Figure 4.1 shows special cases as subsets of the general cases using Venn diagram, whereas Figure 4.2 shows the special cases below the general cases. Note that a G-quasi-abelian code is also H-quasi-abelian for any subgroup $H \subseteq G$. If a cyclic subgroup H is taken, then G-invariant codes are also $\frac{n}{|H|}$-quasi-cyclic codes. So, G-quasi-abelian codes for any G are quasi-cyclic codes for some index. But by considering them only as $\frac{n}{|H|}$-quasi-cyclic codes, neglect some known additional structure of the codes would be neglected. The figures show different classes of codes as G-invariant codes for specific types of G. In the figures, t denotes the number of orbits of the co-ordinate positions under the action of G. The type of G, for which G-invariant codes can be seen as G-quasi-abelian codes will be specified in Section 4.8.

The following are the examples of different types of permutation groups G shown in Figure 4.1 and 4.2. The corresponding figures show the cycle structure of a set of generators of the permutation groups. Whenever the set of generators consists of two generators σ_1 and σ_2, the solid lines with arrows represent the cycles of σ_1 and the dashed lines with arrows represent the cycles of σ_2.

Example 4.1.1. For any $a, b \in F_q$; $a \neq 0$, let $\sigma_{a,b}$ denote the permutation $\sigma_{a,b} : x \mapsto ax + b$. Then $G = \{\sigma_{a,b} | a \in F_q^*, b \in F_q\}$ is a subgroup of S_q (the symmetric group on q letters) and is called the group of affine permutations. For $q > 2$, this group is non-abelian and the corresponding G-invariant codes are known as affine invariant codes.

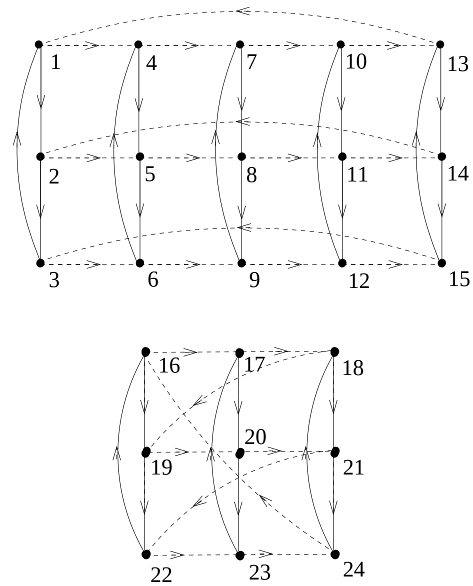

Figure 4.3: Cycle structure of the generators of G in Example 4.1.2

Example 4.1.2. Figure 4.3 shows cycle structure of the generators σ_1 and σ_2 of a permutation group $G = \langle \sigma_1, \sigma_2 \rangle \subseteq S_{24}$. Here G is abelian but G-invariant codes can not be seen as G-quasi-abelian codes.

Example 4.1.3. Figure 4.4 shows cycle structure of the generator σ_1 of a permutation group $G = \langle \sigma_1 \rangle \subseteq S_{16}$. For the time being, ignore the dashed boxes in the figure. Here G is abelian with exponent 15. The index set has 4 orbits under the action of G. Here also G-invariant codes can not be seen as G-quasi-abelian codes.

Example 4.1.4. Figure 4.5 shows cycle structure of the generators σ_1 and σ_2 of a permutation group $G = \langle \sigma_1, \sigma_2 \rangle \subseteq S_{54}$. Here G is abelian and G-invariant codes are same as G-quasi-abelian codes.

Example 4.1.5. Figure 4.6 shows cycle structure of the generator σ_1 of a permutation group $G = \langle \sigma_1 \rangle \subseteq S_{9l}$. For the time being, ignore the dashed boxes in the figure. Here G is abelian and G-invariant codes are same as l-quasi-cyclic codes.

Example 4.1.6. Figure 4.7 shows cycle structure of the generators σ_1 and σ_2 of a permutation group $G = \langle \sigma_1, \sigma_2 \rangle \subseteq S_{27}$.Here $G = \langle \sigma_1 \rangle \times \langle \sigma_2 \rangle = Z_3 \times Z_9$ is abelian and G-invariant codes are same as G-abelian codes.

Example 4.1.7. Figure 4.8 shows cycle structure of the generator σ_1 of a permutation group $G = \langle \sigma_1 \rangle \subseteq S_5$. Here G is abelian and G-invariant codes are same as cyclic codes.

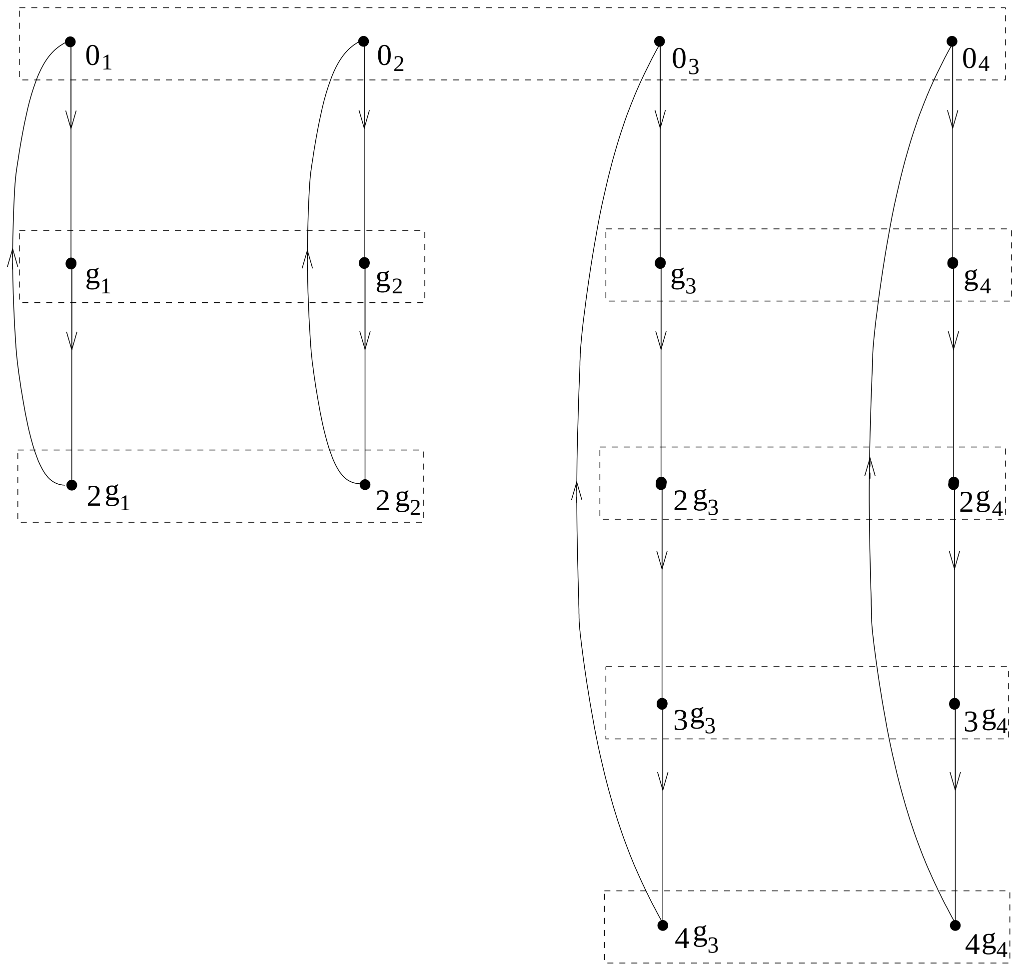

Figure 4.4: Cycle structure of the generator of G in Example 4.1.3

It is known that all cyclic codes of length n are decomposable as direct sum of minimal cyclic codes if and only if n is relatively prime to q. Similarly all abelian codes on an abelian group is decomposable as direct sum of minimal abelian codes if and only if the exponent of the abelian group is relatively prime to q. Same is true for l-quasi-cyclic codes if and only if $\frac{n}{l}$ is relatively prime to q [5]. In all these cases, the condition for decomposability turns out to be the mutual prime-ness of q and the exponent of the defining abelian group of permutations under which the code is closed. We'll show that this is true for any G-invariant code (G abelian), i.e., for an abelian subgroup $G \subseteq S_n$, any G-invariant code of length n can be decomposed as direct sum of minimal G-invariant codes if and only if the exponent of G is relatively prime to q.

Karlin [64] showed a way to decode a class of one-generator quasi-cyclic codes. Heijnen and van Tilborg [65] proposed another decoding technique for the class of one-generator

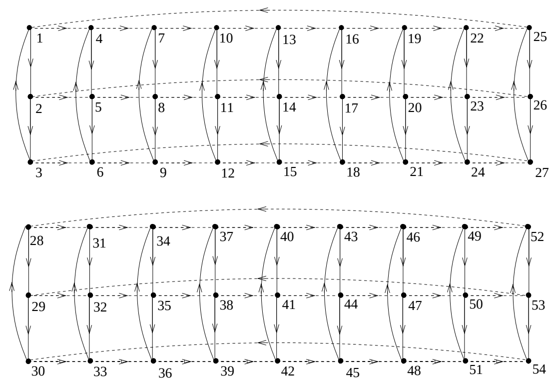

Figure 4.5: Cycle structure of the generators of G in Example 4.1.4

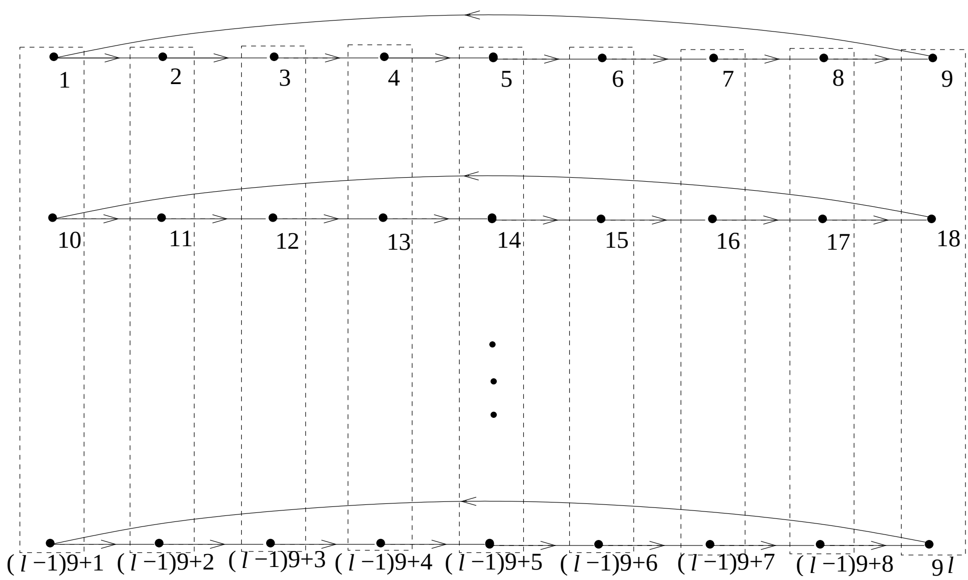

Figure 4.6: Cycle structure of the generator of G in Example 4.1.5

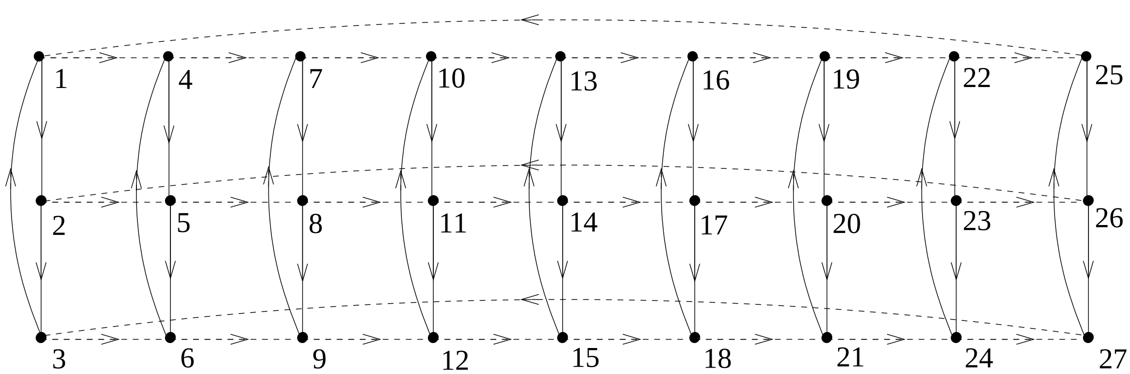

Figure 4.7: Cycle structure of the generators of G in Example 4.1.6

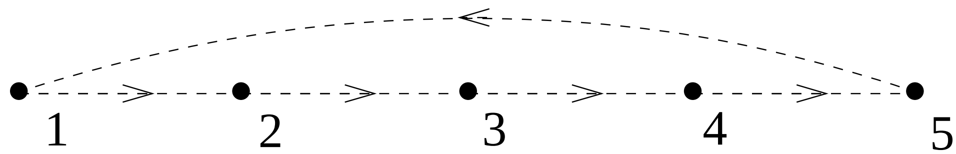

Figure 4.8: Cycle structure of the generator of G in Example 4.1.7

quasi-cyclic codes, which uses the same basic idea but achieves some computational advantages by better usage of the quasi-cyclic property of the code. In this chapter, Karlin's approach is extended to a class of quasi-cyclic codes, not necessarily one-generator. When restricted to one-generator quasi-cyclic codes, this method reduces to Karlin's method. Moreover, our method also applies to a class of quasi-abelian codes specified in subsection 4.8.1.

In Section 4.2, the DFT on abelian group is discussed which is used in Section 4.3 to define a DFT for G-invariant codes for any abelian group G of permutations with exponent relatively prime to q. Such G-invariant codes are characterized in the transform domain and their structural properties are investigated in section 4.4. Dual codes of G-invariant codes and self dual G-invariant codes are characterized in section 4.5 and 4.6. The number of G-invariant self dual codes for any abelian group G is also found. In section 4.7, Tanner's approach for getting a bound on the minimum distance from a set of parity check equations over an extension field is extended and how it can be used to get a minimum distance bound for G-invariant codes is outlined. Characterization of quasi-abelian codes is obtained as a special case of the characterization of G-invariant codes in Section 4.8. Karlin's approach [64] for decoding systematic quasi-cyclic codes with parity circulants in single row is extended to the case of systematic quasi-abelian codes. In particular, this can be used to decode systematic quasi-cyclic codes with columns of parity circulants in the generator matrix, i.e. systematic quasi-cyclic codes which are not necessarily 1-generated, the case which was left open by Kerlin. In Subsection 4.5.3, all the results in [92] regarding the existence/number of self-dual quasi-cyclic codes are shown to follow as special cases of the results in Section 4.5.

4.2 Review of the DFT for Abelian Codes

In this section, the DFT for abelian codes is revisited. There are more than one equivalent ways of presenting it. Here, the DFT is presented in terms of character tables for the sake of notational simplicity in the later sections, where the DFT for abelian codes will be extended to study abelian group invariant codes.

Let ν be the exponent of G and r be the smallest integer such that $\nu|(q^r - 1)$, i.e. such that F_{q^r} contains a primitive ν-th root of unity. Then the group of all distinct F_{q^r} characters is isomorphic to G. In fact an isomorphism $x \mapsto \psi_{(x)}$ can be chosen (see for example [37] and the references in it) such that $\psi_{(x)}(y) = \psi_{(y)}(x)$. We denote $\psi_{(x)}(y)$ as $\psi(x, y)$, considering it as a map $\psi : G \times G \to F_{q^r}$. It satisfies the following properties:

$$\psi(x, yz) = \psi(x, y)\psi(x, z) \tag{4.1a}$$

$$\psi(x, y) = \psi(y, x) \tag{4.1b}$$

$$(\psi(x, y) = \psi(x', y),\ \forall y \in G) \iff x = x' \tag{4.1c}$$

$$\sum_{x \in G} \psi(x, y) = \begin{cases} |G|, & \text{if } y = 1 \\ 0, & \text{if } y \neq 1 \end{cases} \tag{4.1d}$$

where $|G|$ and 1 denote respectively the cardinality of G and the identity element in G.

The DFT of any element $\mathbf{a} = \sum_{x \in G} a_x x \in F_q G$ is defined as $\mathbf{A} \in F_{q^r} G$ such that $A_x = \sum_{y \in G} \psi(x, y) a_y$. The inverse DFT is given by $a_x = |G|^{-1} \sum_{y \in G} \psi(x, y)^{-1} A_y$.

This DFT satisfies the following two properties:

1. **Conjugacy Constraint:** For any $\mathbf{a} \in F_q G$, it's DFT $\mathbf{A}$ satisfies $A_{x^q} = A_x^q$.

2. For some fixed $y \in G$, if $\mathbf{b} \in F_q G$ such that $b_x = a_{yx}$, then the DFT $\mathbf{B}$ is given by $B_x = \psi(x, y)^{-1} A_x$.

Definition 6. For any $x \in G$, the subset $[x]^q \triangleq \{y \in G | y = x^{q^t}$ for some non-negative $t\}$ is called the **q-cyclotomic coset** (or simply **cyclotomic coset**) of x. For any subset $S \subseteq G$, define $[S]^q \triangleq \cup_{s \in S} [s]^q$.

Clearly, $[x]^q = \{x, x^q, \cdots, x^{q^{r_x - 1}}\}$, where r_x is the smallest positive integer satisfying $x^{q^{r_x}} = x$ and is called length or exponent of $[x]^q$. The cyclotomic coset $[x^{-1}]^q$ will be called the **inverse** or **reciprocal cyclotomic coset** of $[x]^q$. If $[x]^q = [x^{-1}]^q$, then it will be called a **self inverse** or **self reciprocal cyclotomic coset**.

Example 4.2.1. In Example 4.1.6, the components can be reindexed with elements from $G \simeq Z_9 \times Z_3$. With this indexing, the self reciprocal and other cyclotomic cosets for different q are as follows.

$q \equiv 2$ or 5 mod 9 [e.g $q = 2,\ 32$] The cyclotomic cosets in G for this case are shown in Table 4.1.

Cyclotomic cosets in G	Type	r_x
$\{(0,0)\}$	self-reciprocal	1
$\{(1,0),(2,0),(4,0),(8,0),(7,0),(5,0)\}$	self-reciprocal	6
$\{(0,1),(0,2)\}$	self-reciprocal	2
$\{(1,1),(2,2),(4,1),(8,2),(7,1),(5,2)\}$	self-reciprocal	6
$\{(2,1),(4,2),(8,1),(7,2),(5,1),(1,2)\}$	self-reciprocal	6
$\{(3,1),(6,2)\}$	self-reciprocal	2
$\{(3,2),(6,1)\}$	self-reciprocal	2
$\{(3,0),(6,0)\}$	self-reciprocal	2

Table 4.1: Cyclotomic cosets of different types for $q \equiv 2$ or 5 mod 9 [e.g $q = 2,\ 32$]

$q \equiv 1$ mod 9 [e.g $q = 64$] All the cyclotomic cosets of G are singletons and all except $(0,0)$ are not self-reciprocal.

$q \equiv 4$ or 7 mod 9 [e.g $q = 4,\ 16$] The cyclotomic cosets in G for this case are shown in Table 4.2.

$q \equiv 8$ mod 9 [e.g $q = 8$] The cyclotomic cosets in G for this case are shown in Table 4.3.

For any element in F_qG, the DFT components in a q-cyclotomic coset are related by the conjugacy constraint and $A_x \in F_{q^{r_x}}$. For an abelian code, i.e., any ideal of F_qG, A_x is zero or takes all possible values from $F_{q^{r_x}}$.

4.3 DFT for G-Invariant Codes

We consider codes over F_q of length n. Suppose the code symbols are indexed by a finite set I, where $|I| = n$. Let $G \subseteq Perm(I)$ be an abelian subgroup of the group of permutations of I. We shall denote by p, the cardinality of the prime subfield of F_q.

Let $I_1, \cdots, I_t$ be the orbits of I under the action of G, that is, G acts on each of

Cyclotomic cosets in G	reciprocal cyclotomic coset	Type	r_x
$\{(0,0)\}$	$\{(0,0)\}$	self-reciprocal	1
$\{(1,0),(4,0),(7,0)\}$	$\{(2,0),(8,0),(5,0)\}$	not self-reciprocal	3
$\{(2,0),(8,0),(5,0)\}$	$\{(1,0),(4,0),(7,0)\}$	not self-reciprocal	3
$\{(0,1)\}$	$\{(0,2)\}$	not self-reciprocal	1
$\{(0,2)\}$	$\{(0,1)\}$	not self-reciprocal	1
$\{(1,1),(4,1),(7,1)\}$	$\{(2,2),(8,2),(5,2)\}$	not self-reciprocal	3
$\{(2,2),(8,2),(5,2)\}$	$\{(1,1),(4,1),(7,1)\}$	not self-reciprocal	3
$\{(2,1),(8,1),(5,1)\}$	$\{(4,2),(7,2),(1,2)\}$	not self-reciprocal	3
$\{(4,2),(7,2),(1,2)\}$	$\{(2,1),(8,1),(5,1)\}$	not self-reciprocal	3
$\{(3,1)\}$	$\{(6,2)\}$	not self-reciprocal	1
$\{(6,2)\}$	$\{(3,1)\}$	not self-reciprocal	1
$\{(3,2)\}$	$\{(3,2)\}$	not self-reciprocal	1
$\{(6,1)\}$	$\{(3,2)\}$	not self-reciprocal	1
$\{(3,0)\}$	$\{(6,0)\}$	not self-reciprocal	1
$\{(6,0)\}$	$\{(3,0)\}$	not self-reciprocal	1

Table 4.2: Cyclotomic cosets of different types for $q \equiv 4$ or 7 mod 9 [e.g $q = 4$, 16]

$I_1, \cdots, I_t$ transitively and $I = I_1 \cup I_2 \cup \cdots \cup I_t$. Let us denote

$$G_k = \{g^{(k)} | g \in G\} \text{ for } k = 1, \cdots, t.$$

where $g^{(k)} \triangleq g|_{I_k} \in Perm(I_k)$ is the permutation g restricted to I_k. Since G_k is abelian and G_k acts on I_k faithfully and transitively, stabilizer of any $i \in I_k$ is $\{1_k\}$ (1_k denotes the identity element of G_k). Because, if H is the stabilizer of $i \in I_k$, then the stabilizer of any other element $i_1 = g(i)$, $g \in G$ is $gHg^{-1} = H$. So, $H = \{1_k\}$, since G_k acts faithfully on I_k. So, for any $i_1 \in I_k$, there is a unique $g \in G_k$, such that $i_1 = g(i)$; that is, the action of G_k on I_k is sharply 1-transitive. This defines a $1-1$ correspondence between G_k and I_k. Using this, the symbols can be indexed by elements of G_k instead of I_k by first associating a fixed element $i \in I_k$ with the identity element 1_k. Hence, the code symbols are indexed by elements of $\mathcal{G} \triangleq \cup_{i=1}^{t} G_i$ instead of I. Then the element g of G acts on $\mathcal{G}$ as $x \overset{g}{\mapsto} g^{(k)}x$ when $x \in G_k$. For any $\mathbf{a} \in F_q^I \simeq F_q^{\mathcal{G}}$, $g \in G$ acts on $\mathbf{a}$ as $\mathbf{a} \overset{g}{\mapsto} \mathbf{b} = g(\mathbf{a})$ such that $b_x = a_{g^{(k)-1}x}$, where $x \in G_k$. Henceforth, we'll use the letters f, g and h, possibly with subscripts, to denote elements of G and the letters x, y and z to denote elements of $\mathcal{G}$.

Any abelian group can be decomposed as direct product of some cyclic subgroups of prime power order. For any prime p_1 dividing order of G, let p_1^l be the highest power of p_1 such that there is a cyclic subgroup of G of order p_1^l. Then p_1^l is the maximum

Cyclotomic cosets in G	Type	r_x
$\{(0,0)\}$	self-reciprocal	1
$\{(1,0),(8,0)\}$	self-reciprocal	2
$\{(2,0),(7,0)\}$	self-reciprocal	2
$\{(4,0),(5,0)\}$	self-reciprocal	2
$\{(0,1),(0,2)\}$	self-reciprocal	2
$\{(1,1),(8,2)\}$	self-reciprocal	2
$\{(2,2),(7,1)\}$	self-reciprocal	2
$\{(4,1),(5,2)\}$	self-reciprocal	2
$\{(2,1),(7,2)\}$	self-reciprocal	2
$\{(4,2),(5,1)\}$	self-reciprocal	2
$\{(8,1),(1,2)\}$	self-reciprocal	2
$\{(3,1),(6,2)\}$	self-reciprocal	2
$\{(3,2),(6,1)\}$	self-reciprocal	2
$\{(3,0),(6,0)\}$	self-reciprocal	2

Table 4.3: Cyclotomic cosets of different types for $q \equiv 8 \bmod 9$ [e.g $q = 8$]

power of p_1 which divides the exponent of G. Let g be a generator of that cyclic subgroup and $h = g^{p_1^{l-1}}$ be an element of order p_1 in that cyclic subgroup. There is at least one k such that $h^{(k)} \neq 1_k$, since G acts faithfully on $\mathcal{G}$. Then $h^{(k)} = \left(g^{(k)}\right)^{p_1^{l-1}}$ has order p_1 and thus $g^{(k)}$ has order p_1^l. So, p_1^l divides exponent of G_k. So, the exponent of G, $exp(G) = lcm\left(\{exp(G_k) | k = 1, \cdots, t\}\right)$.

Let the exponent of G be relatively prime to q. Then on each orbit, DFT can be defined as discussed in the last section. For any $\mathbf{a} \in F_q^{\mathcal{G}}$, DFT is defined orbit wise. That is, the DFT of $\mathbf{a}$ is defined as $\mathbf{A}$, where

$$A_x = \sum_{y \in G_k} \psi_k(x,y) a_y \qquad \forall x \in G_k,\ \forall k.$$

Here ψ_k is as defined in the last section, for G_k. For any code $\mathcal{C} \subset F_q^{\mathcal{G}}$, let us denote $\mathcal{D}_{\mathcal{C}} = \{DFT(\mathbf{a}) | \mathbf{a} \in \mathcal{C}\}$. Clearly, the DFT components A_x are in F_{q^r}, where r is the smallest positive integer such that $exp(G)$ divides $q^r - 1$.

Definition 7. For any two $x, y \in \mathcal{G}$, define

$$\Psi(x,y) = \begin{cases} \psi_k(x,y), & \text{when } x, y \in G_k \text{ for some } k \\ 0, & \text{when } x \in G_{k_1} \text{ and } y \in G_{k_2} \text{ s. t. } k_1 \neq k_2 \end{cases}$$

With this notation, the DFT can be re-written as

$$A_x = \sum_{y \in \mathcal{G}} \Psi(x,y) a_y \qquad \forall x \in \mathcal{G}. \tag{4.2}$$

Definition 8. For any $h \in G$, and $x \in \mathcal{G}$ Let us define the symbol

$$\langle h, x\rangle \triangleq \psi_k(h^{(k)}, x) \quad \text{when } x \in G_k. \tag{4.3}$$

It follows from this definition that the DFT of $\mathbf{b} = h(\mathbf{a})$ is given by $B_x = \langle h, x\rangle A_x$.

Lemma 4.3.1. *Suppose $h_1, h_2 \in G_k$. Then $\langle g, h_1\rangle^l = \langle g, h_2\rangle \; \forall g \in G$ if and only if $h_1^l = h_2$.*

Proof: Trivial using (4.1a) and (4.1c). ∎

For any element $x \in \mathcal{G}$, it is in G_k for some k and so cyclotomic coset of x is defined in the same way as in the previous section as $[x]^q \triangleq \{y \in G_k | y = x^{q^t} \text{ for some non-negative } t\}$. Similarly, r_x will denote the cardinality of $[x]^q$.

Corollary 4.3.2. *For any $x \in \mathcal{G}$, r_x is the smallest positive integer such that $\langle g, x\rangle^{q^{r_x}} = \langle g, x\rangle \; \forall g \in G$.*

So, r_x is the *lcm* of the lengths of the conjugacy classes of $\langle g, x\rangle\,; \forall g \in G$.

Definition 9. The **residue class** of $x \in \mathcal{G}$ is defined as

$$\widetilde{x} \triangleq \{x_1 \in \mathcal{G} | \langle g, x_1\rangle = \langle g, x\rangle \text{ for each } g \in G\}. \tag{4.4}$$

We'll denote the cardinality of $\widetilde{x}$ by e_x. Clearly, all the elements of a residue class are from different orbits. But there may not be elements from all the orbits in a single residue class.

Example 4.3.1 *(Continuation of Example 4.1.3).* The index set has 4 orbits under the action of G and $G_1 \simeq G_2 \simeq Z_3$ and $G_3 \simeq G_4 \simeq Z_5$. Let a set of generators of the groups G_1, G_2, G_3 and G_4 be g_1, g_2, g_3 and g_4 respectively. If $\alpha \in F_{q^r}$ is an element of order 15, then we define DFT in $F_q^{16} \simeq F_q^{\mathcal{G}}$ with respect to the maps ψ_k defined by:

$$\psi_1(g_1, g_1) = \alpha^5$$
$$\psi_2(g_2, g_2) = \alpha^5$$
$$\psi_3(g_3, g_3) = \alpha^3$$
$$\psi_4(g_4, g_4) = \alpha^3$$

The residue classes in $\mathcal{G}$ are shown in Figure 4.4 with dashed boxes.

For an l-quasi-cyclic code of length ml, the code is closed under the cyclic shift by l positions. If the permutation 'cyclic shift by l positions' is denoted by σ, after a suitable co-ordinate permutation, the cycle decomposition of σ can be written as $(0\ 1\ \cdots\ m-1)(m\ m+1\ \cdots\ 2m-1)\cdots((l-1)m\ (l-1)m+1\ \cdots\ ml-1)$. Clearly, $G = \langle\sigma\rangle \simeq Z_m$ and $G_k \simeq Z_m$ for each orbit. So, the same DFT can be applied to each orbit and then the residue classes are nothing but the residue classes modulo m.

Example 4.3.2. (Continuation of Example 4.1.5) The dashed boxes in Figure 4.6 show the residue classes modulo 9 for l-quasi-cyclic codes of length $9l$.

For any subset $X = \{x_1, x_2, \cdots, x_k\} \subseteq \mathcal{G}$, A_X denotes the ordered tuple $(A_{x_1}, A_{x_2}, \cdots, A_{x_k})$ where an arbitrary fixed order in X is assumed. In particular, for any residue class $\widetilde{y_1} = \{y_1, y_2, \cdots, y_l\}$, we'll denote by $A_{\widetilde{y}}$, the ordered l-tuple $(A_{y_1}, A_{y_2}, \cdots, A_{y_l})$ with an arbitrarily chosen fixed order on $\widetilde{y}$. For some ordered tuples $T_1 = (t_{11}, \cdots, t_{1,j_1}), \cdots, T_l = (t_{l,1}, \cdots, t_{l,j_l})$ the concatenated tuple $(t_{11}, \cdots, t_{1,j_1}, \cdots, t_{l,1}, \cdots, t_{l,j_l})$ is denoted as $(T_1, \cdots, T_l)$.

Definition 10. The **cyclotomic residue class** of $x \in \mathcal{G}$ is defined as

$$\begin{aligned}(x)^q &\triangleq \{x_1 \in \mathcal{G} |\text{ for some non-negative t, } \langle g, x_1\rangle^{q^t} = \langle g, x\rangle\ \forall g \in G\} \qquad (4.5)\\ &= [\widetilde{x}]^q.\end{aligned}$$

Clearly, all the residue classes in a cyclotomic residue class are of same cardinality. Figure 4.9 shows the relations between cyclotomic cosets, residue classes and cyclotomic residue classes. By the conjugacy constraint, values of DFT components in one residue class determines values of other transform components in the same cyclotomic residue class. To be specific, $A_{\widetilde{x^{q^i}}} = A_{\widetilde{x}}^{q^i}$ for any $\mathbf{a} \in F_q^{\mathcal{G}}$, where power of the vector $A_{\widetilde{x}}$ is taken component wise. So, values of transform components in one representative residue class from each cyclotomic residue class specifies a vector completely.

Example 4.3.3 *(Continuation of Example 4.3.1).* The value of q mod 3 determines the cyclotomic cosets in the first two orbits and the value of q mod 5 determines the cyclotomic cosets in the last two orbits.

In the following, cyclotomic cosets, the residue classes and the cyclotomic residue classes are elaborated for different q. For all the cases, the corresponding figures show the cyclotomic cosets with solid boxes and the cyclotomic residue classes with dotted boxes and the residue classes with dashed boxes.

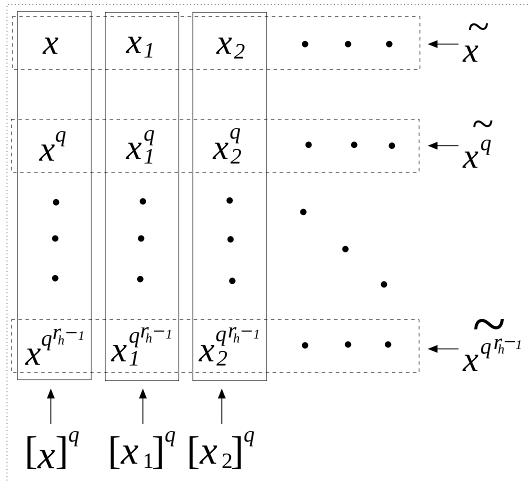

Figure 4.9: A generic cyclotomic residue class $(x)^q$

$q \equiv 2 \bmod 3$, $q \equiv 2$ or $3 \bmod 5$ and $3 \equiv 5 \bmod p$ (e.g. $q = 2, 8$): See Figure 4.10

$q \equiv 1 \bmod 3$, $q \equiv 1 \bmod 5$ and $3 \equiv 5 \bmod p$ (e.g. $q = 16$): See Figure 4.11

$q \equiv 1 \bmod 3$, $q \equiv 4 \bmod 5$ and $3 \equiv 5 \bmod p$ (e.g. $q = 4$): See Figure 4.12

$q \equiv 2 \bmod 3$, $q \equiv 4 \bmod 5$ and $3 \not\equiv 5 \bmod p$ (e.g. $q = 29, 59$): See Figure 4.13

$q \equiv 1 \bmod 3$, $q \equiv 2$ or $3 \bmod 5$ and $3 \not\equiv 5 \bmod p$ (e.g. $q = 7, 13$): See Figure 4.14

Like inverse cyclotomic coset, the **inverse cyclotomic residue class** of $(x)^q$ is defined as $(x^{-1})^q$ and call a cyclotomic residue class, a **self inverse cyclotomic residue class** if it is it's own inverse cyclotomic residue class. Note that a cyclotomic residue class $(x)^q$ is self inverse if and only if the cyclotomic coset $[x]^q$ is self inverse.

In the following, for any subset $S \subseteq F_{q^r} \setminus \{0\}$, we'll denote the multiplicative subgroup of $F_{q^r} \setminus \{0\}$ generated by S as $\langle S \rangle$ and the smallest extension field of F_q containing S as $F_q[S]$. Clearly, $F_q[S] = F_{q^l}$ where l is the smallest positive integer such that $s^{q^l} = s\,; \forall s \in S$. So for any $x \in \mathcal{G}$, Corollary 4.3.2 gives

$$F_q\left[\{\langle g, x \rangle | g \in G\}\right] = F_{q^{r_x}}. \tag{4.6}$$

Lemma 4.3.3. *For any subset $S \subseteq F_{q^r} \setminus \{0\}$, $Span_{F_q}(\langle S \rangle) = F_q[S]$.*

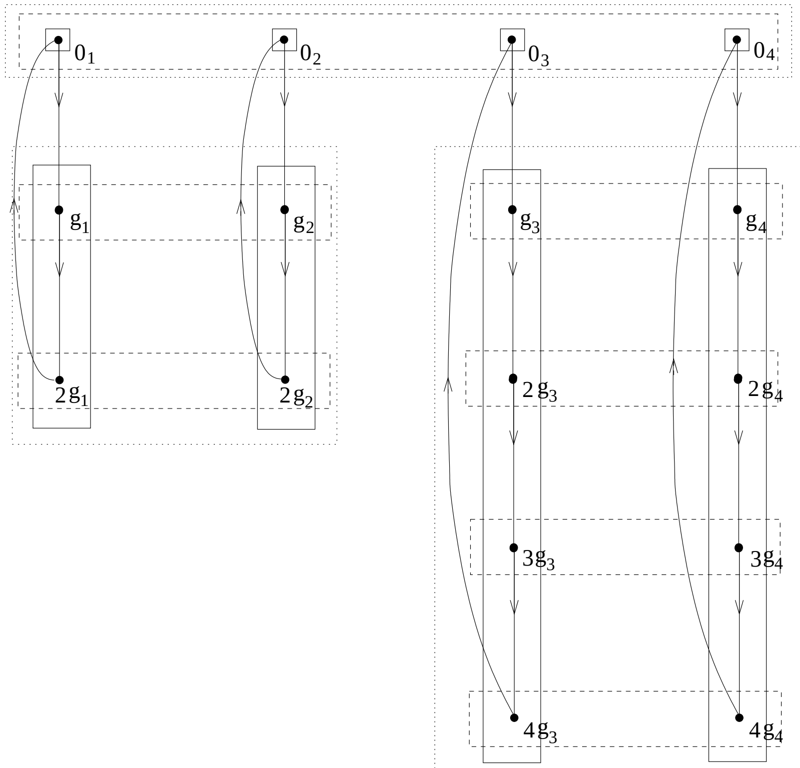

Figure 4.10: The case : $q \equiv 2 \bmod 3$, $q \equiv 2$ or $3 \bmod 5$ and $3 \equiv 5 \bmod p$ (e.g. $q = 2, 8$)

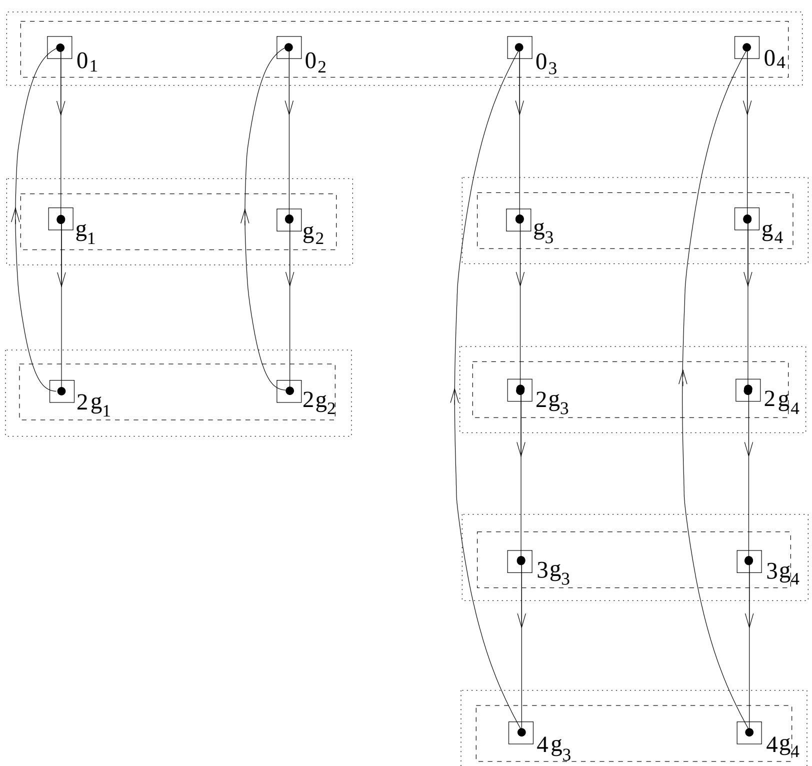

Figure 4.11: The case : $q \equiv 1 \bmod 3$, $q \equiv 1 \bmod 5$ and $3 \equiv 5 \bmod p$ (e.g. $q = 16$)

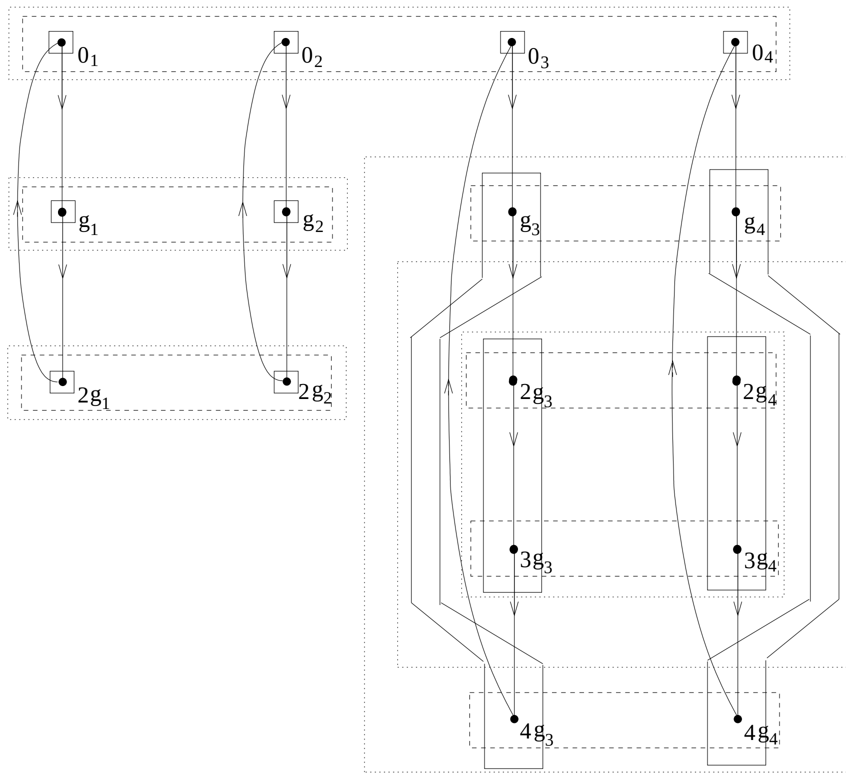

Figure 4.12: $q \equiv 1 \bmod 3$, $q \equiv 4 \bmod 5$ and $3 \equiv 5 \bmod p$ (e.g. $q = 4$)

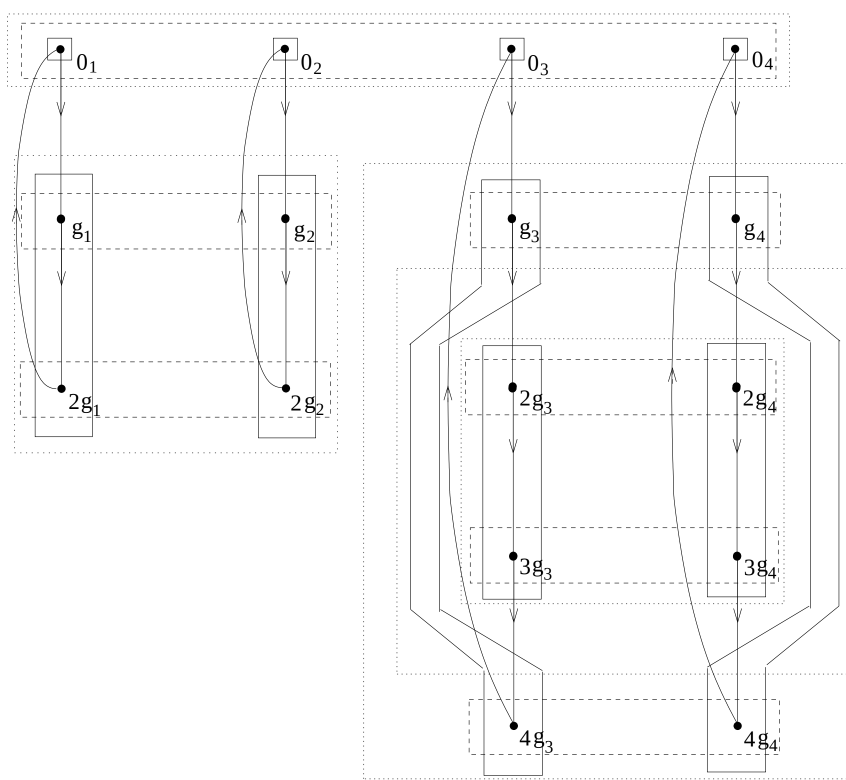

Figure 4.13: $q \equiv 2 \bmod 3$, $q \equiv 4 \bmod 5$ and $3 \not\equiv 5 \bmod p$ (e.g. $q = 29, 59$)

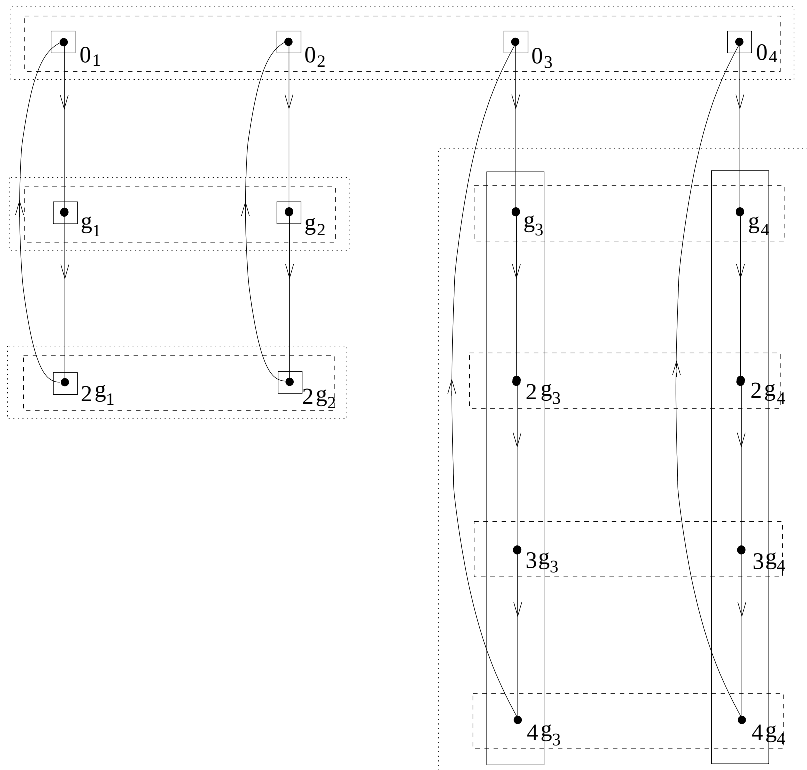

Figure 4.14: $q \equiv 1 \bmod 3$, $q \equiv 2$ or $3 \bmod 5$ and $3 \not\equiv 5 \bmod p$ (e.g. $q = 7, 13$)

Proof: Let us denote $Span_{F_q}(\langle S \rangle)$ by V. Clearly, $V \subseteq F_q[S]$. It is now sufficient to prove that $Span_{F_q}(\langle S \rangle)$ is a subfield of F_{q^r}. Clearly, V is closed under multiplication and $1 \in V$. For any $s \in V \setminus \{0\}$, $s.V = V$ and thus $\exists s_1 \in V$, such that $ss_1 = 1$. So, $s_1 = s^{-1} \in V$. So, inverse of every nonzero element of V is in V and thus V is a field.

4.4 Transform Domain Characterization of G-Invariant Codes

A linear code $\mathcal{C} \subseteq F_q^{\mathcal{G}}$ is G invariant if for every codeword $\mathbf{a} \in \mathcal{C}$ and $h \in G$, $h(\mathbf{a}) \in \mathcal{C}$. The equivalent condition in transform domain is: for any $h \in G$, $\mathbf{A} \in \mathcal{D}_{\mathcal{C}}$ and $\mathbf{B} \in F_{q^r}^{\mathcal{G}}$, $B_x = \langle h, x \rangle A_x \ \forall x \in \mathcal{G} \Rightarrow \mathbf{B} \in \mathcal{D}_{\mathcal{C}}$.

For any ordered tuple $(x_1, x_2, \cdots, x_l)$ on $\mathcal{G}$, we say, $(A_{x_1}, A_{x_2}, \cdots, A_{x_l})$ takes values from
$\{(A_{x_1}, A_{x_2}, \cdots, A_{x_l}) \,|\mathbf{a} \in \mathcal{C}\}$ for $\mathcal{C}$. If for $\mathcal{C}$, $(A_{x_1}, A_{x_2}, \cdots, A_{x_l})$ takes values from $V \subseteq F_{q^r}^l$ and $U \subseteq V$, then the subcode $\{\mathbf{a} \in \mathcal{C} | \, (A_{x_1}, A_{x_2}, \cdots, A_{x_l}) \in U\}$ will be referred as the subcode obtained from $\mathcal{C}$ by restricting $(A_{x_1}, A_{x_2}, \cdots, A_{x_l})$ to U.

Lemma 4.4.1. *For any G-invariant code $\mathcal{C}$ and for any $x \in \mathcal{G}$, $A_{\widetilde{x}}$ takes values from a subspace of $F_{q^{r_x}}^{e_x}$.*

Proof: Suppose $A_{\widetilde{x}}$ takes values from an F_q-subspace (since the code is linear) $V \subseteq F_{q^{r_x}}^{e_x}$ for $\mathcal{C}$. When any element $g \in G$ acts on a codeword $\mathbf{a}$, the e_x-tuple $A_{\widetilde{x}}$ of transform components is multiplied by $\langle g, x\rangle$. Since the code is G-invariant, $\langle g, x\rangle v \in V$ for each $g \in G$ and $v \in V$. So, V is closed under multiplication by $\langle g, x\rangle$; $g \in G$ and thus under multiplication by elements from $Span_{F_q}(\langle\{\langle g, x\rangle | g \in G\}\rangle) = F_q[\{\langle g, x\rangle | g \in G\}] = F_{q^{r_x}}$. So, V is a subspace of $F_{q^{r_x}}^{e_x}$. ∎

For any G-invariant code $\mathcal{C}$ and $x \in \mathcal{G}$, suppose $A_{\widetilde{x}}$ takes values from a subspace $V \subseteq F_{q^{r_x}}^{e_x}$. Then for any subspace $U \subseteq V$, the subcode obtained by restricting $A_{\widetilde{x}}$ to U is also a G-invariant code.

Definition 11. Let $X_1, X_2, \cdots, X_l$ be some disjoint subsets of $\mathcal{G}$ and suppose $R_{X_j} = \{A_{X_j} | \mathbf{a} \in \mathcal{C}\}$ for $j = 1, 2, \cdots, l$. The sets of transform components $\{A_x | x \in X_j\}$; $1 \le j \le l$ are called **unrelated** for $\mathcal{C}$ if $\{(A_{X_1}, A_{X_2}, \cdots, A_{X_l}) | \mathbf{a} \in \mathcal{C}\} = R_{X_1} \times R_{X_2} \times \cdots \times R_{X_l}$. They are called **related** if they are not unrelated.

By Lemma 4.4.1, for any $x_1 \in \widetilde{x}$, A_{x_1} is zero or A_{x_1} takes values from the whole of $F_{q^{r_x}}$ for $\mathcal{C}$. Moreover, if A_{x_1} is not zero for $\mathcal{C}$ and $A_{\widetilde{x}}$ takes values from a one dimensional subspace of $F_{q^{r_x}}^{e_x}$, then any other nonzero transform component A_{x_2} in the same residue class are related to A_{x_1} by constant multiplication, that is $A_{x_2} = cA_{x_1}$; $\forall \mathbf{a} \in \mathcal{C}$ for some constant $c \in F_{q^{r_x}}$. If however, $x_2 \in (x)^q$ i.e. x_2 is in the cyclotomic residue class of x, then $x_2 \in \widetilde{x^{q^i}}$ for some i. In that case, if A_{x_1} is not zero for $\mathcal{C}$ and $A_{\widetilde{x}}$ takes values from a one dimensional subspace of $F_{q^{r_x}}^{e_x}$, then A_{x_2} is related to A_{x_1} as $A_{x_2} = cA_{x_1}^{q^i}$ for some constant $c \in F_{q^{r_x}}$. However, this type of relation is the simplest. In general, some related transform components may not be related only in this way.

Let $\widetilde{x_1}, \widetilde{x_2}, \cdots, \widetilde{x_l}$ be a set of representative residue classes of all the distinct cyclotomic residue classes. Suppose we fix arbitrary subspaces V_i ; $i = 1, 2, \cdots, l$ of $F_{q^{r_{x_i}}}^{e_{x_i}}$; $i = 1, 2, \cdots, l$ respectively and consider the code $\mathcal{C} = \left\{\mathbf{a} \in F_q^{\mathcal{G}} | A_{\widetilde{x_i}} \in V_i \text{ for } i = 1, 2, \cdots, l\right\}$. Clearly, the code is G-invariant. But it is not clear whether any G-invariant code can be obtained this way by choosing suitable V_i ; $i = 1, 2, \cdots, l$. That is, are $A_{\widetilde{x_i}}$; $i = 1, \cdots, l$ unrelated for any G-invariant code ? Theorem 4.4.8 ahead answers this question in affirmative.

Lemma 4.4.2. *For a linear code $\mathcal{C}$, suppose, $A_{\tilde{x}}$ takes values from a subspace $V \subseteq F_{q^{r_x}}^{e_x}$, and $V = V_1 + V_2$. If the subcodes obtained by restricting $A_{\tilde{x}}$ to V_1 and V_2 are respectively $\mathcal{C}_1$ and $\mathcal{C}_2$, then $\mathcal{C} = \mathcal{C}_1 + \mathcal{C}_2$.*

Proof: Trivial. ■

In Lemma 4.4.2, if V is direct sum of V_1 and V_2, then $\mathcal{C}$ need not be the direct sum of $\mathcal{C}_1$ and $\mathcal{C}_2$, i.e. $\mathcal{C}_1 \cap \mathcal{C}_2$ need not be $\{\mathbf{0}\}$. In fact, $\mathcal{C}_1 \cap \mathcal{C}_2$ is the subcode obtained by restricting $A_{\tilde{x}}$ to $V_1 \cap V_2 = \{0\}$.

4.4.1 Minimal G-invariant Codes

We call a G-invariant code minimal if it does not have any proper G-invariant subcode. In a minimal G-invariant code, any nonzero A_x should take values from a 1-dimensional $F_{q^{r_x}}$-subspace, since otherwise, we can restrict A_x to a 1-dimensional $F_{q^{r_x}}$-subspace to get a proper G-invariant subcode.

Now, consider any $x, y \in \mathcal{G}$ such that none of A_x and A_y are zero for all the codewords of a minimal G-invariant code $\mathcal{C}$. Suppose A_x and A_y take values from the 1-dimensional $F_{q^{r_x}}$ and $F_{q^{r_y}}$ -subspaces V_1 and V_2 respectively. Since the code is minimal, if A_x is restricted to $\{0\}$, then the subcode obtained is the zero code. Since the code is F_q-linear, for any other element β in V_1, there is only one codeword in $\mathcal{C}$ with $A_x = \beta$. This is in fact true for any nonzero transform component in $\mathcal{C}$. So, A_x and A_y are related by a linear invertible map of V_1 onto V_2. But because the code is G-invariant, arbitrary linear invertible map can not relate two nonzero transform components.

Suppose in a G-invariant code, two transform components A_x and A_y take values from V_1 and V_2 respectively. If A_y is related to A_x by a homomorphism $\sigma : V_1 \longrightarrow V_2$, then σ satisfies

$$\sigma(\langle g, x\rangle v) = \langle g, y\rangle \sigma(v) \;\; \forall g \in G, \; \forall v \in V_1 \tag{4.7}$$

The following lemmas will help to identify the possible relations among transform components for a minimal G-invariant code. For a map σ of a finite field, we denote by $f_\sigma(X)$, a polynomial which induces σ, that is, $\sigma(a) = f_\sigma(a)$.

Lemma 4.4.3. *Let α and β be two elements of F_{q^l} and let the length of the F_q-conjugacy class of α be l_1. Suppose $a \in F_{q^l}^*$ and $\sigma : aF_{q^{l_1}} \longrightarrow F_{q^l}$ is an F_q linear nonzero map. Then*

σ satisfies $\sigma(\alpha b) = \beta\sigma(b)$;$\forall b \in aF_{q^{l_1}}$ if and only if $\beta = \alpha^{q^j}$ and $f_\sigma(X) = cX^{q^j}$ for some unique $c \in a'a^{-q^j}F_{q^{l_1}}$ and $j < l_1$.

Proof: ($\Rightarrow$): Clearly, kernel of σ is invariant under multiplication by α. So, it is either $\{0\}$ or F_{q^l}. Since σ is nonzero, the kernel is $\{0\}$. So, σ is an isomorphism or $aF_{q^{l_1}}$ onto it's image. Now, $Im(\sigma)$ is β-invariant F_q-subspace, i.e, it is an $F_{q^{l_2}}$-subspace, where l_2 is the length of the conjugacy class of β. Then, the map $\sigma^{-1} : Im(\sigma) \longrightarrow aF_{q^{l_2}}$ is invertible satisfying $\sigma^{-1}(\beta b) = \alpha\sigma^{-1}(b)\ \forall b \in Im(\sigma)$. Now, if $Im(\sigma)$ is not a minimal β-invariant F_q-subspace, then there is a minimal β-invariant F_q-subspace $V \subset Im(\sigma)$ and then $\sigma^{-1}(V)$ is a proper nonzero α-invariant F_q-subspace of $aF_{q^{l_1}}$: a contradiction. So, $Im(\sigma) = a'F_{q^{l_2}}$ for some $a' \in F_{q^l}$. Since σ is invertible, $l_1 = l_2$.

Rest of the proof follows from Lemma 3.2.2. ■

Lemma 4.4.4. *Let α, β and l_1 be as in Lemma 4.4.3 and V be an h dimensional $F_{q^{l_1}}$-subspace of F_{q^l}. Suppose $\sigma : V \longrightarrow F_{q^l}$ is a nonzero F_q-linear map. If σ satisfies $\sigma(\alpha b) = \beta\sigma(b)$;$\forall b \in V$ then $\beta = \alpha^{q^j}$ and $f_\sigma(X) = \sum_{i=0}^{h-1} c_i X^{q^{il_1+j}}$ for some unique $c_i \in F_{q^{sr}}$ for $0 \le i \le h-1$.*

Proof: Suppose $V = \oplus_{i=0}^{h-1} V_i$ where $V_i = s_i F_{q^{l_1}}$. Since σ is nonzero, it's restriction on at least one of $V_i; 0 \le i \le h-1$ is nonzero, and thus by Lemma 4.4.3, the first statement follows. Suppose $\sigma_i = \sigma|_{V_i}$. Then, $f_{\sigma_i}(X) = c_i' X^{q^j}$ for some unique c_i'. So,

$$
\begin{aligned}
& f_\sigma(X) = \sum_{w=0}^{h-1} c_w X^{q^{wl_1+j}} \\
\Leftrightarrow\ & c_i'(s_i a)^{q^j} = \sum_{w=0}^{h-1} c_w (s_i a)^{q^{wl_1+j}} \quad \forall a \in F_{q^{l_1}},\ \forall i \in [0, h-1] \\
\Leftrightarrow\ & c_i' s_i^{q^j} a^{q^j} = \left(\sum_{w=0}^{h-1} c_w \left(s_i^{q^j} \right)^{q^{wl_1}} \right) a^{q^j} \quad \forall a \in F_{q^{l_1}},\ \forall i \in [0, h-1] \\
\Leftrightarrow\ & c_i' s_i^{q^j} = \sum_{w=0}^{h-1} c_w \left(s_i^{q^j} \right)^{q^{wl_1}} \quad \forall i \in [0, h-1] \\
\Leftrightarrow\ & c_i' s_i' = \sum_{w=0}^{h-1} c_w (s_i')^{q^{wl_1}} \quad \forall i \in [0, h-1] \quad \text{where } s_i' = (s_i)^{q^j} \\
\Leftrightarrow\ & M \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{h-1} \end{pmatrix} = \begin{pmatrix} c_0' s_0' \\ c_1' s_0' \\ \vdots \\ c_{h-1}' s_{h-1}' \end{pmatrix}
\end{aligned} \tag{4.8}
$$

where

$$M = \begin{pmatrix} s'_0 & s'^{q^{l_1}}_0 & s'^{q^{2l_1}}_0 & \cdots & s'^{q^{(h-1)l_1}}_0 \\ s'_1 & s'^{q^{l_1}}_1 & s'^{q^{2l_1}}_1 & \cdots & s'^{q^{(h-1)l_1}}_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s'_{h-1} & s'^{q^{l_1}}_{h-1} & s'^{q^{2l_1}}_{h-1} & \cdots & s'^{q^{(h-1)l_1}}_{h-1} \end{pmatrix}$$

Now, $\{s_0, s_1, s_2, \cdots, s_{h-1}\}$ are linearly independent over $F_{q^{l_1}}$ since $V_j = \oplus_{i=0}^{h-1} s_i F_{q^{l_1}}$. So, $\{s'_0, s'_1, s'_2, \cdots, s'_{h-1}\}$ are also linearly independent over $F_{q^{l_1}} \Rightarrow M$ is nonsingular $\Rightarrow$ there exists unique solution of (4.8) for $c_0, c_1, \cdots, c_{h-1}$. (For the first implication, see [81, Chap. 3].) ■

Lemma 4.4.5. *Let α_i ; $i = 1, \cdots, k$ be some elements of F_{q^l} with length of their conjugacy classes l_i ; $i = 1, \cdots, k$ respectively. Suppose $l' = lcm(l_1, \cdots, l_k)$ and $\sigma : F_{q^{l'}} \longrightarrow F_{q^l}$ is a nonzero F_q-linear map. If σ satisfies*

$$\sigma(\alpha_i b) = \beta_i \sigma(b) \ \forall b \in F_{q^{l'}} \tag{4.9}$$

for some $\beta_i \in F_{q^l}$; $i = 1, \cdots, k$, then there exists a non-negative integer j such that $\beta_i = \alpha_i^{q^j}$ for all $i = 1, \cdots k$ and $f_\sigma(X) = cX^{q^j}$ for some unique $c \in F_{q^l}$.

Proof: Suppose $l'_i = \frac{l'}{l_i}$; $i = 1, \cdots, k$. By Lemma 4.4.4, $\beta_i = \alpha_i^{q^{j_i}}$ for some non-negative j_i ; $i = 1, \cdots, k$.

Now, $\exists$ a unique polynomial $f_\sigma(X)$ of degree $< q^{l'}$. Applying Lemma 4.4.4 for each i we see that, σ is induced by

$$f_i(X) = \sum_{h_i=0}^{l'_i-1} c_{i,h_i} X^{q^{h_i l_i + j_i}}$$

where c_{h_i} ; $0 \leq h_i \leq l'_i - 1$ are some unique constants.

Since all the polynomials $f_i(X)$ are of degree $< q^{l'}$, they have to be same. In particular, their smallest degree terms are same and that means $h_1 l_1 + j_1 = \cdots = h_k l_k + j_k = j(say)$. Now, if there is any other nonzero monomial than X^j, then such a monomial is of degree $h'_1 l_1 + j_1 = \cdots = h'_k l_k + j_k = j'(say)$. So,

$$\begin{aligned} (h'_1 - h_1) l_1 = \cdots &= (h'_k - h_k) l_k \\ \Rightarrow l' = lcm(l_1, \cdots, l_k) &\mid (h'_1 - h_1) l_1 \end{aligned}$$

This is a contradiction to the fact that $(h_1' - h_1) < l_1' = \frac{l'}{l_1}$. So,

$$f_\sigma(X) = cX^{q^j} \tag{4.10}$$

for some unique constant c and $\alpha_i = \beta_i^{q^j}$; $i = 1, \cdots, k$. ■

The following theorem characterizes minimal G-invariant codes in transform domain.

Theorem 4.4.6. *$\mathcal{C}$ is a minimal G-invariant code if and only if transform components in only one cyclotomic residue class is nonzero and $A_{\tilde{x}}$ for any x in that cyclotomic residue class takes values from a one-dimensional subspace of $F_{q^{r_x}}^{e_x}$.*

Proof: The reverse implication is trivial. In a minimal G-invariant code $\mathcal{C}$, if $A_{\tilde{x}}$ and $A_{\tilde{y}}$ are nonzero, then $A_{\tilde{x}}$ and $A_{\tilde{y}}$ take values from one dimensional $F_{q^{r_x}}$ and $F_{q^{r_y}}$-subspaces of $F_{q^{r_x}}^{e_x}$ and $F_{q^{r_y}}^{e_y}$ respectively since otherwise we can restrict them to one dimensional subspaces to get proper G-invariant subcodes of $\mathcal{C}$. Moreover, if A_x and A_y are nonzero, then A_y is dependent on A_x by an F_q-linear invertible map σ, i.e., $A_y = \sigma A_x$. Since the code is G-invariant, σ should satisfy $\sigma(\langle g, x\rangle b) = \langle g, y\rangle \sigma(b)\ \forall b \in F_{q^{r_x}}, \forall g \in G$. So by using Lemma 4.4.5, there is a j such that $\langle g, x\rangle^{q^j} = \langle g, y\rangle\ \forall g \in G \Rightarrow y \in (x)^q$. So, transform components in only one cyclotomic residue class are nonzero. ■

Clearly, any nonzero vector $\mathbf{a} \in F_q^{\mathcal{G}}$ is contained in a minimal G-invariant code if and only if the DFT of the vector is nonzero only in one cyclotomic residue class and the minimal G-invariant code is F_q-spanned by the vectors $\{g(\mathbf{a}) | g \in G\}$.

4.4.2 Arbitrary G-Invariant Codes

Let $\mathcal{C}$ be an arbitrary G-invariant code and suppose $A_{\tilde{x}}$ is nonzero for $\mathcal{C}$ and takes values from a subspace V of $F_{q^{r_x}}^{e_x}$. Let V_1 and V_2 be two subspaces of V such that $V = V_1 + V_2$. If $\mathcal{C}_1$ and $\mathcal{C}_2$ are the G-invariant subcodes obtained by restricting $A_{\tilde{x}}$ in the subspaces V_1 and V_2 respectively, then clearly, $\mathcal{C} = \mathcal{C}_1 + \mathcal{C}_2$. By successively doing this, the code can be decomposed as sum of a family of subcodes, each of which has any nonzero transform components $A_{\tilde{x}}$ taking values from some one dimensional subspace of $F_{q^{r_x}}^{e_x}$. Now, let us consider one such code (which is a subcode of the original code). Let $\{\tilde{x}_1, \tilde{x}_2, \cdots, \tilde{x}_k\}$ be a set of representative residue classes of different cyclotomic residue classes, where transform components are nonzero for the code. We construct a subset L of $\{\tilde{x}_1, \tilde{x}_2, \cdots, \tilde{x}_k\}$ as follows. First assign $L = \{\tilde{x}_1\}$. Suppose $A_{\tilde{x}_i}$; $i = 1, \cdots, k$ take values from the one dimensional $F_{q^{r_x}}$-subspaces V_i ; $i = 1, \cdots, k$ respectively. In the subcode obtained by restricting $A_{\widetilde{x_1}}$ to $\{0\}$, $A_{\widetilde{x_2}}$ will take values from either V_2 or $\{0\}$. If it takes values from $\{0\}$, then clearly, $A_{\widetilde{x_2}}$ is related to $A_{\widetilde{x_1}}$ by an isomorphism. Otherwise, $A_{\widetilde{x_1}}$ and $A_{\widetilde{x_2}}$ take values independently and in that case add $\widetilde{x}_2$ in L. Next restrict the transform components in all the residue classes indexed by elements of L to $\{0\}$ and check $A_{\widetilde{x}_i}$ not yet considered. If it's values vary over V_i, then put $\widetilde{x}_i$ in L. Continuing this way, we'll get a set L such that the residue classes of transform components indexed by it's elements are unrelated and the values of all other transform components are determined by them.

Now, subcode can be decomposed as direct sum of $|L|$ subcodes: $\mathcal{C}_i$; $i \in L$, where $\mathcal{C}_i$ is obtained by restricting $A_{\widetilde{x_j}}$; $j \notin L$ to zero. Clearly, each subcode thus obtained is a minimal G-invariant code. So, any G-invariant code can be decomposed as sum of some minimal G-invariant codes. Just taking a minimal family of such minimal subcodes such that their sum is still the original code, the code can be expressed as direct sum of some minimal G-invariant codes. So we have,

Theorem 4.4.7. *If the order of an abelian group G is relatively prime to q, then any G-invariant code can be decomposed as direct sum of some minimal G-invariant codes.*

However, the decomposition of a G-invariant code in terms of some minimal G-invariant codes is not unique, though for the special case of abelian codes, such a decomposition (as direct sum of minimal abelian codes) is unique.

It is known that if the exponent of an abelian group is not relatively prime to q, then there are abelian codes on that group, which can not be decomposed as direct sum of minimal abelian codes. If the exponent of G is not relatively prime to q, then for some k, the exponent of G_k is not relatively prime to k. Then an abelian code on G_k can be taken, which can not be decomposed as direct sum of minimal abelian codes. That code can be padded with zeros on all other orbits to get a G-invariant code, which is not decomposable as direct sum of minimal G-invariant codes.

For a minimal G-invariant code, transform components in different cyclotomic residue classes are unrelated. By Theorem 4.4.7, so is true for any G-invariant code. This fact together with Lemma 4.4.1 gives the following characterization of G-invariant codes in the transform domain.

Theorem 4.4.8 (Transform Domain Characterization). *Let G be an abelian group* *of permutations with order relatively prime to q. Then a code is G-invariant if and only if*

1. *For any $x \in \mathcal{G}$, $A_{\widetilde{x}}$ takes values from a subspace of $F_{q^{r_x}}^{e_x}$.*
2. *If $x_1, \cdots, x_k$ are representatives of the distinct cyclotomic residue classes of $\mathcal{G}$, then $A_{\widetilde{x_1}}, \cdots,$*
   $A_{\widetilde{x_k}}$ are unrelated.

Example 4.4.1 *(Continuation of Example 4.3.3).* Consider the case $q \equiv 2 \bmod 3$, $q \equiv 2$ or $3 \bmod 5$ (e.g. $q = 2, 8$). The following table shows the allowed vector spaces for a set of representative residue classes of the cyclotomic residue classes. For any G-invariant code, the transform components in those residue classes take values from some subspaces of the mentioned vector spaces. Moreover, those subspaces completely determine the G-invariant code.

Cyclotomic residue classes	r_x	e_x	Allowed vector space
$\{0_1, 0_2, 0_3, 0_4\}$	1	4	F_q^4
$\{g_1, g_2, 2g_1, 2g_2\}$	2	2	$F_{q^2}^2$
$\{g_3, g_4, 2g_3, 2g_4, 3g_3, 3g_4, 4g_3, 4g_4\}$	4	2	$F_{q^4}^2$

Table 4.4: The allowed vector spaces for transform components of representative residue classes of different cyclotomic residue classes

Though the decomposition of a G-invariant code is not unique in general, by second part of Theorem 4.4.8, any G-invariant code can be decomposed uniquely as direct sum of some G-invariant codes, each having nonzero transform components only in some distinct cyclotomic residue class. So we have,

Corollary 4.4.9. *Let $(x_i)^q$; $i = 1, 2, \cdots, k$ be the distinct cyclotomic residue classes. Then,*

$$\mathcal{C} = \bigoplus_{i=1}^{k} \mathcal{C}_{(x_i)^q} \tag{4.11}$$

where $\mathcal{C}_{(x_i)^q}$ denotes the subcode of $\mathcal{C}$ obtained by restricting all the transform components outside $(x_i)^q$ to zero.

For quasi-cyclic codes, this gives the primary components of the code [7] and for cyclic and Abelian codes these subcodes, when nonzero, are minimal cyclic and abelian codes respectively.

4.5 Duals of G-Invariant Codes : The Case $|G_1| \equiv |G_2| \equiv \cdots \equiv |G_t|$ mod p

For two vectors $\mathbf{a}, \mathbf{b} \in F_q^{\mathcal{G}}$, the Euclidean inner product of them is defined as

$$E(\mathbf{a}, \mathbf{b}) = \sum_{x \in \mathcal{G}} a_x b_x \tag{4.12}$$

The Euclidean inner product of $\mathbf{a}$ and $\mathbf{b}$ will also be denoted by $\mathbf{a}.\mathbf{b}$. For two vectors $\mathbf{a}, \mathbf{b} \in F_{q^2}^{\mathcal{G}}$, their Hermitian inner product is defined as

$$H(\mathbf{a}, \mathbf{b}) = \sum_{x \in \mathcal{G}} a_x b_x^q \tag{4.13}$$

Two vectors are called orthogonal w. r. t. Euclidean or Hermitian inner product, if respectively the Euclidean or Hermitian inner product of the vectors is zero. Two codes $\mathcal{C}_1$ and $\mathcal{C}_2$, are called Euclidean dual of each other if $\mathcal{C}_2 = \{\mathbf{b} | E(\mathbf{a}, \mathbf{b}) = 0\,;\, \forall \mathbf{a} \in \mathcal{C}_1\}$. Similarly Hermitian dual codes are defined. Euclidean duality will be simply referred as duality and explicitly mention Hermitian duality when needed. A code is called self dual when it is dual of itself. Similarly a code is called Hermitian self dual when it is Hermitian dual of itself.

Clearly, dual of a G-invariant code is also G-invariant.

In this section, only the case when all the orbit cardinalities are same modulo p is considered. This case gives fairly simple characterization of dual and self dual G-invariant codes and all the special cases fall under this case.

Theorem 4.5.1. *Let G be such that $|G_1| \equiv ... \equiv |G_t|$ mod p. For a G-invariant code $\mathcal{C}$, a vector $\mathbf{b} \in F_q^{\mathcal{G}}$ is orthogonal to $\mathcal{C}$ if and only if for all $\mathbf{a} \in \mathcal{C}$,*

$$\sum_{y \in \widetilde{x}} A_y B_{y^{-1}} = 0 \qquad \text{for all cyclotomic residue classes } (x)^q \tag{4.14}$$

Proof: Clearly, $\mathbf{b}$ is orthogonal to $\mathcal{C}$ if and only if

$$\begin{aligned}
\mathbf{a} \perp \mathbf{b}\,;\, \forall \mathbf{a} \in \mathcal{C} &\iff \sum_{y \in \mathcal{G}} a_y b_y = 0 \quad \forall \mathbf{a} \in \mathcal{C} \\
&\iff \sum_{y \in \mathcal{G}} A_y B_{y^{-1}} = 0 \quad \forall \mathbf{a} \in \mathcal{C} \quad \text{since } |G_1| \equiv ... \equiv |G_t| \text{ mod } p \\
&\iff \sum_{y \in (x)^q} A_y B_{y^{-1}} = 0 \text{ for each cyclotomic coset } (x)^q, \quad \forall \mathbf{a} \in \mathcal{C}
\end{aligned} \tag{4.15}$$

$$\begin{aligned}
&\iff \sum_{i=0}^{r_x-1}\sum_{y\in\widetilde{x}} A_{y^{q^i}} B_{\left(y^{q^i}\right)^{-1}} = 0 \quad " \\
&\iff \sum_{i=0}^{r_x-1}\sum_{y\in\widetilde{x}} A_{y^{q^i}} B_{(y^{-1})^{q^i}} = 0 \quad " \\
&\iff \sum_{i=0}^{r_x-1}\sum_{y\in\widetilde{x}} A_y^{q^i} B_{y^{-1}}^{q^i} = 0 \quad " \\
&\iff \sum_{i=0}^{r_x-1}\left(\sum_{y\in\widetilde{x}} A_y B_{y^{-1}}\right)^{q^i} = 0 \quad " \\
&\iff Tr_{F_{q^{r_x}}/F_q}\left(\sum_{y\in\widetilde{x}} A_y B_{y^{-1}}\right) = 0 \quad " \\
&\iff \sum_{y\in\widetilde{x}} A_y B_{y^{-1}} = 0 \quad " \qquad (4.16)
\end{aligned}$$

The fact that transform components in different cyclotomic residue classes are unrelated for G-invariant code is used to get (4.15), and (4.16) is obtained by using the fact that $A_{\widetilde{x}}$ takes values from a subspace of $F_{q^{r_x}}^{e_x}$. ■

Note that if (4.14) is satisfied for a residue class $\widetilde{x}$ then it is also satisfied for any other residue class in the same cyclotomic residue class. So, it is sufficient to consider only one representative residue class in each cyclotomic residue class. When two residue classes $\widetilde{x}$ and $\widetilde{x^{-1}}$ are considered, compatible orders are taken in them, i.e. if $A_{\widetilde{x}} = \left(A_x, A_{x_1}, \cdots, A_{x_{e_x-1}}\right)$, then $A_{\widetilde{x^{-1}}} = \left(A_{x^{-1}}, A_{x_1^{-1}}, \cdots, A_{x_{e_x-1}^{-1}}\right)$.

Let $\{x_1, x_2, \cdots, x_l\}$ be a set of representatives of the distinct cyclotomic residue classes of $\mathcal{G}$. Suppose, for the codes $\mathcal{C}_1$ and $\mathcal{C}_2$, $A_{\widetilde{x}}$ takes values from V_x and U_x respectively. Then V_x and U_x can also be considered as linear codes of length e_x over $F_{q^{r_x}}$. Using Theorem 4.5.1, the following characterization of the dual code of a G-invariant code is obtained.

Theorem 4.5.2. *Let G be such that $|G_1| \equiv ... \equiv |G_t|$ mod p. Suppose $\{x_1, x_2, \cdots, x_l\}$ is a set of representatives of the distinct cyclotomic residue classes in $\mathcal{G}$. Two G-invariant codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are dual of each other if and only if for each x_i; $i = 1, 2, \cdots, l$, V_{x_i} and $U_{x_i^{-1}}$ are dual codes of each other.*

4.5.1 Self Dual G-Invariant Codes

For characterizing self dual G-invariant codes, the cyclotomic residue classes are classified into three categories:

1. Self inverse cyclotomic residue classes $(x)^q$ with $x = x^{-1}$: In this case, suppose $x = x^{-1} \in G_k$, i.e, $x^2 = 1_k$. Then either $x = 1_k$ or order of G_k is even $\Rightarrow q$ is odd (Since $(q, |G_k|) = 1$) $\Rightarrow x^q = x \Rightarrow r_x = 1$. This type of cyclotomic residue classes are called as Type A cyclotomic residue classes and the cyclotomic cosets in them as Type A cyclotomic cosets.

2. Self inverse cyclotomic residue classes $(x)^q$ with $x \neq x^{-1}$: In this case, $x^{-1} = x^{q^i}$ for some $i < r_x; i \neq 0$. So, $x = (x^{-1})^{-1} = \left(x^{q^i}\right)^{-1} = (x^{-1})^{q^i} = x^{q^{2i}} \Rightarrow r_x|2i \Rightarrow 2|r_x$ and $i = \frac{r_x}{2}$. This type of cyclotomic residue classes will be called as Type B cyclotomic residue classes and the cyclotomic cosets in them as Type B cyclotomic cosets.

3. Cyclotomic residue classes which are not self inverse: This type of cyclotomic residue classes is called as Type C cyclotomic residue classes and the cyclotomic cosets in them as Type C cyclotomic cosets.

Let us denote the distinct self inverse cyclotomic residue classes as $(x_1)^q, \cdots, (x_{i_1})^q, (y_1)^q, \cdots, (y_{i_2})^q$ and the other distinct cyclotomic residue classes as $(z_1)^q, (z_1^{-1})^q \cdots, (z_{i_3})^q, (z_{i_3}^{-1})^q$, where $x_i = x_i^{-1}$ for $i = 1, \cdots, i_1$ and $y_i \neq y_i^{-1}$ for $i = 1, \cdots, i_2$. The following theorem gives the transform domain characterization of self dual G-invariant code.

Theorem 4.5.3. *Let G be such that $|G_1| \equiv ... \equiv |G_t|$ mod p and $\mathcal{C}$ be a G-invariant code, where $A_{\widetilde{x_i}}$, $A_{\widetilde{y_j}}$, $A_{\widetilde{z_k}}$ and $A_{\widetilde{z_k^{-1}}}$ take values from the subspaces V_{x_i}, V_{y_j}, V_{z_k} and $V_{z_k^{-1}}$ respectively for $i = 1, \cdots, i_1$; $j = 1, \cdots, i_2$; $k = 1, \cdots, i_3$. The code is self dual if and only if*

1. *V_{x_i} is a self-dual code for $i = 1, \cdots, i_1$.*

2. *V_{y_j} is a Hermitian self-dual code for $j = 1, \cdots, i_2$.*

3. *V_{z_k} is the dual code of $V_{z_k^{-1}}$ for $k = 1, \cdots, i_3$.*

Proof: If the code is self dual, then by Theorem 4.5.2, V_{y_j} is dual of $V_{y_j^{-1}}$. Now,

$$\begin{aligned} & V_{y_j} \text{ is dual of } V_{y_j^{-1}} \\ \Longleftrightarrow\quad & V_{y_j} = \left\{ v \in F_{q^{r_{y_j}}}^{e_{y_j}} \mid \sum_{i=1}^{e_{y_j}} v_i u_i = 0 \ \ \forall u \in V_{y_j^{-1}} \right\} \end{aligned}$$

Now, $V_{y_j^{-1}} = \left\{ (u_1^{q^{\frac{r_{y_j}}{2}}}, \cdots, u_{e_{y_j}}^{q^{\frac{r_{y_j}}{2}}}) | u \in V_{y_j} \right\}$. So,

$$\begin{aligned} & V_{y_j} \text{ is dual of } V_{y_j^{-1}} \\ \Longleftrightarrow\quad & V_{y_j} = \left\{ v \in F_{q^{r_{y_j}}}^{e_{y_j}} \mid \sum_{i=1}^{e_{y_j}} v_i u_i^{\frac{r_{y_j}}{2}} = 0 \ \ \forall u \in V_{y_j} \right\} \\ \Longleftrightarrow\quad & V_{y_j} \text{ is Hermitian self dual.} \end{aligned}$$

The rest of the proof follows directly from Theorem 4.5.2. ∎

Corollary 4.5.4. *Let G be such that $|G_1| \equiv ... \equiv |G_t| \bmod p$. Suppose $[f_1]^q, \cdots, [f_{i_1}]^q, [g_1]^q, \cdots, [g_{i_2}]^q$ are the self-inverse q-cyclotomic cosets in G such that $f_i^{-1} = f_i$; for $1 \leq i \leq i_1$ and $g_i^{-1} \neq g_i$; for $1 \leq i \leq i_2$ and $[h_1]^q, [h_1^{-1}]^q, \cdots, [h_{i_3}]^q, [h_{i_3}^{-1}]^q$ are the other q-cyclotomic cosets in G. Then a G-quasi-abelian code $\mathcal{C}$ of length $t|G|$ over F_q is self-dual if and only if*

1. *V_{f_i} is a self-dual code for $i = 1, \cdots, i_1$.*

2. *V_{g_j} is a Hermitian self-dual code for $j = 1, \cdots, i_2$.*

3. *V_{h_k} is the dual code of $V_{h_k^{-1}}$ for $k = 1, \cdots, i_3$.*

The number of self dual codes and Hermitian self dual codes of any length is known [93, 94]. Let us denote by $N_E(q, l)$ and $N_H(q, l)$, the number of self dual and Hermitian self dual codes of length l over F_q. If l is odd, then both these numbers are zero. Also, let $N(q, l)$ denote the number of subspaces of F_q^l. The exact values of $N(q, l)$, $N_E(q, l)$ and $N_H(q, l)$ are as given below.

$$N(q,l) = \sum_{i=0}^{l} \prod_{j=0}^{i-1} \frac{q^l - q^j}{q^i - q^j} \tag{4.17}$$

$$N_E(q,l) = \begin{cases} \prod_{i=1}^{\frac{l}{2}-1} (q^i + 1), & \text{for q and l even} \\ 2\prod_{i=1}^{\frac{l}{2}-1} (q^i + 1), & \text{for } q \equiv 1 \bmod 4, \ \text{l even} \\ 2\prod_{i=1}^{\frac{l}{2}-1} (q^i + 1), & \text{for } q \equiv 3 \bmod 4, \ \text{l is devisible by 4} \\ 0, & \text{otherwise} \end{cases} \tag{4.18}$$

$$N_H(q,l) = \begin{cases} \prod_{i=0}^{\frac{l}{2}-1}(q^{i+\frac{1}{2}}+1), & \text{when } l \text{ is even} \\ 0, & \text{otherwise} \end{cases} \quad (4.19)$$

Theorem 4.5.3 directly gives:

Theorem 4.5.5. *Let G be such that $|G_1| \equiv ... \equiv |G_t|$ mod p. Number of self dual G-invariant codes over F_q is $\prod_{i=1}^{i_1} N_E(q^{r_{x_i}}, e_{x_i}) \prod_{j=1}^{i_2} N_H(q^{r_{y_j}}, e_{y_j}) \prod_{k=1}^{i_3} N(q^{r_{z_k}}, e_{z_k})$, where the empty product is 1 by convention.*

In the above theorem, the first factor is contributed by the Type A cyclotomic residue classes, the second factor is contributed by Type B cyclotomic residue classes and the third factor is contributed by the Type C cyclotomic residue classes.

Example 4.5.1 *(Continuation of Example 4.3.3).* In the following, the number of self-dual G-invariant codes is found for different q's for which $|G_1| \equiv |G_2| \equiv \cdots \equiv |G_t|$ mod p holds.

$q \equiv 2$ mod 3, $q \equiv 2$ or 3 mod 5 and $3 \equiv 5$ mod p (e.g. $q = 2, 8$):

Different types of cyclotomic residue classes are shown in Table 4.5. So, the number

Cyclotomic residue classes	Type	r_x	e_x
$\{0_1, 0_2, 0_3, 0_4\}$	A	1	4
$\{g_1, g_2, 2g_1, 2g_2\}$	B	2	2
$\{g_3, g_4, 2g_3, 2g_4, 3g_3, 3g_4, 4g_3, 4g_4\}$	B	4	2

Table 4.5: Different types of cyclotomic residue classes for $q \equiv 2$ mod 3, $q \equiv 2$ or 3 mod 5 and $3 \equiv 5$ mod p (e.g. $q = 2, 8$)

of self-dual G-invariant codes over F_q is $N_E(q,4)N_H(q^2,2)N_H(q^4,2)$.

$q \equiv 1$ mod 3, $q \equiv 1$ mod 5 and $3 \equiv 5$ mod p (e.g. $q = 16$):

Different types of cyclotomic residue classes are shown in Table 4.6.

From Table 4.6, clearly the number of self-dual G-invariant codes over F_q is $N_E(q,4)\,(N(q,2))^3$.

$q \equiv 1$ mod 3, $q \equiv 4$ mod 5 and $3 \equiv 5$ mod p (e.g. $q = 4$):

Different types of cyclotomic residue classes are shown in Table 4.7.

From Table 4.7, clearly the number of self-dual G-invariant codes over F_q is $N_E(q,4)N(q,2)(N_H(q^2,2))^2$.

Cyclotomic residue classes	Type	r_x	e_x
$\{0_1, 0_2, 0_3, 0_4\}$	A	1	4
$\{g_1, g_2\}$	C	1	2
$\{2g_1, 2g_2\}$	C	1	2
$\{g_3, g_4\}$	C	1	2
$\{2g_3, 2g_4\}$	C	1	2
$\{3g_3, 3g_4\}$	C	1	2
$\{4g_3, 4g_4\}$	C	1	2

Table 4.6: Different types of cyclotomic residue classes for $q \equiv 1 \bmod 3$, $q \equiv 1 \bmod 5$ and $3 \equiv 5 \bmod p$ (e.g. $q = 16$)

Cyclotomic residue classes	Type	r_x	e_x
$\{0_1, 0_2, 0_3, 0_4\}$	A	1	4
$\{g_1, g_2\}$	C	1	2
$\{2g_1, 2g_2\}$	C	1	2
$\{2g_3, 2g_4, 3g_3, 3g_4\}$	B	2	2
$\{g_3, g_4, 4g_3, 4g_4\}$	B	2	2

Table 4.7: Different types of cyclotomic residue classes for $q \equiv 1 \bmod 3$, $q \equiv 4 \bmod 5$ and $3 \equiv 5 \bmod p$ (e.g. $q = 4$)

Corollary 4.5.6. *If G is such that $|G_1| \equiv ... \equiv |G_t| \bmod p$ and there is a self-inverse cyclotomic coset $[x]^q \subseteq \mathcal{G}$ with e_x odd, then there is no self-dual G-invariant code over F_q.*

Proof: If $[x]^q$ is a self-inverse cyclotomic coset, it contributes $N_E(q^{r_x}, e_x)$ or $N_H(q^{r_x}, e_x)$ to the product in Theorem 4.5.5. Both these numbers are 0 when e_x is odd and thus result follows. ■

Example 4.5.2 *(Continuation of Example 4.1.2).* G has exponent 45. Let $\alpha \in F_{q^r}$ be an element of order 45. The set of indexes has two orbits under the action of G and $G_1 \simeq Z_{15}$ and $G_2 \simeq Z_9$. Let g_1 and g_2 be generators of G_1 and G_2. The co-ordinate positions can be indexed by elements $\mathcal{G}$ as shown in Figure 4.15. The DFT in $F_q^{24} \simeq F_q^{\mathcal{G}}$ is defined with respect to the maps ψ_k defined by:

$$\psi_1(g_1, g_1) = \alpha^3$$
$$\psi_2(g_2, g_2) = \alpha^5.$$

So,

$$\psi_1(\sigma_1|_{G_1}, ig_1) = \psi_1(10g_1, ig_1) = \alpha^{30i} \text{ for } 0 \leq i \leq 15$$

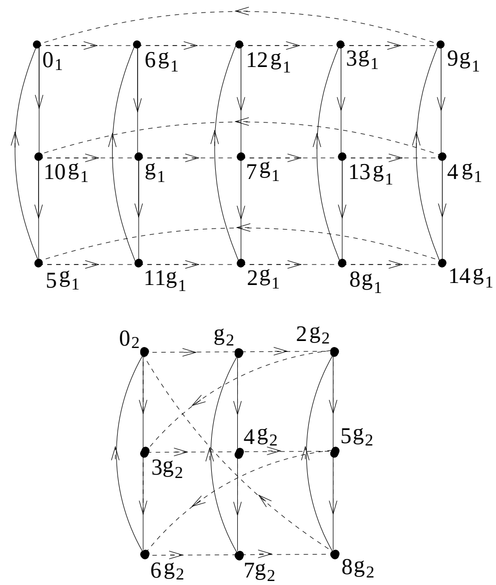

Figure 4.15: Re-indexing the components as in Example 4.5.2

$$\psi_1(\sigma_2|_{G_1}, ig_1) = \psi_1(6g_1, ig_1) = \alpha^{18i} \text{ for } 0 \le i \le 15$$
$$\psi_2(\sigma_1|_{G_2}, jg_2) = \psi_1(3g_2, jg_2) = \alpha^{15j} \text{ for } 0 \le i \le 9$$
$$\psi_2(\sigma_2|_{G_2}, jg_2) = \psi_1(g_2, jg_2) = \alpha^{5j} \text{ for } 0 \le i \le 9.$$

ig_1 and jg_2 are in the same residue class if and only if $\psi_1(\sigma_1|_{G_1}, ig_1) = \psi_2(\sigma_1|_{G_2}, jg_2)$ i.e. $\alpha^{30i} = \alpha^{15j}$ and $\psi_1(\sigma_2|_{G_1}, ig_1) = \psi_2(\sigma_2|_{G_2}, jg_2)$ i.e. $\alpha^{18i} = \alpha^{5j}$ i.e. $i = j = 0$. So, all the residue classes of $\mathcal{G}$ except $\{0_1, 0_2\}$ are singletons.

When $q \equiv 2 \bmod 9$ and $9 \equiv 15 \bmod p$, there is no self-dual G-inverse code over F_q, since $[g_2]^q = \{g_2, 2g_2, 4g_2, 8g_2, 7g_2, 5g_2\}$ is a self-inverse cyclotomic residue class with $e_{g_2} = 1$.

Corollary 4.5.7. *If G is such that $|G_1| \equiv ... \equiv |G_t|$ mod p and the number t of orbits is odd, then there is no self dual G-invariant code.*

Proof: For any k, $\widetilde{0_k} = \{0_j | j = 1, \cdots, t\}$ and $[0_k]^q = \{0_k\}$ is a self-inverse cyclotomic coset. So, applying Corollary 4.5.6 on this cyclotomic coset, the result follows. ∎

Corollary 4.5.8. *Let G be an abelian group with order relatively prime to q. Suppose $[f_1]^q, \cdots, [f_{i_1}]^q$ are the Type A q-cyclotomic cosets, $[g_1]^q, \cdots, [g_{i_2}]^q$ are the Type B q-cyclotomic cosets and $[h_1]^q, [h_1^{-1}]^q, \cdots, [h_{i_3}]^q, [h_{i_3}^{-1}]^q$ are the Type C q-cyclotomic cosets in G. Then the number of self-dual G-quasi-abelian codes of length $t|G|$ is $\prod_{i=1}^{i_1} N_E(q^{r_{f_i}}, t)$ $\prod_{j=1}^{i_2} N_H(q^{r_{g_j}}, t) \prod_{k=1}^{i_3} N(q^{r_{h_k}}, t)$.*

Example 4.5.3 *(Continuation of Example 4.1.4).* There are two orbits and $G_1 \equiv G_2 \equiv G \equiv Z_9 \times Z_3$. In the following, the cyclotomic cosets and the number of self-dual G-quasi-abelian codes of length 54 are discussed for different cases.

<u>$q \equiv 2$ or $5 \bmod 9$ [e.g $q = 2,\ 32$]</u> The cyclotomic cosets in G are shown in Table 4.8. Number

Cyclotomic cosets in G	Type	r_x
$\{(0,0)\}$	A	1
$\{(1,0),(2,0),(4,0),(8,0),(7,0),(5,0)\}$	B	6
$\{(0,1),(0,2)\}$	B	2
$\{(1,1),(2,2),(4,1),(8,2),(7,1),(5,2)\}$	B	6
$\{(2,1),(4,2),(8,1),(7,2),(5,1),(1,2)\}$	B	6
$\{(3,1),(6,2)\}$	B	2
$\{(3,2),(6,1)\}$	B	2
$\{(3,0),(6,0)\}$	B	2

Table 4.8: Different types of cyclotomic residue classes for $q \equiv 2$ or $5 \bmod 9$ [e.g $q = 2,\ 32$]

of self-dual G-quasi-abelian codes of length 54 is $N_E(q,2)\left(N_H(q^2,2)\right)^4\left(N_H(q^6,2)\right)^3$.

<u>$q \equiv 1 \bmod 9$ [e.g $q = 64$]</u> All the cyclotomic cosets of $G \simeq Z_9 \times Z_3$ are singletons and all except $(0,0)$ are of type C. Number of self-dual G-quasi-abelian codes of length 54 is $N_E(q,2)\left(N(q,2)\right)^{26}$.

<u>$q \equiv 4$ or $7 \bmod 9$ [e.g $q = 4,\ 16$]</u> The cyclotomic cosets in G are shown in Table 4.9. Number of self-dual G-quasi-abelian codes of length 54 is $N_E(q,2)\left(N(q,2)\right)^4\left(N(q^3,2)\right)^3$.

<u>$q \equiv 8 \bmod 9$ [e.g $q = 8$]</u> The cyclotomic cosets in G are shown in Table 4.10. Number of self-dual G-quasi-abelian codes of length 54 is $N(q,2)\left(N_H(q^2,2)\right)^{13}$.

For any group G of permutations, let $\widetilde{0}$ denote the residue class $\{0_1, \cdots, 0_t\}$, where 0_k denotes the identity element of G_k. For any G-invariant binary code, the code $\mathcal{C}_0 \triangleq \{A_{\widetilde{0}} | a \in \mathcal{C}\}$ will be called as the binary component of $\mathcal{C}$.

Any binary self-dual code in which Hamming weight of every codeword is divisible by 4 is called a Type II code or doubly even self-dual code. In the following, we have the characterization of Type II G-invariant code.

Theorem 4.5.9. *Let G be a group of permutations of odd exponent. Then a G-invariant binary self-dual code $\mathcal{C}$ is Type II if and only if it's binary component $\mathcal{C}_0$ is Type II.*

Proof: Size of each orbit is odd since G has odd exponent.

Cyclotomic cosets in G	Type	r_x
$\{(0,0)\}$	A	1
$\{(1,0),(4,0),(7,0)\}$	C	3
$\{(2,0),(8,0),(5,0)\}$	C	3
$\{(0,1)\}$	C	1
$\{(0,2)\}$	C	1
$\{(1,1),(4,1),(7,1)\}$	C	3
$\{(2,2),(8,2),(5,2)\}$	C	3
$\{(2,1),(8,1),(5,1)\}$	C	3
$\{(4,2),(7,2),(1,2)\}$	C	3
$\{(3,1)\}$	C	1
$\{(6,2)\}$	C	1
$\{(3,2)\}$	C	1
$\{(6,1)\}$	C	1
$\{(3,0)\}$	C	1
$\{(6,0)\}$	C	1

Table 4.9: Different types of cyclotomic residue classes for $q \equiv 4$ or 7 mod 9 [e.g $q = 4$, 16]

($\Rightarrow$) : Since the code is Type II and each orbit size is odd, 4 divides t.

For any $\mathbf{v} \in \mathcal{C}_0$, there is a codeword $\mathbf{a} \in \mathcal{C}$ such that $A_{\tilde{0}} = \mathbf{v}$ and $A_x = 0 \ \forall\, x \notin \tilde{0}$.

$$wt_H(\mathbf{a}) = \sum_{\substack{k=1 \text{to } t \\ v_k \neq 0}} |G_k|$$

Since $4|wt_H(\mathbf{a})$ and $|G_k|$ is odd for each k, $wt_H(\mathbf{v})$ is also divisible by 4. So, $\mathcal{C}_0$ is Type II.

($\Leftarrow$) : Suppose, $\mathcal{C}_{\tilde{0}}$ is Type II. Then 4 divides t.

For any $\mathbf{a} \in \mathcal{C}$, suppose $A_{\tilde{0}} = \mathbf{v} \in \mathcal{C}_0$.

Exactly $wt_H(\mathbf{v})$ orbits of $\mathbf{a}$ has odd weights. Since $wt_H(\mathbf{v})$ and $(t - wt_H(\mathbf{v}))$ are both divisible by 4, weight of $\mathbf{a}$ is divisible by 4. ■

4.5.2 Self Dual Quasi-cyclic Codes

For l-quasi-cyclic codes, $G \simeq G_k \simeq Z_{\frac{n}{l}}$. and $Z_{\frac{n}{l}}$ denotes the quotient group $Z/\frac{n}{l}Z \simeq \{0, 1, \cdots, \frac{n}{l} - 1\}$ with modulo $\frac{n}{l}$ addition. In this case, the q-cyclotomic cosets in $Z_{\frac{n}{l}}$ are the q-cyclotomic cosets modulo $\frac{n}{l}$, which play an important role in case of cyclic codes of length $\frac{n}{l}$. Each residue class contains one element from each orbit. It is well

Cyclotomic cosets in G	Type	r_x
$\{(0,0)\}$	A	1
$\{(1,0),(8,0)\}$	B	2
$\{(2,0),(7,0)\}$	B	2
$\{(4,0),(5,0)\}$	B	2
$\{(0,1),(0,2)\}$	B	2
$\{(1,1),(8,2)\}$	B	2
$\{(2,2),(7,1)\}$	B	2
$\{(4,1),(5,2)\}$	B	2
$\{(2,1),(7,2)\}$	B	2
$\{(4,2),(5,1)\}$	B	2
$\{(8,1),(1,2)\}$	B	2
$\{(3,1),(6,2)\}$	B	2
$\{(3,2),(6,1)\}$	B	2
$\{(3,0),(6,0)\}$	B	2

Table 4.10: Different types of cyclotomic residue classes for $q \equiv 8 \bmod 9$ [e.g $q = 8$]

known that there is a $1-1$ correspondence between the prime factors of the polynomial $Y^{\frac{n}{l}} - 1$ and the q-cyclotomic cosets modulo $\frac{n}{l}$. The degree of a prime factor of $Y^{\frac{n}{l}} - 1$ is same as the cardinality r_j of the corresponding q-cyclotomic coset $[j]^q$. Moreover, the self reciprocal cyclotomic cosets in $Z_{\frac{n}{l}}$ correspond to the prime factors $f(Y)$ whose reciprocal polynomial $f^*(Y)$ is an associate of $f(Y)$. Such polynomials will be called as self reciprocal polynomials.

For any $k \in Z_{\frac{n}{l}}$, if $-k \equiv k \bmod \frac{n}{l}$, then $2k \equiv 0 \bmod \frac{n}{l} \Rightarrow k \equiv 0 \bmod \frac{n}{l}$ or $k \equiv \frac{\frac{n}{l}}{2} \bmod \frac{n}{l}$ for even $\frac{n}{l}$. So,

$$i_1 = \begin{cases} 1 & \text{if } \frac{n}{l} \text{ is odd} \\ 2 & \text{if } \frac{n}{l} \text{ is even} \end{cases}.$$

Theorem 4.5.9 specializes to the case of quasi-cyclic codes as following.

Corollary 4.5.10. *A self-dual binary code $\mathcal{C}$ is a Type II l-quasi-cyclic code of length n ($\frac{n}{l}$ odd) if and only if it's binary component $\mathcal{C}_0$ is of Type II.*

Proof: Putting $G = \langle\sigma\rangle$ where σ represents the permutation 'l-times cyclic shift'. ■

This corollary gives Propositions 7.1 and 7.3 of [92] as special cases as following.

Corollary 4.5.11. *[92, Proposition 7.1] A self-dual binary code $\mathcal{C}$ is a Type II l-quasi-cyclic code of length $3l$ if and only if it's binary component $\mathcal{C}_0$ is of Type II.*

Proof: Putting $\frac{n}{l} = 3$ in Corollary 4.5.10. ■

Corollary 4.5.12. *[92, Proposition 7.3] For $\frac{n}{l} = 5$ or 7, a self-dual binary code $\mathcal{C}$ is a Type II l-quasi-cyclic code of length n if and only if it's binary component $\mathcal{C}_0$ is of Type II.*

Proof: Putting $\frac{n}{l} = 5$ or $\frac{n}{l} = 7$ in Corollary 4.5.10. ■

Corollary 4.5.8 specializes for quasi-cyclic codes as following.

Corollary 4.5.13. *Let $\frac{n}{l}$ be a positive integer relatively prime to q. Suppose $[x_1]^q, \cdots, [x_{i_1}]^q$ are the Type A q-cyclotomic cosets modulo $\frac{n}{l}$, $[y_1]^q, \cdots, [y_{i_2}]^q$ are the Type B q-cyclotomic cosets modulo $\frac{n}{l}$ and $[z_1]^q, [-z_1]^q, \cdots, [z_{i_3}]^q, [-z_{i_3}]^q$ are the Type C q-cyclotomic cosets modulo $\frac{n}{l}$. Then the number of self-dual l-quasi-cyclic codes of length n is $\prod_{i=1}^{i_1} N_E(q^{r_{x_i}}, l)$ $\prod_{j=1}^{i_2} N_H(q^{r_{y_j}}, l) \prod_{k=1}^{i_3} N(q^{r_{z_k}}, l)$.*

Example 4.5.4 *(Continuation of Example 4.1.5).* The q-cyclotomic cosets in Z_9 for $q = 2$ are shown in Table 4.11. So by Corollary 4.5.13, the number of binary l-quasi-cyclic codes

2-Cyclotomic cosets in Z_9	Type	r_x
$\{0\}$	A	1
$\{1, 2, 4, 8, 7, 5\}$	B	6
$\{3, 6\}$	B	2

Table 4.11: Different types of 2-cyclotomic classes in Z_9

of length $9l$ is $N_E(q, l)N_H(q^6, l)N_H(q^2, l)$.

The number of l-quasi-cyclic codes of length $9l$ over F_q for any other q can be calculated similarly from the q-cyclotomic cosets in Z_9.

All the results of [92] regarding existence/nonexistence and number of self-dual quasi-cyclic codes of specific parameters are obtainable as special cases from Corollary 4.5.13. To be specific, Propositions 6.1, 6.2, 6.3, 6.6, 6.9, 6.10, 6.12, 6.13, 6.15 and 6.17 of [92] are direct consequences of Corollary 4.5.13. Those are explained in details in Subsection 4.5.3.

4.5.3 Some Corollaries

Corollary 4.5.14. *[92, Proposition 6.1] Let $\frac{n}{l}$ be relatively prime to q. Then self-dual*

2-quasi-cyclic codes over F_q of length $2\frac{n}{l}$ exist if and only if exactly one of the following conditions is satisfied:

1. *q is a power of 2.*
2. *$q = p^b$, where p is a power congruent to 1 mod 4; or*
3. *$q = p^{2b}$, where p is a prime congruent to 3 mod 4.*

Proof: Here $l = 2$. So, for any self-inverse cyclotomic coset $[k]^q$; $k \in Z_{\frac{n}{l}}$, such that $k \equiv -k \bmod l$, $N_E(q^{r_k}, 2) > 0$ if and only if either q is even or $q \equiv 1 \bmod 4$. So, the result follows. ∎

Corollary 4.5.15. *[92, Proposition 6.2] Let q be a prime power satisfying one of the conditions in Corollary 4.5.14 and let $\frac{n}{l}$ be an integer relatively prime to q. Suppose that $Y^{\frac{n}{l}} - 1 = \delta g_1 \cdots g_{j_1} h_1 h_2^* \cdots h_{j_2} h_{j_2}^*$ in $F_q[Y]$, where δ is a nonzero element of F_q, $g_1, \cdots, g_{j_1}, h_1, h_1^*, \cdots, h_t, h_{j_2}^*$ are monic irreducible polynomials such that g_i are self-reciprocal and h_j and h_j^* are reciprocals. Suppose further that $g_1 = Y - 1$ and if $\frac{n}{l}$ is even, $g_2 = Y + 1$. Let the degree of g_i be $2d_i$, and let the degree of h_j (hence also h_j^*) be e_j. Then the number of distinct self-dual 2-quasi-cyclic codes of length $2\frac{n}{l}$ over F_q is given by*

$$\begin{array}{ll} 4\prod_{i=3}^{j_1}(q^{d_i}+1)\prod_{j=1}^{j_2}N(q^{e_j},2) & \text{if } \frac{n}{l} \text{ is even and } q \text{ is odd} \\ 2\prod_{i=2}^{j_1}(q^{d_i}+1)\prod_{j=1}^{j_2}N(q^{e_j},2) & \text{if } \frac{n}{l} \text{ is odd and } q \text{ is odd} \\ \prod_{i=2}^{j_1}(q^{d_i}+1)\prod_{j=1}^{j_2}N(q^{e_j},2) & \text{if } \frac{n}{l} \text{ is odd and } q \text{ is even} \end{array}$$

Proof: The prime factors $g_1, \cdots, g_{j_1}$ of $Y^{\frac{n}{l}} - 1$ corresponds to the self-inverse cyclotomic cosets modulo $\frac{n}{l}$ in $Z_{\frac{n}{l}}$. The factors $Y - 1$ and $Y + 1$ (when $\frac{n}{l}$ is even) corresponds to the cyclotomic cosets $[0]^q = \{0\}$ and $[\frac{\frac{n}{l}}{2}]^q = \{\frac{\frac{n}{l}}{2}\}$ respectively. The other cyclotomic cosets, which are not self-inverse, correspond to the factors $h_1, h_1^*, \cdots, h_{j_2}, h_{j_2}^*$. So, the result follows. ∎

Corollary 4.5.16. *[92, Proposition 6.3] Let $\frac{n}{l}$ be relatively prime to q and let l be odd. Then no self-dual l-quasi-cyclic codes over F_q of length n exist. Moreover, when $q \equiv 3 \bmod 4$, self-dual l-quasi-cyclic codes over F_q of length n exist only if $l \equiv 0 \bmod 4$.*

Proof: Trivial. ∎

Corollary 4.5.17. *[92, Proposition 6.6] Suppose $q \equiv 1 \bmod 4$ and l is even, or $q \equiv 3 \bmod 4$. The number of distinct self-dual l-quasi-cyclic codes of length $2l$ over F_q is $4\prod_{i=1}^{\frac{l}{2}-1}(q^i+1)^2$.*

Proof: Here $\frac{n}{l} = 2$, l even. The cyclotomic cosets are $[0]^q = \{0\}$ and $[1]^q = \{1\}$, both of Type A. So the result follows from Corollary 4.5.13 and expression (4.18). ■

Corollary 4.5.18. *[92, Proposition 6.9] Suppose that q and l satisfy one of the following:*

1. *$q \equiv 11 \bmod 12$ and $l \equiv 0 \bmod 4$; or*

2. *$q \equiv 2 \bmod 3$ but $q \not\equiv 11 \bmod 4$, and l is even.*

Then the number of distinct self-dual l-quasi-cyclic codes over F_q of length $3l$ is given by $b(q+1)\prod_{i=1}^{\frac{l}{2}-1}(q^i+1)(q^{2i+1}+1)$, where $b = 1$ if q is even, 2 if q is odd.

Proof: In the cases under consideration, the cyclotomic cosets modulo 3 are

Type A	$\{0\}$
Type B	$\{1,2\}$
Type C	none

Thus the result follows. ■

Corollary 4.5.19. *[92, Proposition 6.10] Let q and l satisfy one of the following:*

1. *$q \equiv 7 \bmod 12$ and $l \equiv 0 \bmod 4$; or*

2. *$q \equiv 1 \bmod 3$ but $q \not\equiv 7 \bmod 4$, and l is even.*

Then the number of distinct self-dual l-quasi-cyclic codes over F_q of length $3l$ is given by $b\left(\prod_{i=1}^{\frac{l}{2}-1}(q^i+1)\right)N(q,l)$, where $b = 1$ if q is even, 2 if q is odd.

Proof: In the cases under consideration, the cyclotomic cosets modulo 3 are

Type A	$\{0\}$
Type B	none
Type C	$\{1\},\{2\}$

Thus the result follows. ■

Corollary 4.5.20. *[92, Proposition 6.12] Let q be an odd prime power such that -1 is not a square in F_q and let $l \equiv 0 \bmod 4$. Then the number of distinct self-dual l-quasi-cyclic codes over F_q of length $4l$ is $4(q+1)\prod_{i=1}^{\frac{l}{2}-1}(q^i+1)^2(q^{2i+1}+1)$,*

Proof: In this case, $Y^4 - 1$ factors into prime factors over F_q as $(Y-1)(Y+1)(Y^2+1)$. So, the cyclotomic cosets modulo 4 are

Type A	$\{0\}$,$\{2\}$
Type B	$\{1,3\}$
Type C	none

So the result follows from Corollary 4.5.13. ∎

Corollary 4.5.21. *[92, Proposition 6.13] Let l be even and let q be an odd prime power such that -1 is a square in F_q. Then the number of distinct self-dual l-quasi-cyclic codes over F_q of length $4l$ is $\left(4\prod_{i=1}^{\frac{l}{2}-1}(q^i+1)^2\right)N(q,l)$,*

Proof: In this case, Y^4-1 factors into prime factors over F_q as $(Y-1)(Y+1)(Y-\gamma)(Y+\gamma)$, where $\gamma \in F_q$ is such that $\gamma^2 = -1$. So, the cyclotomic cosets modulo 4 are

Type A	$\{0\}$,$\{2\}$
Type B	none
Type C	$\{\gamma\}$, $\{-\gamma\}$

So, the result follows from Corollary 4.5.13. ∎

Corollary 4.5.22. *[92, Proposition 6.15] Let l be even and let q be such that $Y^4 + Y^3 + Y^2 + Y + 1$ is irreducible in $F_q[Y]$. If $q \equiv 3 \bmod 4$, suppose further that $l \equiv 0 \bmod 4$. Then the number of distinct self-dual l-quasi-cyclic codes over F_q of length $5l$ is $b(q^2+1)\prod_{i=1}^{\frac{l}{2}-1}(q^i+1)(q^{4i+2}+1)$, where $b=1$ if q is even, 2 if q is odd.*

Proof: For the case under consideration, $Y^5 - 1$ factors into prime factors over F_q as $(Y-1)(Y^4+Y^3+Y^2+Y+1)$. So, the cyclotomic cosets modulo 5 are

Type A	$\{0\}$
Type B	$\{1,2,3,4\}$
Type C	none

So, the result follows from Corollary 4.5.13. ∎

Corollary 4.5.23. *[92, Proposition 6.17] When l is even, $\frac{n}{l}$ is an integer and q is a prime power relatively prime to $\frac{n}{l}$ such that $Y^{\frac{n}{l}}-1$ factors completely into linear factors over F_q, with the additional constraint that $l \equiv 0 \bmod 4$, the number of distinct self-dual l-quasi-cyclic codes over F_q of length n is equal to*

$$\begin{array}{ll} \left(\prod_{i=3}^{\frac{l}{2}-1}(q^i+1)\right) N(q,l)^{\frac{(\frac{n}{l}-1)}{2}} & \text{if } q \text{ is even} \\ \left(2\prod_{i=2}^{\frac{l}{2}-1}(q^i+1)\right) N(q,l)^{\frac{(\frac{n}{l}-1)}{2}} & \text{if } \frac{n}{l} \text{ is odd and } q \text{ is odd} \\ \left(2\prod_{i=2}^{\frac{l}{2}-1}(q^i+1)\right)^2 N(q,l)^{\frac{(\frac{n}{l}-2)}{2}} & \text{if } \frac{n}{l} \text{ is even and } q \text{ is odd} \end{array}$$

Proof: For the case under consideration, the cyclotomic cosets modulo $\frac{n}{l}$ are

Type A	$\{0\}$ and $\{\frac{\frac{n}{l}}{2}\}$ when $\frac{n}{l}$ is even and q is odd
Type B	none
Type C	all the other cyclotomic cosets

So, the result follows from Corollary 4.5.13. ■

4.6 Duals of G-Invariant Codes : The General Case

To characterize duals of G-invariant codes, some generalizations of Euclidean and Hermitian dual codes are needed. Let $\mathbf{v} = (v_1, \cdots, v_l) \subseteq F_q^l$ be a vector with each component nonzero. For any two vectors $\mathbf{a}, \mathbf{b} \in F_q^l$, the $\mathbf{v}$-weighted Euclidean inner product (or $E_{\mathbf{v}}$ inner product) of $\mathbf{a}$ and $\mathbf{b}$ is defined as

$$E_{\mathbf{v}}(\mathbf{a}, \mathbf{b}) = \sum_{x=1}^{l} v_x a_x b_x \tag{4.20}$$

Similarly for any $\mathbf{v} \in F_q^l$, $\mathbf{v}$-weighted Hermitian inner product or $H_{\mathbf{v}}$-inner product of $\mathbf{a} \in F_{q^2}^l$ and $\mathbf{b} \in F_{q^2}^l$ is defined as

$$H_{\mathbf{v}}(\mathbf{a}, \mathbf{b}) = \sum_{x=1}^{l} v_x a_x b_x^q \tag{4.21}$$

Note that, since $\mathbf{v} \in F_q^l$, $H_{\mathbf{v}}(\mathbf{a}, \mathbf{b}) = 0$ if and only if $H_{\mathbf{v}}(\mathbf{b}, \mathbf{a}) = 0$ since $H_{\mathbf{v}}(\mathbf{a}, \mathbf{b}) = H_{\mathbf{v}}(\mathbf{b}, \mathbf{a})^q$.

For any $x \in \mathcal{G}$, we'll denote by i_x, the cardinality of the orbit containing x. For any residue class $\widetilde{x}$, $i_{\widetilde{x}}$ will denote the e_x-tuple with components i_y ; $y \in \widetilde{x}$ in the same order as A_y's in $A_{\widetilde{x}}$. With missuse of notation, $i_{\widetilde{x}}^{-1}$ will denote the component-wise inverse (in $F_p \subseteq F_q$) of $i_{\widetilde{x}}$.

Now, Theorem 4.5.1 can be generalized to:

Theorem 4.6.1. *For a G-invariant code $\mathcal{C}$, a vector $\mathbf{b} \in F_q^{\mathcal{G}}$ is orthogonal to $\mathcal{C}$ if and only if for all $\mathbf{a} \in \mathcal{C}$,*

$$\sum_{y \in \widetilde{x}} i_y^{-1} A_y B_{y^{-1}} = 0 \qquad \text{for all cyclotomic residue classes } (x)^q \tag{4.22}$$

So in general, two G-invariant codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are duals of each other if and only if for each x_i ; $i = 1, 2, \cdots, l$ (see Theorem 4.5.2), V_{x_i} and U_{x_i} are $E_{\mathbf{i}_{\widetilde{x_i}}^{-1}}$-duals of each other. This gives a modified versions of Theorem 4.5.3 and 4.5.5 as bellow. Here $N_{E_{\mathbf{i}_{\widetilde{x_i}}^{-1}}}(q, l)$ and $N_{H_{\mathbf{i}_{\widetilde{x_i}}^{-1}}}(q, l)$ denote the number of respectively $E_{\mathbf{i}_{\widetilde{x_i}}^{-1}}$-self dual codes and $H_{\mathbf{i}_{\widetilde{x_i}}^{-1}}$-self dual codes of length l over F_q. Note that if $\mathbf{i}_{\widetilde{x}}^{-1}$ is a scalar (in F_q) multiple of $\mathbf{v}$, then two subspaces $V \subseteq F_q^l$ and $U \subseteq F_q^l$ are $E_{\mathbf{i}_{\widetilde{x}}^{-1}}$-duals of each other if and only if they are $E_{\mathbf{v}}$-duals of each other. Similarly $V \subseteq F_{q^2}^l$ and $U \subseteq F_{q^2}^l$ are $H_{\mathbf{i}_{\widetilde{x}}^{-1}}$-duals if and only if they are $H_{\mathbf{v}}$-duals of each other. So, when all components of $\mathbf{i}_{\widetilde{x}}$ are same, $E_{\mathbf{i}_{\widetilde{x}}^{-1}}$-duality and $H_{\mathbf{i}_{\widetilde{x}}^{-1}}$-duality are same as Euclidean and Hermitian duality respectively.

Theorem 4.6.2. *Let $\mathcal{C}$ be a G-invariant code, where $A_{\widetilde{x_i}}$, $A_{\widetilde{y_j}}$, $A_{\widetilde{z_k}}$ and $A_{\widetilde{z_k^{-1}}}$ takes values from the subspaces V_{x_i}, V_{y_j}, V_{z_k} and $V_{z_k^{-1}}$ respectively for $i = 1, \cdots, i_1$; $j = 1, \cdots, i_2$; $k = 1, \cdots, i_3$. The code is self dual if and only if*

1. *V_{x_i} is a $E_{\mathbf{i}_{\widetilde{x_i}}}$-self-dual code for $i = 1, \cdots, i_1$.*
2. *V_{y_j} is a $H_{\mathbf{i}_{\widetilde{y_j}}}$-Hermitian self-dual code for $j = 1, \cdots, i_2$.*
3. *V_{z_k} is the $E_{\mathbf{i}_{\widetilde{z_k}}}$-dual code of $V_{z_k^{-1}}$ for $k = 1, \cdots, i_3$.*

Theorem 4.6.3. *Number of self dual G-invariant codes over F_q is $\prod_{i=1}^{i_1} N_{E_{\mathbf{i}_{\widetilde{x_i}}}}(q^{r_{x_i}}, e_{x_i}) \prod_{j=1}^{i_2} N_{H_{\mathbf{i}_{\widetilde{y_j}}}}(q^{r_{y_j}}, e_{y_j}) \prod_{k=1}^{i_3} N(q^{r_{z_k}}, e_{z_k})$, where the empty product is 1 by convention.*

It is easy to see that if l is odd, then $N_{E_{\mathbf{v}}}(q, l) = N_{H_{\mathbf{v}}}(q^2, l) = 0$ for any $\mathbf{v} \in F_q^l$. So, Corollary 4.5.6 and 4.5.7 are valid even in the general case, i.e. even when $|G_1| \equiv |G_2| \equiv \cdots \equiv |G_t| \bmod p$ is not true.

Though values of $N_E(q,l)$ and $N_H(q,l)$ are known, the values of $N_{E_\mathbf{v}}(q,l)$ and $N_{H_\mathbf{v}}(q^2,l)$ are not known for arbitrary $\mathbf{v}$. The following theorem allows computation of these quantities for certain cases.

Theorem 4.6.4. *If either all components of $\mathbf{v} \in F_q^l$ are quadratic residues in F_q or all components are quadratic non-residues in F_q, then*

1. $N_{E_\mathbf{v}}(q,l) = N_E(q,l)$ *and*

2. $N_{H_\mathbf{v}}(q^2,l) = N_H(q^2,l)$

Proof: If all the components of $\mathbf{v}$ are quadratic non residues in F_q, then we can divide this vector by one of it's components to get a scalar multiple of the vector, in which each component is quadratic residue. So, it is sufficient to assume that the components of $\mathbf{v}$ are quadratic residues. Suppose $\mathbf{v} = (v_1, \cdots, v_l) = (s_1^2, \cdots, s_l^2)$.

We shall give a 1-1 correspondence between the $E_\mathbf{v}$-self dual codes and the Euclidean self-dual codes to prove the first part of the result. For the second part, we shall give a 1-1 correspondence between the $H_\mathbf{v}$-self dual codes and the Hermitian self-dual codes.

Let $U \subseteq F_q^l$ be a $E_\mathbf{v}$-self dual code of length l over F_q. Then we'll show that the subspace $W \triangleq \{(s_1a_1, \cdots, s_la_l) | \mathbf{a} = (a_1, \cdots, a_l) \in V\}$ is a Euclidean self dual code. Suppose $(s_1a_1, \cdots, s_la_l), (s_1b_1, \cdots, s_lb_l) \in W$. Then,

$$\sum_{i=1}^{l} v_i a_i b_i = 0$$
$$\Rightarrow \sum_{i=1}^{l} (s_i a_i)(s_i b_i) = 0$$
$$\Rightarrow (s_1a_1, \cdots, s_la_l) \text{ and } (s_1b_1, \cdots, s_lb_l) \text{ are orthogonal w. r. t. Euclidean inner product}$$

So, any two vectors in W are orthogonal w. r. t. Euclidean inner product and since dimension of W is same as dimension of V, which is $\frac{l}{2}$, W is a Euclidean self dual code. Similarly, it is easy to check that for any Euclidean self dual code W, the code $U \triangleq \{(s_1^{-1}a_1, \cdots, s_l^{-1}a_l) | \mathbf{a} = (a_1, \cdots, a_l) \in W\}$ is a $E_\mathbf{v}$ - self dual code. This proves the first part of the theorem.

Proof of the second part is similar, noting that $\mathbf{v} = (v_1, \cdots, v_l) = (s_1^2, \cdots, s_l^2) = (s_1^{q+1}, \cdots, s_l^{q+1})$ since $s_i \in F_q$ and thus $s_i^q = s_i \; \forall i$. ■

This theorem not only gives the number of weighted Euclidean self-dual and weighted Hermitian self-dual codes in terms of the numbers of Euclidean and Hermitian self dual codes respectively in the mentioned cases, but the proof also shows how to construct those codes from Euclidean and Hermitian self-dual codes.

Example 4.6.1 *(Continuation of Example 4.5.1).* In the following, the number of self-dual codes are found for different q's for which $|G_1| \equiv |G_2| \equiv \cdots \equiv |G_t| \bmod p$ does not hold.

$q \equiv 2 \bmod 3$, $q \equiv 4 \bmod 5$ and $3 \not\equiv 5 \bmod p$ (e.g. $q = 29, 59$):

Different types of cyclotomic residue classes are shown in Table 4.12.

Cyclotomic residue classes	Type	r_x	e_x
$\{0_1, 0_2, 0_3, 0_4\}$	A	1	4
$\{g_1, g_2, 2g_1, 2g_2\}$	B	2	2
$\{g_3, g_4, 4g_3, 4g_4\}$	B	2	2
$\{2g_3, 2g_4, 3g_3, 3g_4\}$	B	2	2

Table 4.12: Different types of cyclotomic residue classes for $q \equiv 2 \bmod 3$, $q \equiv 4 \bmod 5$ and $3 \not\equiv 5 \bmod p$ (e.g. $q = 29, 59$)

For $q = 59$, $11^2 \equiv 3 \bmod 59$ and $8^2 \equiv 5 \bmod 59$. So, the number of self dual G-invariant codes over F_{59} is $N_E(59,4)(N_H(59^2,2))^3 = 120 \times 60^3$.

For $q = 29$, $5 \equiv 11^2 \bmod 29$ but 3 is not a quadratic residue modulo 29. $3 \times 10 \equiv 1 \bmod 29$ i.e. $3^{-1} = 10$ in F_{29} and $5 \times 6 \equiv 1 \bmod 29$ i.e. $5^{-1} = 6$ in F_{29} So, the number of self dual G-invariant codes over F_{29} is $N_{E_{(10,10,6,6)}}(29,4)(N_H(29^2,2))^3$.

$q \equiv 1 \bmod 3$, $q \equiv 2$ or $3 \bmod 5$ and $3 \not\equiv 5 \bmod p$ (e.g. $q = 7, 13$):

Different types of cyclotomic residue classes are shown in Table 4.13.

Cyclotomic residue classes	Type	r_x	e_x
$\{0_1, 0_2, 0_3, 0_4\}$	A	1	4
$\{g_1, g_2\}$	C	1	2
$\{2g_1, 2g_2\}$	C	1	2
$\{g_3, g_4, 2g_3, 2g_4, 3g_3, 3g_4, 4g_3, 4g_4\}$	B	4	2

Table 4.13: Different types of cyclotomic residue classes for $q \equiv 1 \bmod 3$, $q \equiv 2$ or $3 \bmod 5$ and $3 \not\equiv 5 \bmod p$ (e.g. $q = 7, 13$)

For $q = 7$, both 3 and 5 are quadratic non residues in F_7. So, the number of self dual

G-invariant codes over F_7 is $N_E(7,4)(N_H(7^4,2))N(7,2) = 16 \times 50 \times 10$.

For $q = 13$, $3 \equiv 4^2 \bmod 13$ but 5 is not a quadratic residue modulo 29. $3 \times 9 \equiv 1 \bmod 13$ i.e. $3^{-1} = 9$ in F_{13} and $5 \times 8 \equiv 1 \bmod 13$ i.e. $5^{-1} = 8$ in F_{13} So, the number of self dual G-invariant codes over F_{13} is $N_{E_{(9,9,8,8)}}(13,4)N_H(13^4,2)N(13,2)$.

4.7 Minimum Distance of G-Invariant codes

As discussed in the previous two chapters, a lower bound on the minimum Hamming distance of a code can be obtained from a set of parity check equations over an extension field.

If $(x_1)^q, \cdots, (x_k)^q$ denote the distinct cyclotomic residue classes, then we know that any G-invariant code $\mathcal{C}$ is specified by the subspaces $V_{x_1}, \cdots, V_{x_k}$ of $F_{q^{r_{x_1}}}^{e_{x_1}}, \cdots, F_{q^{r_{x_k}}}^{e_{x_k}}$ respectively, from which $A_{\widetilde{x_1}}, \cdots, A_{\widetilde{x_k}}$ take values. Now, each of V_x ; $x = x_1, \cdots, x_k$ can be considered as a linear code over $F_{q^{r_x}}$ of length e_x. So, V_x is determined by a set of parity check equations. As shown below, for any such parity check equation, we can get a parity check equation over $F_{q^{r_x}}$ of $\mathcal{C}$.

Suppose $\widetilde{x} = \{y_1, \cdots, y_l\}$, where $x = y_i$ for some i and $l = e_x$. Let $\sum_{i=1}^{l} c_i A_{y_i} = 0$ be a parity check equation of V_x. Then,

$$\begin{aligned} & \sum_{i=1}^{l} c_i A_{y_i} = 0 \\ \Rightarrow \quad & \sum_{i=1}^{l} c_i \sum_{y \in \mathcal{G}} \Psi(y, y_i) a_y = 0 \\ \Rightarrow \quad & \sum_{y \in \mathcal{G}} \left(\sum_{i=1}^{l} c_i \Psi(y, y_i) \right) a_y = 0 \end{aligned}$$

Clearly, this gives a parity check equation of $\mathcal{C}$ over $F_{q^{r_x}}$. The component wise conjugate vectors of the parity check vectors obtained this way and the vectors in their span are also parity check vectors of the code.

4.8 Quasi-abelian Codes

For any abelian group G, the G-quasi-abelian codes of length $t|G|$ (which are submodules of $(F_qG)^t$) are closed under the action of G on the co-ordinates. So such codes are invariant under the co-ordinate permutations induced by elements of G. However, this case has a more organized structure that, all the orbits of the co-ordinates under the action of G are of same size $|G|$ and there are t such orbits. This raises a natural reverse question: for a given abelian group G of permutations on code co-ordinates, when can the G-invariant codes be viewed as G-quasi-abelian codes. The following theorem answers this question.

Theorem 4.8.1. *The G-invariant codes are G-quasi-abelian codes i.e. they can be viewed as submodules of $(F_qG)^t$ for some t if and only if $|G| = |G_k|$; $\forall k$.*

Proof: We need to prove the reverse implication only. If $|G| = |G_k|$, then $g \mapsto g^{(k)}$ is an isomorphism of G onto G_k. So, any G-invariant code can be viewed as a submodule of $(F_qG)^t$. ■

Note that to see the G-invariant codes as G-quasi-abelian codes, $G_{k_1} \simeq G_{k_2}$; $\forall k_1, k_2 \in I_t$ is not sufficient. Each of them also have to be isomorphic to the group G, which is not the case in general. The following is such an example.

Example 4.8.1. Consider the group of permutations $G = \langle\{\sigma_1, \sigma_2\}\rangle$ of $I_{54} = \{1, 2, \cdots, 54\}$, where cycle decompositions of σ_1 and σ_2 are as below.

$$\sigma_1 = (1,2,3)(4,5,6)(7,8,9)(10,11,12)(13,14,15)(16,17,18)(19,20,21)(22,23,24)(25,26,27)$$
$$(28,29,30,37,38,39,46,47,48)(31,32,33,40,41,42,49,50,51)(34,35,36,43,44,45,52,53,54);$$
$$\sigma_2 = (1,4,7,10,13,16,19,22,25)(2,5,8,11,14,17,20,23,26)(3,6,9,12,15,18,21,24,27)$$
$$(28,31,34,37,40,43,46,49,52)(29,32,35,38,41,44,47,50,53)(30,33,36,39,42,45,47,51,54)$$

The cycles are shown in Figure 4.16. The solid lines with arrows represent the cycles of σ_1 and the dashed lines with arrows represent the cycles of σ_2. It can be checked that the order of the group G is 81, whereas the two groups G_1 and G_2 of restricted permutations are isomorphic to each other and of order 27 and thus are not isomorphic to G. So, G-invariant codes can not be seen as G-quasi-abelian codes in this case.

For G-quasi-abelian codes, the co-ordinates in different orbits can be indexed by copies $G_1, \cdots,$
G_t of the same group G. So, for any element $g \in G$, we have an element $g^{(i)} \in G_i$ for each i. So every residue class is of the form $\{g^{(1)}, \cdots, g^{(t)}\}$. We'll denote it by $\widetilde{g}$ instead of $\widetilde{g^{(i)}}$. For G-quasi-abelian codes, every cyclotomic residue class has same number of elements in each orbit.

The transform domain characterization of G-invariant codes specializes for the G-quasi-abelian codes as:

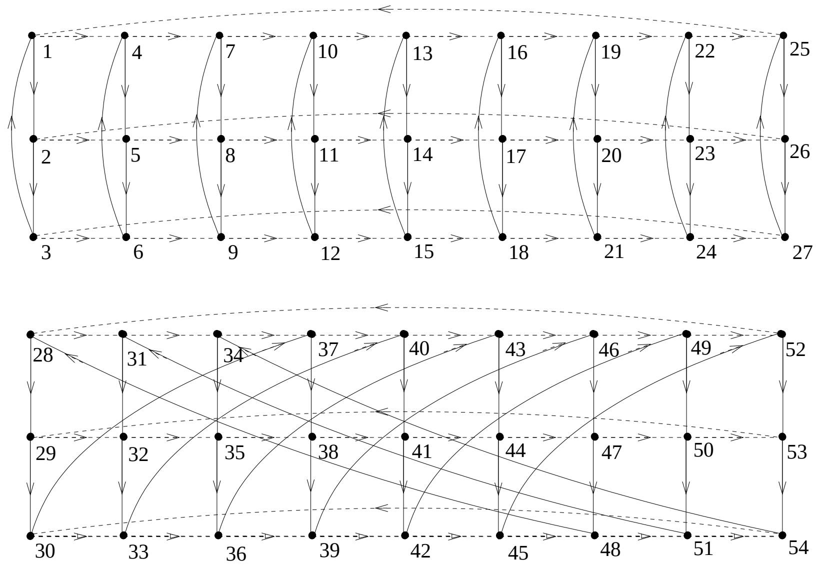

Figure 4.16: Cycle structures of σ_1 and σ_2 of Example 4.8.1

Theorem 4.8.2. *Let G be an abelian group of permutations with order relatively prime to q. Then a code $\mathcal{C} \subseteq (F_qG)^t$ is G-quasi-abelian if and only if*

1. *For any $g \in G$, $A_{\widetilde{g}}$ takes values from a subspace of $F^t_{q^{r_g}}$.*
2. *If $[g_1]^q, \cdots, [g_k]^q$ are of the distinct q-cyclotomic cosets in G, then $A_{\widetilde{g_1}}, \cdots, A_{\widetilde{g_k}}$ are unrelated.*

Definition 12. If for a G-quasi-abelian code, symbols in some orbits form a set of information symbols and the symbols in the other orbits are the parity check symbols then the code is called a **systematic G-quasi-abelian code**.

For a systematic G-quasi-abelian code $\mathcal{C} \subseteq (F_qG)^t$ of dimension $k|G|$ $(k \leq t)$, without loss of generality we can assume that the first k orbits are information symbols and the rest are parity check symbols. Then there exist some $c_{l,j} \in F_qG\,; l = 1, \cdots, t-k, \;; j = 1, \cdots, k$ such that each codeword is of the form $(a_1, a_2, \cdots, a_k, \sum_{j=1}^{k} a_j c_{1,j}, \sum_{j=1}^{k} a_j c_{2,j}, \cdots, \sum_{j=1}^{k} a_j c_{t-k,j}) \in (F_qG)^t$. If the DFT of a_j and $c_{i,j}$ are denoted by A_j and $C_{i,j}$ respectively, then each codeword in transform domain is of the form $(A_1, A_2, \cdots, A_k, \sum_{j=1}^{k} A_j \odot C_{1,j}, \sum_{j=1}^{k} A_j \odot C_{2,j}, \cdots, \sum_{j=1}^{k} A_j \odot C_{t-k,j}) \in (F_qG)^t$, where $'\odot'$ represents component-wise product.

4.8.1 Decoding of Systematic Quasi-Abelian Codes

For a systematic G-quasi-abelian code with one information orbit, there are $c_j\,;\, j = 1, \cdots, t-1 \in F_qG$, such that every codeword is of the form $(a, c_1a, c_2a, \cdots, c_{t-1}a)$. For quasi-cyclic codes, i.e., for cyclic G and when c_j is a unit in F_qG for $j = 1, \cdots, t-1$, Karlin [64] used alternate syndromes based on $c_j\,;\, j = 1, \cdots, t-1$ and their inverses to gain considerable reduction in decoding operations. The same technique can be used to decode this class of systematic G-quasi-abelian codes.

In the following, Karlin's approach is extended for systematic G-quasi-abelian codes with multiple information orbits. This is a two-step generalization of Karlin's algorithm, one step is from quasi-cyclic codes to quasi-abelian codes and the other is from one information orbit i.e. 1-generated codes to multiple generated codes.

For a systematic G-quasi-abelian code $\mathcal{C} \subseteq (F_qG)^t$ of dimension $k|G|$ $(k \leq t)$, there exist some $c_{l,j} \in F_qG\,;\, l = 1, \cdots, t-k,\ ;\ j = 1, \cdots, k$ such that each codeword is of the form $\mathbf{a} = (a_1, a_2, \cdots, a_k, a_{k+1}, \cdots, a_t) \in (F_qG)^t$ where $a_{k+i} = \sum_{j=1}^{k} a_j c_{i,j}$. We restrict our attention to the case where $c_{i,j}\,;\, i = 1, \cdots, t-k,\ ;\ j = 1, \cdots, k$ are such that any $k \times k$ submatrix of the transposed generator matrix

$$M = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ c_{1,1} & c_{1,2} & \cdots & c_{1,k} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,k} \\ \vdots & \vdots & \ddots & \vdots \\ c_{t-k,1} & c_{t-k,2} & \cdots & c_{t-k,k} \end{pmatrix}$$

is invertible over F_qG. That is, any k orbits form a set of information symbols. For any subset $X \subseteq [1, t]$, the $|X| \times k$ submatrix comprising of the corresponding rows of M is denoted by M_X. Similarly $\mathbf{a}_X$ will denote the vector of length $|X|$ comprising of the components $a_i \in F_qG\,;\ i \in X$. The complement $[1, t] \setminus X$ is denoted by $\bar{X}$. So, if we know k components of a codeword $(a_1, a_2, \cdots, a_t)$ i.e., $\mathbf{a}_X$ for some X of size k, then we can solve uniquely for the others as $\mathbf{a}_{\bar{X}} = M_{\bar{X}} M_X^{-1} \mathbf{a}_X$.

Suppose $\mathbf{a} = (a_1, a_2, \cdots, a_t)$ is the transmitted codeword and the received vector is $\mathbf{a}' = (a'_1, a'_2, \cdots, a'_t)$. Let $\mathbf{e} = (e_1, e_2, \cdots, e_t) = \mathbf{a}' - \mathbf{a}$ denote the error vector. Suppose the code's known minimum distance is $2l+1$ and a vector is received with at most l errors. That is, the Hamming weight of the error, $\sum_{i=1}^{t} wt_H(e_i) \leq l$. Then the transmitted vector is the only vector of the form $\left(a_1, a_2, \cdots, a_k, \sum_{j=1}^{k} a_j c_{1,j}, \sum_{j=1}^{k} a_j c_{2,j}, \cdots, \sum_{j=1}^{k} a_j c_{t-k,j}\right)$ having distance from the received vector $\leq l$.

Given a received vector $\mathbf{a}'$, for each $X \subseteq [1,t]$ of size k we can compute a syndrome $S_X = M_{\bar{X}} M_X^{-1} \mathbf{a}'_X + \mathbf{a}'_{\bar{X}} = M_{\bar{X}} M_X^{-1} (\mathbf{a}_X + \mathbf{e}_X) + \mathbf{a}_{\bar{X}} + \mathbf{e}_{\bar{X}} = M_{\bar{X}} M_X^{-1} \mathbf{e}_X + \mathbf{e}_{\bar{X}}$. So, given e_X, we can calculate $e_{\bar{X}}$ as $e_{\bar{X}} = S_X - M_{\bar{X}} M_X^{-1} \mathbf{e}_X$. Now, if the error is of weight less than l, then there is at least one subset X of size k such that weight of e_X is at most $\lfloor \frac{kl}{t} \rfloor$. So, if we presume an e_X of weight at most $\lfloor \frac{kl}{t} \rfloor$, and $wt_H\left(e_X, S_X - M_{\bar{X}} M_X^{-1} \mathbf{e}_X\right) \leq l$, then e_X and $e_{\bar{X}} = S_X - M_{\bar{X}} M_X^{-1} \mathbf{e}_X$ give the actual error.

Now, any $e_X \in (F_q G)^{|X|}$ can be considered as a vector of length $|X||G|$ over F_q. If $e_X^{(1)}, e_X^{(2)} \in (F_q G)^{|X|}$ are such that $e_X^{(1)} = e_X^{(2)} g$ for some $g \in G$, i.e. one is obtained from the other by a permutation induced by an element of G, then we call them to be equivalent. Let us call the equivalence classes as the G-quasi-abelian equivalence classes. All the elements of an equivalence class clearly has same Hamming weight. If we compute $M_{\bar{X}} M_X^{-1} \mathbf{e}_X$ for one representative of an equivalence class, then for any $\mathbf{e}'_X = \mathbf{e}_X g$ in the same equivalence class, $M_{\bar{X}} M_X^{-1} \mathbf{e}'_X = g M_{\bar{X}} M_X^{-1} \mathbf{e}_X$ can be computed from $M_{\bar{X}} M_X^{-1} \mathbf{e}_X$ just by permuting it's components.

Using these concepts, the decoding algorithm can be put as follows.

1. For each subset $X \subseteq [1,t]$ of size k calculate S_X.
2. For $i = 0$ to $\lfloor \frac{kl}{t} \rfloor$
3. For each subset $X \subseteq [1,t]$ of size k
4. For each G-quasi-abelian equivalence class of Hamming weight i, take a representative e_X. Compute $M_{\bar{X}} M_X^{-1} \mathbf{e}_X$
5. For each $g \in G$
5. Compute $e_{\bar{X}} = S_X - g M_{\bar{X}} M_X^{-1} \mathbf{e}_X$
6. Check if Hamming weight of $e_{\bar{X}}$ is less than or equal to $t-i$. If so, take $(e_X, e_{\bar{X}})$ as the error and quit. Otherwise, continue with the loops.

Number of syndromes (in $(F_q G)^{t-k}$) calculated by this algorithm is $\binom{t}{k}$. If $k=1$ and G is cyclic, then it specializes to the algorithm proposed by Karlin [64] and Heijnen and van Tilborg [65] for decoding systematic quasi-cyclic codes with single row of circulants in the generator matrix, i.e. 1-generator systematic quasi-cyclic codes.. For $t=2$, it further specializes to the single parity circulant case.

4.9 Discussion

The class of codes considered in this chapter is a generalization of cyclic codes, quasi-cyclic codes, abelian codes and quasi-abelian codes. All these special families of codes are defined as codes closed under one or more permutations of the code components. Algebraic structure of these special families of codes were investigated by different authors and in all the cases, there seemed to have some common structures. For example, when all the aforesaid permutations has orders relatively prime to q, those codes are decomposable as direct sum of minimal codes. It is shown in this chapter that, such structures are not anything special to those codes, but it is present in the family of G-invariant codes for any abelian group G of permutations with order of G relatively prime to q.

Also, a two-fold extension of Karlin's decoding algorithm for quasi-cyclic code is given. It is an extension from the case of one generator systematic quasi-cyclic codes to arbitrary systematic quasi-cyclic codes and also from the case of quasi-cyclic codes to quasi-abelian codes. However, since the algebraic structure of G-invariant codes for any arbitrary abelian G (with order relatively prime to q) is only as complex as that of quasi-cyclic codes and quasi-abelian codes, it would be interesting to see whether this decoding algorithm can be extended to cover this general class of codes.

The results of Section 4.5 give as special cases all the results of [92] regarding self-dual quasi-cyclic codes. Theorem 4.6.3 gives the number of self-dual G-invariant codes in terms of the number of weighted self-dual codes and weighted Hermitian self-dual codes when $|G_1| \equiv |G_2| \equiv \cdots \equiv |G_t| \mod p$ does not hold. Theorem 4.6.4 enables computations of these numbers in terms of the known numbers for some special cases of weight vectors. It remains an open problem to compute the values of $N_{E_{\mathbf{v}}}(q,l)$ and $N_{H_{\mathbf{v}}}(q,l)$ for arbitrary weight vector $\mathbf{v}$ and thus enable computation of the number of self-dual G-invariant codes for arbitrary abelian group G of permutations.

In Chapter 3, the quasi-cyclic codes were studied using conventional DFT. Since DFT is defined only when the length n is relatively prime to the characteristic of the field, the scope of this treatment is restricted to the same case. Under the action of the co-ordinate permutation 'l-times cyclic shift', there are l equal length cycles of the co-ordinate positions. A parallel work by Ling and Solé [8] effectively takes the DFT cycle-wise and investigates the structure of quasi-cyclic codes. Their approach is restricted to the case: $(\frac{n}{l}, q) = 1$, a weaker restriction than that $((n, q) = 1)$ needed in our approach. Restriction of the DFT defined in this chapter to the cyclic group G generated by the permutation 'l-times cyclic shift' gives their DFT.

Chapter 5

Codes Closed under Arbitrary Abelian Group of Permutations : Galois Rings

5.1 Introduction

In this chapter, the work of the previous chapter is extended for codes over Galois rings. Other than cyclic codes, work on codes over more general commutative rings have been very limited. Like the previous chapter, works in this chapter includes cyclic codes,quasi-cyclic codes, abelian codes and quasi-abelian codes as special cases.

In Section 5.2, basic properties of Galois rings and the DFT for abelian codes over Galois rings are discussed as a preparation to the later sections. Section 5.3 defines DFT for codes over Galois rings which are closed under arbitrary abelian group of permutations in a very similar way as in the previous chapter for codes over finite fields. Codes over Galois rings which are closed under an arbitrary abelian group G of permutations are characterized in DFT domain in Section 5.4. Dual code of any G-invariant code and the self-dual G-invariant codes are characterized in DFT domain in Section 5.5 and 5.6. The special case of abelian codes over Galois rings is discussed in Section 5.7. Subsection 5.7.1 generalizes the results of [27] on permutation groups of cyclic codes over Galois rings to abelian codes. The minimum distance of G-invariant codes over Galois rings is discussed in Section 5.8. The number of Submodules of $(GR(p^e, m))^l$ is derived in Section 5.9. Section 5.10 concludes this chapter.

5.2 Preliminaries

5.2.1 Galois Rings

Some basic important properties of Galois rings are discussed here. For details on these properties and their proofs, the reader is referred to [95].

Let $\phi(x) \in \mathbb{Z}_{p^e}[x]$ be a basic irreducible polynomial of degree r (such a polynomial exists by Hensel's lemma). The Galois ring $GR(p^e, r)$ is defined as the quotient $\frac{\mathbb{Z}_{p^e}[x]}{(\phi(x))}$. If m is a positive integer such that $m|r$, then $GR(p^e, m)$ is a subring of $GR(p^e, r)$. Moreover, any subring of $GR(p^e, r)$ is of the form $GR(p^e, m)$ for some $m|r$. The ring $GR(p^e, r)$ is a finite chain ring i.e., it is a finite ring whose ideals can be linearly ordered by inclusion. It's only maximal ideal is given by $(p) = pGR(p^e, r)$ and the quotient field is $\frac{GR(p^e,r)}{pGR(p^e,r)} \simeq F_{p^r}$. For any element $u \in GR(p^e, r)$, let us denote by $\bar{u}$, the image of u under the canonical homomorphism of $GR(p^e, r)$ onto F_{p^r}. All the ideals of $GR(p^e, r)$ are ordered as

$$\{0\} = p^e GR(p^e, r) \subset p^{e-1} GR(p^e, r) \subset \cdots \subset p^2 GR(p^e, r) \subset pGR(p^e, r) \subset GR(p^e, r) \quad (5.1)$$

Any element $u \in GR(p^e, r)$ can be expressed as

$$u = p^i u'$$

where $u' \in GR^*(p^e, r)$ and i is unique in this expression. u' is unique upto modulo p^{e-i}. The abelian group $GR^*(p^e, r)$ is direct product of two groups H_1 and H_2, where H_1 is cyclic of order $p^r - 1$ and H_2 is of order $p^{(e-1)r}$. Suppose $H_1 = \{1, \xi, \xi^2, \cdots, \xi^{p^r-2}\}$. Then the set $\mathcal{T}_r = H_1 \cup \{0\} = \{0, 1, \xi, \xi^2, \cdots, \xi^{p^r-2}\}$ forms a set of coset representatives of $GR(p^e, r)$ modulo $pGR(p^e, r)$. Every element $u \in GR(p^e, r)$ can be uniquely expressed as

$$u = u_0 + pu_1 + \cdots + p^{e-1} u_{e-1} \quad (5.2)$$

where $u_0, u_1, \cdots, u_{e-1} \in \mathcal{T}_r$. The Frobenius map on $GR(p^e, r)$ is defined as

$$\begin{aligned} \theta : GR(p^e, r) &\rightarrow GR(p^e, r) \\ u_0 + pu_1 + \cdots + p^{e-1} u_{e-1} &\mapsto u_0^p + pu_1^p + \cdots + p^{e-1} u_{e-1}^p. \end{aligned}$$

This is an automorphism of $GR(p^e, r)$ and fixes only the elements of $\mathbb{Z}_{p^e}$. For $e = 1$, this map reduces to the well known Frobenius automorphism of F_{p^r}.

For any divisor m of r, the map $\theta_m \triangleq \theta^m$ is an automorphism of $GR(p^e, r)$ and fixes only the elements of $GR(p^e, m)$. This map generates the Galois group of $GR(p^e, r)$ over $GR(p^e, m)$. The trace map of $GR(p^e, r)$ into $GR(p^e, m)$ is defined as

$$\begin{aligned} Tr_{(p^e,r,m)} : GR(p^e, r) &\rightarrow GR(p^e, m) \\ a &\mapsto a + \theta_m(a) + \cdots + \theta_m^{\frac{r}{m}-1}(a) \end{aligned}$$

Clearly, the map induced by $Tr_{(p^e,r,m)}$ on the quotient field F_{p^r} is the usual trace map of F_{p^r} over F_{p^m}.

Lemma 5.2.1. *Suppose $u \in GR(p^e, mr)$. If $Tr_{(p^e,rm,m)}(au) = 0 \ \forall a \in GR(p^e, mr)$, then $u = 0$.*

Proof: Let H_1 be the subgroup of $GR^*(p^e, mr)$ of order $p^{mr} - 1$. Then $\exists \alpha \in H_1$, such that $Tr_{(p^e,mr,m)}(\alpha) \notin pGR(p^e, mr)$, since otherwise $\forall \alpha \in H_1$,

$$\begin{aligned} Tr_{(p^e,mr,m)}(\alpha) = \sum_{i=0}^{r-1} \alpha^{q^i} &\in pGR(p^e, mr) \\ \Rightarrow \sum_{i=0}^{r-1} \bar{\alpha}^{q^i} &= 0 \ \forall \bar{\alpha} \in F_{q^r}. \end{aligned}$$

But the left hand side is the usual trace of $\bar{\alpha}$ over F_q. This gives a contradiction, since the usual trace of F_{q^r} over F_q is a nonzero map.

So, $Tr_{(p^e,mr,m)}$ is a nonzero map and hence if $Tr_{(p^e,mr,m)}(au) = 0 \ \forall a \in GR(p^e, mr)$, then $u \in p^i GR(p^e, mr)$ for some $i > 0$. Let i be the maximum positive integer satisfying this. Suppose $u \neq 0$. Then $i \neq e$. So, $uGR(p^e, mr) = p^i GR(p^e, mr)$ and thus

$$Tr_{(p^e,mr,m)}(w) = 0 \quad \forall w \in p^i GR(p^e, mr). \tag{5.3}$$

Suppose, $\alpha \in H_1$ is such that $Tr_{(p^e,mr,m)}(\alpha) \notin pGR(p^e, mr)$. Then $Tr_{(p^e,mr,m)}(p^i\alpha) = p^i Tr_{(p^e,mr,m)}(\alpha) \neq 0$ - contradiction to (5.3). ∎

This lemma shows that the kernel of the map $Tr_{(p^e,mr,m)}$ does not contain any nonzero ideal of $GR(p^e, mr)$ as subset.

5.2.2 DFT for Abelian Codes over Galois Rings

The DFT for abelian codes over Galois rings can be taken as straight forward extension of the known DFT for abelian codes over $\mathbb{Z}_{p^e}$ [63] or DFT for cyclic codes over Galois Rings

[27] or DFT for abelian codes over finite fields [37, 91]. In the last chapter, the DFT for abelian codes over finite fields was discussed using group characters. In this section, the approach is extended to define DFT for abelian codes over Galois rings. Though DFT can be equivalently defined without using the concept of group characters, usage of character tables will simplify notations in the later sections.

Let us consider the Galois ring $GR(p^e, m)$ and the abelian group G with exponent ν relatively prime to p. Let us denote p^m as q. Similar to an F_q-character of G, a $GR(p^e, m)$-character of G is defined as a homomorphism of G into $GR^*(p^e, m)$. Since exponent of G is relatively prime to p, the image of any $GR(p^e, m)$-character of G is a subgroup of $H_1 \subset \mathcal{T}_m$. The set of all $GR(p^e, m)$ characters also forms an abelian group. If r is the smallest positive integer such that ν divides $q^r - 1$, then $GR(p^e, mr)$ is the smallest extension of $GR(p^e, m)$ which contains a ν-th root of unity. Then the group of $GR(p^e, mr)$-characters of G is isomorphic to G.

The following lemma, which is well known for finite fields, is also valid for Galois rings and can be proved similarly as it's counterpart for finite fields.

Lemma 5.2.2. *[91] If $a \in GR(p^e, r)$ has order l, relatively prime to p, then*

$$\sum_{i=0}^{l-1} a^{ij} = \begin{cases} l, & \text{if } j = 0 \\ 0, & \text{if } j \neq 0 \end{cases} \tag{5.4}$$

This lemma allows us to choose a map $\psi : G \times G \to F_{q^r}$ which satisfies the equations (4.1a)-(4.1d).

DFT of any element of $\mathbf{a} \in GR(p^e, m)G$ is defined as $\mathbf{A} \in GR(p^e, mr)G$ such that $A_x = \sum_{y \in G} \psi(x, y) a_y$. The inverse DFT is given by $a_x = |G|^{-1} \sum_{y \in G} \psi(x, y)^{-1} A_y$.

Theorem 5.2.3 (Conjugacy Constraint). *For any $\mathbf{a} \in GR(p^e, m)G$, it's DFT $\mathbf{A}$ satisfies $A_{x^q} = \theta_m(A_x)$.*

Proof:

$$\begin{aligned} \theta_m(A_x) &= \theta_m\left(\sum_{y \in G} \psi(x, y) a_y\right) \\ &= \sum_{y \in G} (\psi(x, y))^q \, \theta_m(a_y) \quad \text{since } \psi(x, y) \in H_1 \\ &= \sum_{y \in G} \psi(x^q, y) a_y \quad \text{since } a_y \in GR(p^e, m) \\ &= A_{x^q} \end{aligned}$$

■

Lemma 5.2.4. *If* $\mathbf{a}, \mathbf{b} \in GR(p^e, m)$ *such that* $\mathbf{b} = g\mathbf{a}$ *i.e.,* $b_x = a_{g^{-1}x}$, $\forall x \in G$ *for some* $g \in G$, *then the corresponding DFT components are related as*

$$B_y = \psi(g, x)A_y \ \forall y \in G \tag{5.5}$$

5.3 DFT for Codes Closed under Arbitrary Abelian Group of Permutations

Let us consider codes over $GR(p^e, m)$ $(p^m = q)$ of length n. Suppose the code symbols are indexed by a finite set I, where $|I| = n$. Let $G \subseteq Perm(I)$ be an abelian subgroup of the group of permutations of I. The DFT for G-invariant codes over Galois rings can be defined in the same way as in chapter 4 (for codes over finite fields).

Let the exponent of G be relatively prime to q. Then on each orbit, we can define DFT as discussed in the last section. For any $\mathbf{a} \in (GR(p^e, m))^{\mathcal{G}}$, the DFT is defined orbit wise. That is, the DFT of $\mathbf{a}$ is defined as $\mathbf{A}$, where

$$A_x = \sum_{y \in G_k} \psi_k(x, y)a_y \qquad \forall x \in G_k, \ \forall k.$$

Here ψ_k is ψ (as defined in the last section) for G_k. Clearly, the DFT components A_x are in $GR(p^e, mr)$, where r is the smallest positive integer such that $exp(G)$ divides $q^r - 1$.

Definition 13. For any two $x, y \in \mathcal{G}$, let us define

$$\Psi(x, y) = \begin{cases} \psi_k(x, y), & \text{when } x, y \in G_k \text{ for some } k \\ 0, & \text{when } x \in G_{k_1} \text{ and } y \in G_{k_2} \text{ s. t. } k_1 \neq k_2 \end{cases}$$

With this notation, the DFT can be re-written as

$$A_x = \sum_{y \in \mathcal{G}} \Psi(x, y)a_y \qquad \forall x \in \mathcal{G}. \tag{5.6}$$

Definition 14. For any $h \in G$, and $x \in \mathcal{G}$ let us define the symbol

$$\langle h, x \rangle \stackrel{\triangle}{=} \psi_k(h^{(k)}, x) \quad \text{when } x \in G_k. \tag{5.7}$$

It follows from this definition that the DFT of $\mathbf{b} = h(\mathbf{a})$ is given by $B_x = \langle h, x \rangle A_x$.

For any element $x \in \mathcal{G}$, it is in G_k for some k and so cyclotomic coset of x is defined in the same way as in the previous section as $[x]^q \triangleq \{y \in G_k | y = x^{q^t} \text{ for some non-negative } t\}$. Similarly, r_x will denote the cardinality of $[x]^q$. By the same argument as in Corollary 5.2.3, the DFT components in a cyclotomic coset are related by $A_{x^q} = \theta_m(A_x)$.

Corollary 5.3.1. *For any $x \in \mathcal{G}$, r_x is the smallest positive integer such that $\langle g, x\rangle^{q^{r_x}} = \langle g, x\rangle \ \forall g \in G$.*

So, r_x is the *lcm* of the lengths of the conjugacy classes of $\langle g, x\rangle$; $\forall g \in G$.

The residue class and cyclotomic residue class are defined in the same way as in the previous chapter. And they have the same structure as before i.e., as depicted in Figure 4.9.

Example 5.3.1. Consider the same permutation group G of Example 4.3.1. Let H_1 be the subgroup of $GR^*(p^e, mr)$ of order $p^{mr} - 1$. If $\alpha \in H_1$ is an element of order 15, then DFT in $(GR(p^e, mr))^{16} \simeq (GR(p^e, mr))^{\mathcal{G}}$ is defined with respect to the maps ψ_k defined by:

$$\psi_1(g_1, g_1) = \alpha^5$$
$$\psi_2(g_2, g_2) = \alpha^5$$
$$\psi_3(g_3, g_3) = \alpha^3$$
$$\psi_4(g_4, g_4) = \alpha^3$$

The residue classes in $\mathcal{G}$ are shown in Figure 4.4 with dashed boxes.

Definition 15. The **Cyclotomic residue class** of $x \in \mathcal{G}$ is defined as

$$\begin{aligned}(x)^q &\triangleq \{x_1 \in \mathcal{G} | \text{ for some non-negative t}, \langle g, x_1\rangle^{q^t} = \langle g, x\rangle \ \forall g \in G\} \\ &= [\widetilde{x}]^q.\end{aligned} \quad (5.8)$$

By the conjugacy constraint, values of DFT components in one residue class determines values of other transform components in the same cyclotomic residue class. To be specific, $A_{\widetilde{x^{q^i}}} = \theta_m^i(A_{\widetilde{x}})$ for any $\mathbf{a} \in (GR(p^e, m))^{\mathcal{G}}$, where the action of θ_m on $A_{\widetilde{x}}$ is component wise. So, values of transform components in one representative residue class from each cyclotomic residue class specifies a vector completely.

In the following, for any subset $S \subseteq GR^*(p^e, mr)$, we'll denote the multiplicative subgroup of $GR^*(p^e, mr)$ generated by S as $\langle S\rangle$ and the smallest extension ring of $GR(p^e, m)$

containing S as $GR(p^e, m)(S)$. Clearly, $GR(p^e, m)(S) = GR(p^e, ml)$ where l is the smallest positive integer such that $s^{q^l} = s\,;\ \forall s \in S$. So for any $x \in \mathcal{G}$, Corollary 5.3.1 gives

$$GR(p^e, m)\,(\{\langle g, x\rangle | g \in G\}) = GR(p^e, mr_x). \tag{5.9}$$

Lemma 5.3.2. *For any subset $S \subseteq GR^*(p^e, mr)$, $Span_{GR(p^e,m)}(\langle S\rangle) = GR(p^e, m)(S)$.*

Proof: Let us denote $Span_{GR(p^e,m)}(\langle S\rangle)$ by V. Clearly, $V \subseteq GR(p^e, m)(S)$. It is now sufficient to prove that V is a subring of $GR(p^e, mr)$. Clearly, V is closed under multiplication and $1 \in V$. So, V is a subring of $GR(p^e, mr)$. ■

5.4 Transform Domain Characterization of G-Invariant Codes

If in a G-invariant code, two transform components A_x and A_y are unrelated, then consider the subcodes $\mathcal{C}_1$ and $\mathcal{C}_2$ obtained by restricting respectively A_x and A_y to $\{0\}$. Clearly, the original code is sum of the codes $\mathcal{C}_1$ and $\mathcal{C}_2$. Suppose $S_1, \cdots, S_l$ are some disjoint subsets of the index set such that $x, y \in \cup_{i=1}^{l} S_i$. Then the transform components in $S_1, \cdots, S_l$ are unrelated in $\mathcal{C}$ if and only if they are unrelated in $\mathcal{C}_1$ and $\mathcal{C}_2$. We can continue this process on $\mathcal{C}_1$ and $\mathcal{C}_2$ and repeatedly on the resulting subcodes to get a set of subcodes whose sum is $\mathcal{C}$ and in each of which either there is only one nonzero transform component or any pair of nonzero transform components is related. So, if the transform components in $S_1, \cdots, S_l$ are related in $\mathcal{C}$, then there is a G-invariant subcode of $\mathcal{C}$ where two transform components $A_x, A_y\,;\ x \in S_i\,, y \in S_j\ ; i \neq j$ are related.

Lemma 5.4.1. *Let V be a one dimensional vector space over $F_{q^{l'}}$ and W be a vector space over $F_q(\overline{\beta}_1, \cdots, \overline{\beta}_k)$. If $\sigma : V \longrightarrow W$ satisfies*

$$\sigma(\overline{\alpha}_i b) = \overline{\beta}_i \sigma(b)\ \forall b \in V \tag{5.10}$$

then there exists a non-negative integer j such that $\overline{\beta}_i = \overline{\alpha}_i^{q^j}$ for all $i = 1, \cdots k$.

Proof: Using Lemma 4.4.5. ■

Lemma 5.4.2. *Let $\alpha_i\,;\ i = 1, \cdots, k$ and $\beta_i\,;\ i = 1, \cdots, k$ be some elements of $GR(p^e, mr)^*$ with order relatively prime to p. Suppose $GR(p^e, m)(\alpha_1, \cdots, \alpha_k) = GR(p^e, ml_1)$ and $GR(p^e, m)(\alpha_1, \cdots, \alpha_k) = GR(p^e, ml_2)$. If $R \subsetneq p^{r_1} GR(p^e, ml_1) \times p^{r_2} GR(p^e, ml_2)\,;\ r_1, r_2 < e$*

is a $GR(p^e,m)$ *module with* $\{a|(a,b) \in R \text{ for some } b\} = p^{r_1}GR(p^e,ml_1)$, $\{b|(a,b) \in R \text{ for some } a\} = p^{r_2}GR(p^e,ml_2)$ *and*

$$(a,b) \in R \Rightarrow (\alpha_i a, \beta_i b) \in R \text{ ; for } i = 1,\cdots,k, \tag{5.11}$$

then there exists a non-negative integer j *such that* $\beta_i = \alpha_i^{q^j}$ *for all* $i = 1,\cdots k$.

Proof: For any $V \subseteq p^{r_1}GR(p^e,ml_1)$, we shall call $\{(a,b) \in R|a \in V\}$ as the subset of R obtained by restricting a to V. Similarly for any $V \subseteq p^{r_2}GR(p^e,ml_2)$, we shall call $\{(a,b) \in R|b \in V\}$ as the subset of R obtained by restricting b to V.

Without loss of generality, we can assume that $\{b|(a,b) \in R; a \in p^{r_1+1}GR(p^e,ml_1)\} = p^{r_3}GR(p^e,ml_2)$ for some $r_3 > r_2$. Since otherwise, we can take the smallest $r_4 > r_1$ such that $\{b|(a,b) \in R; a \in p^{r_4}GR(p^e,ml_1)\} = p^{r_3}GR(p^e,ml_2)$ for some $r_3 > r_2$ and instead of R, we can consider the subset of R obtained by restricting a to $p^{r_4-1}GR(p^e,ml_1)$.

Now, consider the subset

$$\overline{R} \subseteq \frac{p^{r_1}GR(p^e,ml_1)}{p^{r_1+1}GR(p^e,ml_1)} \times \frac{p^{r_2}GR(p^e,ml_2)}{p^{r_2+1}GR(p^e,ml_2)} = \{(\overline{a},\overline{b})|(a,b) \in R\} \tag{5.12}$$

induced by R. Here $\overline{a}$ and $\overline{b}$ denote the images of a and b in $\frac{p^{r_1}GR(p^e,ml_1)}{p^{r_1+1}GR(p^e,ml_1)}$ and $\frac{p^{r_2}GR(p^e,ml_2)}{p^{r_2+1}GR(p^e,ml_2)}$ respectively. $\overline{R} \neq \frac{p^{r_1}GR(p^e,ml_1)}{p^{r_1+1}GR(p^e,ml_1)} \times \frac{p^{r_2}GR(p^e,ml_2)}{p^{r_2+1}GR(p^e,ml_2)}$ since $\{b|(a,b) \in R; a \in p^{r_1+1}GR(p^e,ml_1)\} \subseteq p^{r_2+1}GR(p^e,ml_2)$. Now, $\frac{p^{r_1}GR(p^e,ml_1)}{p^{r_1+1}GR(p^e,ml_1)}$ is a $GR(p^e,ml_1)$ module with anihilator $pGR(p^e,ml_1)$ and $\frac{p^{r_2}GR(p^e,ml_2)}{p^{r_2+1}GR(p^e,ml_2)}$ is a $GR(p^e,ml_2)$ module with anihilator $pGR(p^e,ml_2)$. So, $\frac{p^{r_1}GR(p^e,ml_1)}{p^{r_1+1}GR(p^e,ml_1)}$ is a $\frac{GR(p^e,ml_1)}{pGR(p^e,ml_1)} \simeq GF(p^{ml_1})$-vector space. Since it's cardinality is p^{ml_1}, it's dimension is one. Similarly $\frac{p^{r_2}GR(p^e,ml_2)}{p^{r_2+1}GR(p^e,ml_2)}$ is a one dimensional $\frac{GR(p^e,ml_2)}{pGR(p^e,ml_2)} \simeq GF(p^{ml_2})$-vector space. Since $\{\overline{b}|(0,\overline{b}) \in \overline{R}\} = \{0\}$, for any $\overline{a} \in \frac{p^{r_1}GR(p^e,ml_1)}{p^{r_1+1}GR(p^e,ml_1)}$, there is a unique $\overline{b}$ such that $(\overline{a},\overline{b}) \in \overline{R}$. This defines a map $\sigma : \frac{p^{r_1}GR(p^e,ml_1)}{p^{r_1+1}GR(p^e,ml_1)} \longrightarrow \frac{p^{r_2}GR(p^e,ml_2)}{p^{r_2+1}GR(p^e,ml_2)}$ satisfying equation (5.10). So by Lemma 5.4.1, there exists a non-negative integer j such that $\overline{\alpha}_i = \overline{\beta}_i^{q^j} \Rightarrow \alpha_i^{q^j} = \beta_i^{q^j}$; for $i = 1,\cdots,k$. ■

Theorem 5.4.3 (Transform Domain Characterization). *Let* G *be an abelian group of permutations with order relatively prime to* q. *Then a code over* $GR(p^e,m)$ *is* G*-invariant if and only if*

1. *For any* $x \in \mathcal{G}$, $A_{\widetilde{x}}$ *takes values from a submodule of* $(GR(p^e,mr_x))^{e_x}$.

2. *If* $x_1,\cdots,x_k$ *are representatives of the distinct cyclotomic residue classes of* $\mathcal{G}$, *then* $A_{\widetilde{x_1}},\cdots,A_{\widetilde{x_k}}$ *are unrelated.*

5.5 Duals of G-Invariant Codes : The Case $|G_1| \equiv |G_2| \equiv \cdots \equiv |G_t| \bmod p^e$

For two vectors $\mathbf{a}, \mathbf{b} \in (GR(p^e, m))^{\mathcal{G}}$, the Euclidean inner product of them is defined as

$$E(\mathbf{a}, \mathbf{b}) = \sum_{x \in \mathcal{G}} a_x b_x \tag{5.13}$$

The Euclidean inner product of $\mathbf{a}$ and $\mathbf{b}$ will also be denoted by $\mathbf{a}.\mathbf{b}$. For two vectors $\mathbf{a}, \mathbf{b} \in (GR(p^e, 2m))^{\mathcal{G}}$, their Hermitian inner product is defined as

$$H(\mathbf{a}, \mathbf{b}) = \sum_{x \in \mathcal{G}} a_x \theta_m(b_x) \tag{5.14}$$

Two vectors are called orthogonal w. r. t. Euclidean or Hermitian inner product, if respectively the Euclidean or Hermitian inner product of the vectors is zero. Two codes $\mathcal{C}_1$ and $\mathcal{C}_2$, are called Euclidean dual of each other if $\mathcal{C}_2 = \{\mathbf{b} | E(\mathbf{a}, \mathbf{b}) = 0\,;\, \forall \mathbf{a} \in \mathcal{C}_1\}$. Similarly Hermitian dual codes are defined. Euclidean duality will simply be referred as duality and explicitly mention Hermitian duality when needed. A code is called self dual when it is dual of itself. Similarly a code is called Hermitian self dual when it is Hermitian dual of itself. A code is called self-orthogonal if it is a subcode of it's dual.

Clearly, dual of a G-invariant code is also G-invariant.

In this section, only case when all the orbit cardinalities are same modulo p is considered. This case gives fairly simple characterization of dual and self dual G-invariant codes and all the special cases fall under this case.

Theorem 5.5.1. *Let G be such that $|G_1| \equiv ... \equiv |G_t|$ mod p^e. For a G-invariant code $\mathcal{C}$, a vector $\mathbf{b} \in (GR(p^e, m))^{\mathcal{G}}$ is orthogonal to $\mathcal{C}$ if and only if for all $\mathbf{a} \in \mathcal{C}$,*

$$\sum_{y \in \widetilde{x}} A_y B_{y^{-1}} = 0 \qquad \text{for all cyclotomic residue classes } (x)^q \tag{5.15}$$

Proof: Clearly, $\mathbf{b}$ is orthogonal to $\mathcal{C}$ if and only if

$$\begin{aligned} \mathbf{a} \perp \mathbf{b}\,;\, \forall \mathbf{a} \in \mathcal{C} \quad &\Longleftrightarrow \quad \sum_{y \in \mathcal{G}} a_y b_y = 0 \quad \forall \mathbf{a} \in \mathcal{C} \\ &\Longleftrightarrow \quad \sum_{y \in \mathcal{G}} A_y B_{y^{-1}} = 0 \quad \forall \mathbf{a} \in \mathcal{C} \quad \text{since } |G_1| \equiv ... \equiv |G_t| \bmod p^e \\ &\Longleftrightarrow \quad \sum_{y \in (x)^q} A_y B_{y^{-1}} = 0 \text{ for each cyclotomic coset } (x)^q, \quad \forall \mathbf{a} \in \mathcal{C} \end{aligned} \tag{5.16}$$

$$\begin{aligned}
&\Longleftrightarrow \quad \sum_{i=0}^{r_x-1}\sum_{y\in\widetilde{x}} A_{y^{q^i}} B_{\left(y^{q^i}\right)^{-1}} = 0 \quad \text{''} \\
&\Longleftrightarrow \quad \sum_{i=0}^{r_x-1}\sum_{y\in\widetilde{x}} A_{y^{q^i}} B_{(y^{-1})^{q^i}} = 0 \quad \text{''} \\
&\Longleftrightarrow \quad \sum_{i=0}^{r_x-1}\sum_{y\in\widetilde{x}} \theta_m^i(A_y)\theta_m^i(B_y^{-1}) = 0 \quad \text{''} \\
&\Longleftrightarrow \quad \sum_{i=0}^{r_x-1} \theta_m^i\left(\sum_{y\in\widetilde{x}} A_y B_{y^{-1}}\right) = 0 \quad \text{''} \\
&\Longleftrightarrow \quad Tr_{(p^e,mr_x,m)}\left(\sum_{y\in\widetilde{x}} A_y B_{y^{-1}}\right) = 0 \quad \text{''} \\
&\Longleftrightarrow \quad \sum_{y\in\widetilde{x}} A_y B_{y^{-1}} = 0 \quad \text{''} \qquad (5.17)
\end{aligned}$$

The fact that transform components in different cyclotomic residue classes are unrelated for G-invariant code is used to get (5.16), and (5.17) is obtained by using Lemma 5.2.1 and the fact that $A_{\widetilde{x}}$ takes values from a submodule of $(GR(p^e, mr_x))^{e_x}$. ■

Note that if (5.15) is satisfied for a residue class $\widetilde{x}$ then it is also satisfied for any other residue class in the same cyclotomic residue class. So, it is sufficient to consider only one representative residue class in each cyclotomic residue class. When two residue classes $\widetilde{x}$ and $\widetilde{x^{-1}}$ are considered, the compatible orders are taken in them, i.e. if $A_{\widetilde{x}} = \left(A_x, A_{x_1}, \cdots, A_{x_{e_x-1}}\right)$, then $A_{\widetilde{x^{-1}}} = \left(A_{x^{-1}}, A_{x_1^{-1}}, \cdots, A_{x_{e_x-1}^{-1}}\right)$.

Let $\{x_1, x_2, \cdots, x_l\}$ be a set of representatives of the distinct cyclotomic residue classes of $\mathcal{G}$. Suppose, for the codes $\mathcal{C}_1$ and $\mathcal{C}_2$, $A_{\widetilde{x}}$ takes values from V_x and U_x respectively. Then V_x and U_x can also be considered as linear codes of length e_x over $F_{q^{r_x}}$. Using Theorem 5.5.1, the following characterization of the dual code of a G-invariant code is obtained.

Theorem 5.5.2. *Let G be such that $|G_1| \equiv ... \equiv |G_t|$ mod p^e. Suppose $\{x_1, x_2, \cdots, x_l\}$ is a set of representatives of the distinct cyclotomic residue classes in $\mathcal{G}$. Two G-invariant codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are dual of each other if and only if for each x_i; $i = 1, 2, \cdots, l$, V_{x_i} and $U_{x_i^{-1}}$ are dual codes of each other.*

5.5.1 Self Dual G-Invariant Codes

Let us denote the distinct self inverse cyclotomic residue classes as $(x_1)^q, \cdots, (x_{i_1})^q, (y_1)^q, \cdots,$ $(y_{i_2})^q$ and the other distinct cyclotomic residue classes as $(z_1)^q, (z_1^{-1})^q \cdots, (z_{i_3})^q, (z_{i_3}^{-1})^q$, where $x_i = x_i^{-1}$ for $i = 1, \cdots, i_1$ and $y_i \neq y_i^{-1}$ for $i = 1, \cdots, i_2$. The following theorem gives the transform domain characterization of self dual G-invariant code. This theorem and the other subsequent results in this section are stated without proofs, since their finite field versions are already present in Chapter 4 and their proofs for codes over Galois rings are similar to those for codes over finite fields.

Theorem 5.5.3. *Let G be such that $|G_1| \equiv ... \equiv |G_t| \bmod p^e$ and $\mathcal{C}$ be a G-invariant code over $GR(p^e, m)$, where $A_{\widetilde{x_i}}$, $A_{\widetilde{y_j}}$, $A_{\widetilde{z_k}}$ and $A_{\widetilde{z_k^{-1}}}$ take values from the submodules V_{x_i}, V_{y_j}, V_{z_k} and $V_{z_k^{-1}}$ respectively for $i = 1, \cdots, i_1$; $j = 1, \cdots, i_2$; $k = 1, \cdots, i_3$. The code is self dual if and only if*

1. *V_{x_i} is a self-dual code for $i = 1, \cdots, i_1$.*

2. *V_{y_j} is a Hermitian self-dual code for $j = 1, \cdots, i_2$.*

3. *V_{z_k} is the dual code of $V_{z_k^{-1}}$ for $k = 1, \cdots, i_3$.*

Corollary 5.5.4. *Suppose $[f_1]^q, \cdots, [f_{i_1}]^q, [g_1]^q, \cdots, [g_{i_2}]^q$ are the self-inverse q-cyclotomic cosets in G such that $f_i^{-1} = f_i$; for $1 \leq i \leq i_1$ and $g_i^{-1} \neq g_i$; for $1 \leq i \leq i_2$ and $[h_1]^q, [h_1^{-1}]^q, \cdots, [h_{i_3}]^q, [h_{i_3}^{-1}]^q$ are the other q-cyclotomic cosets in G. Then a G-quasi-abelian code $\mathcal{C}$ of length $t|G|$ over $GR(p^e, m)$ is self-dual if and only if*

1. *V_{f_i} is a self-dual code for $i = 1, \cdots, i_1$.*

2. *V_{g_j} is a Hermitian self-dual code for $j = 1, \cdots, i_2$.*

3. *V_{h_k} is the dual code of $V_{h_k^{-1}}$ for $k = 1, \cdots, i_3$.*

The number of self dual codes and Hermitian self dual codes of any length over finite fields is known [93, 94] and are given in the last chapter. Let us denote by $N_E(p^e, m, l)$ and $N_H(p^e, m, l)$, the number of self dual and Hermitian self dual codes of length l over $GR(p^e, m)$. Also, let $N(p^e, m, l)$ denote the number of submodules of $(GR(p^e, m))^l$. The exact values of $N_E(p^e, m, l)$ and $N_H(p^e, m, l)$ are not known for arbitrary p, e and m. In [96], the value of $N_E(2^2, 1, l)$ is computed and it is

$$N_E(2^2,1,l) = \sum_{i=0}^{\frac{l}{2}} \sigma(l,i) 2^{\frac{i(i+1)}{2}} \tag{5.18}$$

where $\sigma(l,i)$ is the number of binary self-orthogonal $[l,i]$ codes with all weights divisible by 4 and is equal to 1 if $i = 0$ and otherwise given by

$$\prod_{j=0}^{i-1} \frac{2^{k-2j-2} + 2^{[\frac{k}{2}]-i-1} - 1}{2^{i+1}-1}, \quad \text{if } k \equiv \pm 1 \pmod 8$$

$$\prod_{j=0}^{i-1} \frac{2^{k-2j-2} - 1}{2^{i+1}-1}, \quad \text{if } k \equiv \pm 2 \pmod 8$$

$$\prod_{j=0}^{i-1} \frac{2^{k-2j-2} - 2^{[\frac{k}{2}]-i-1} - 1}{2^{i+1}-1}, \quad \text{if } k \equiv \pm 3 \pmod 8$$

$$\left[\prod_{j=0}^{i-2} \frac{2^{k-2j-2} + 2^{[\frac{k}{2}]-i-1} - 1}{2^{i+1}-1}\right] \cdot \left[\frac{1}{2^{i-1}} + \frac{2^{k-2i} + 2^{\frac{k}{2}-i} - 2}{2^i - 1}\right], \quad \text{if } k \equiv \pm 0 \pmod 8$$

$$\left[\prod_{j=0}^{i-2} \frac{2^{k-2j-2} - 2^{[\frac{k}{2}]-i-1} - 1}{2^{i+1}-1}\right] \cdot \left[\frac{1}{2^{i-1}} + \frac{2^{k-2i} - 2^{\frac{k}{2}-i} - 2}{2^i - 1}\right], \quad \text{if } k \equiv \pm 4 \pmod 8$$

It is shown in the appendix that the number of submodules of $(GR(p^e, m))^l$ of type $(k_0, k_1, \cdots, k_{e-1})$ is

$$N_{(k_0,k_1,\cdots,k_e)}(p^e, m, l) = \prod_{i=0}^{e-1} \prod_{j=0}^{k_i-1} \frac{p^{(e-i)m(l-k'_{i-1}-j)} - p^{(e-i-1)m(l-k'_{i-1}-j)}}{p^{m\eta_{i,j}} - p^{m(\eta_{i,j}-k_i+j)}}. \tag{5.19}$$

where $k'_{-1} = 0$, $k'_i = k'_{i-1} + k_i$ for $k \geq 0$, and $\eta_{i,j} = (k_i - j)(e-i) + k_{i+1}(e-i-1) + \cdots + k_{e-1}$.

The number of submodules of $(GR(p^e, m))^l$ is then

$$N(p^e, m, l) = \sum_{\substack{(k_0,\cdots,k_{e-1}) \\ k_0+\cdots+k_{e-1} \leq l}} N_{(k_0,\cdots,k_{e-1})}(p^e, m, l) \tag{5.20}$$

Theorem 5.5.3 directly gives:

Theorem 5.5.5. *Let G be such that $|G_1| \equiv ... \equiv |G_t|$ mod p^e. Number of self dual G-invariant codes over $GR(p^e, m)$ is $\prod_{i=1}^{i_1} N_E(p^e, mr_{x_i}, e_{x_i}) \prod_{j=1}^{i_2} N_H(p^e, mr_{y_j}, e_{y_j}) \prod_{k=1}^{i_3} N(p^e, mr_{z_k}, e_{z_k})$, where the empty product is 1 by convention.*

In the above theorem, the first factor is contributed by the Type A cyclotomic residue classes, the second factor is contributed by Type B cyclotomic residue classes and the third factor is contributed by the Type C cyclotomic residue classes.

Corollary 5.5.6. *Let G be an abelian group with order relatively prime to p. Suppose $[f_1]^q, \cdots, [f_{i_1}]^q$ are the Type A q-cyclotomic cosets, $[g_1]^q, \cdots, [g_{i_2}]^q$ are the Type B q-cyclotomic cosets and $[h_1]^q, [h_1^{-1}]^q, \cdots, [h_{i_3}]^q, [h_{i_3}^{-1}]^q$ are the Type C q-cyclotomic cosets in G. Then the number of self-dual G-quasi-abelian codes of length $t|G|$ over $GR(p^e, m)$ is $\prod_{i=1}^{i_1} N_E(p^e, mr_{f_i}, t) \prod_{j=1}^{i_2} N_H(p^e, mr_{g_j}, t) \prod_{k=1}^{i_3} N(p^e, mr_{h_k}, t)$.*

For l-quasi-cyclic codes, $G \simeq G_k \simeq \mathbb{Z}_{\frac{n}{l}}$. In this case, the q-cyclotomic cosets in $\mathbb{Z}_{\frac{n}{l}}$ are the q-cyclotomic cosets modulo $\frac{n}{l}$, which play an important role in case of cyclic codes of length $\frac{n}{l}$. Each residue class contains one element from each orbit. It is well known that there is a $1-1$ correspondence between the prime factors of the polynomial $Y^{\frac{n}{l}} - 1$ and the q-cyclotomic cosets modulo $\frac{n}{l}$. The degree of a prime factor of $Y^{\frac{n}{l}} - 1$ is same as the cardinality r_j of the corresponding q-cyclotomic coset $[j]^q$. Moreover, the self reciprocal cyclotomic cosets in $\mathbb{Z}_{\frac{n}{l}}$ correspond to the prime factors $f(Y)$ whose reciprocal polynomial $f^*(Y)$ is an associate of $f(Y)$. We'll call such polynomials as self reciprocal polynomials.

For any $k \in \mathbb{Z}_{\frac{n}{l}}$, if $-k \equiv k \bmod \frac{n}{l}$, then $2k \equiv 0 \bmod \frac{n}{l} \Rightarrow k \equiv 0 \bmod \frac{n}{l}$ or $k \equiv \frac{\frac{n}{l}}{2} \bmod \frac{n}{l}$ for even $\frac{n}{l}$. So,

$$i_1 = \begin{cases} 1 & \text{if } \frac{n}{l} \text{ is odd} \\ 2 & \text{if } \frac{n}{l} \text{ is even} \end{cases}.$$

Corollary 5.5.6 specializes for quasi-cyclic codes as following.

Corollary 5.5.7. *Let $\frac{n}{l}$ be a positive integer relatively prime to q. Suppose $[x_1]^q, \cdots, [x_{i_1}]^q$ are the Type A q-cyclotomic cosets modulo $\frac{n}{l}$, $[y_1]^q, \cdots, [y_{i_2}]^q$ are the Type B q-cyclotomic cosets modulo $\frac{n}{l}$ and $[z_1]^q, [-z_1]^q, \cdots, [z_{i_3}]^q, [-z_{i_3}]^q$ are the Type C q-cyclotomic cosets modulo $\frac{n}{l}$. Then the number of self-dual l-quasi-cyclic codes of length n over $GR(p^e, m)$ is $\prod_{i=1}^{i_1} N_E(q^{r_{x_i}}, l) \prod_{j=1}^{i_2} N_H(q^{r_{y_j}}, l) \prod_{k=1}^{i_3} N(q^{r_{z_k}}, l)$.*

5.6 Duals of G-Invariant Codes : The General Case

To characterize duals of G-invariant codes, some generalizations of Euclidean and Hermitian dual codes are needed. Let $\mathbf{v} = (v_1, \cdots, v_l) \subseteq (GR(p^e, m))^l$ be such that each component is invertible. For any two vectors $\mathbf{a}, \mathbf{b} \in (GR(p^e, m))^l$, let us define the **v**-weighted Euclidean inner product (or $E_{\mathbf{v}}$ inner product) of **a** and **b** as

$$E_{\mathbf{v}}(\mathbf{a}, \mathbf{b}) = \sum_{x=1}^{l} v_x a_x b_x \tag{5.21}$$

Similarly for any $\mathbf{v} \in (GR(p^e, m))^l$, **v**-weighted Hermitian inner product or $H_{\mathbf{v}}$-inner product of $\mathbf{a} \in (GR(p^e, 2m))^l$ and $\mathbf{b} \in (GR(p^e, 2m))^l$ is defined as

$$H_{\mathbf{v}}(\mathbf{a}, \mathbf{b}) = \sum_{x=1}^{l} v_x a_x \theta_m(b_x) \tag{5.22}$$

Note that, since $\mathbf{v} \in (GR(p^e, 2m))^l$, $H_{\mathbf{v}}(\mathbf{a}, \mathbf{b}) = 0$ if and only if $H_{\mathbf{v}}(\mathbf{b}, \mathbf{a}) = 0$ since $H_{\mathbf{v}}(\mathbf{a}, \mathbf{b}) = \theta_m(H_{\mathbf{v}}(\mathbf{b}, \mathbf{a}))$.

For any $x \in \mathcal{G}$, let us denote by i_x, the cardinality of the orbit containing x. For any residue class $\widetilde{x}$, $i_{\widetilde{x}}$ will denote the e_x-tuple with components i_y ; $y \in \widetilde{x}$ in the same order as A_y's in $A_{\widetilde{x}}$. With missuse of notation, $i_{\widetilde{x}}^{-1}$ will denote the component-wise inverse (in $\mathbb{Z}_{p^e} \subseteq GR(p^e, m)$) of $i_{\widetilde{x}}$.

Now, Theorem 5.5.1 can be generalized to:

Theorem 5.6.1. *For a G-invariant code $\mathcal{C}$, a vector $\mathbf{b} \in (GR(p^e, m))^{\mathcal{G}}$ is orthogonal to $\mathcal{C}$ if and only if for all $\mathbf{a} \in \mathcal{C}$,*

$$\sum_{y \in \widetilde{x}} i_y^{-1} A_y B_{y^{-1}} = 0 \qquad \textit{for all cyclotomic residue classes } (x)^q \tag{5.23}$$

So in general, two G-invariant codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are duals of each other if and only if for each x_i ; $i = 1, 2, \cdots, l$ (see Theorem 5.5.2), V_{x_i} and U_{x_i} are $E_{\mathbf{i}_{\widetilde{x_i}}^{-1}}$-duals of each other. This gives a modified versions of Theorem 5.5.3 and 5.5.5 as bellow. Here $N_{E_{\mathbf{i}_{\widetilde{x_i}}^{-1}}}(p^e, m, l)$ and $N_{H_{\mathbf{i}_{\widetilde{x_i}}^{-1}}}(p^e, m, l)$ denote the number of respectively $E_{\mathbf{i}_{\widetilde{x_i}}^{-1}}$-self dual codes and $H_{\mathbf{i}_{\widetilde{x_i}}^{-1}}$-self dual codes of length l over $GR(p^e, m)$.

Theorem 5.6.2. *Let $\mathcal{C}$ be a G-invariant code over $GR(p^e, m)$, where $A_{\widetilde{x_i}}$, $A_{\widetilde{y_j}}$, $A_{\widetilde{z_k}}$ and $A_{\widetilde{z_k^{-1}}}$ takes values from the submodules V_{x_i}, V_{y_j}, V_{z_k} and $V_{z_k^{-1}}$ respectively for $i = 1, \cdots, i_1$; $j = 1, \cdots, i_2$; $k = 1, \cdots, i_3$. The code is self dual if and only if*

1. *V_{x_i} is a $E_{\mathbf{i}_{\widetilde{x_i}}}$-self-dual code for $i = 1, \cdots, i_1$.*

2. *V_{y_j} is a $H_{\mathbf{i}_{\widetilde{y_j}}}$-Hermitian self-dual code for $j = 1, \cdots, i_2$.*

3. V_{z_k} *is the* $E_{\mathbf{i}_{\widetilde{z_k}}}$*-dual code of* $V_{z_k^{-1}}$ *for* $k = 1, \cdots, i_3$.

Theorem 5.6.3. *Number of self dual G-invariant codes over* $GR(p^e, m)$ *is* $\prod_{i=1}^{i_1} N_{E_{\mathbf{i}_{\widetilde{x_i}}}}(p^e, mr_{x_i}, e_{x_i}) \prod_{j=1}^{i_2} N_{H_{\mathbf{i}_{\widetilde{y_j}}}}(p^e, mr_{y_j}, e_{y_j}) \prod_{k=1}^{i_3} N(p^e, mr_{z_k}, e_{z_k})$*, where the empty product is 1 by convention.*

For some special cases, the following theorem allows computation of the number of weighted self-dual codes in terms of the number of self-dual codes.

Theorem 5.6.4. *If either all components of* $\mathbf{v} \in (GR^*(p^e, m))^l$ *are quadratic residues or all components are quadratic non-residues, then* $N_{E_{\mathbf{v}}}(p^e, m, l) = N_E(p^e, m, l)$.

Proof: Like the case with finite fields, ratio or product of two quadratic non-residues in $GR^*(p^e, m)$ are quadratic residues. So, the same proof (see Theorem 4.6.4) holds. ■

5.7 Abelian Codes in Transform Domain

In this section, the special case: abelian codes over Galois rings is discussed. In [27], the authors characterized cyclic codes over Galois rings in terms of Mattson-Solomon polynomial or DFT. Our DFT domain characterization of codes closed under arbitrary abelian group specializes to abelian codes and gives a similar description of any abelian code in DFT domain.

The G-invariant codes are exactly the abelian codes on the group G if and only if there is only one orbit of the index set under the action of G. So, the code components are usually indexed by the elements of G. The transform domain characterization of G-invariant codes gives as a special case, the following transform domain characterization of abelian codes on any abelian group G with exponent relatively prime to p.

Theorem 5.7.1. *Let G be an abelian group of order relatively prime to q. Then a code of length $|G|$ (and components indexed by G) over* $GR(p^e, m)$ *is G-abelian if and only if*

1. *For any* $x \in G$, A_x *takes values from an ideal of* $GR(p^e, mr_x)$.

2. *If* $x_1, \cdots, x_k$ *are representatives of the distinct cyclotomic cosets of G, then* $A_{x_1}, \cdots, A_{x_k}$ *are unrelated.*

So, any abelian code on G is completely specified by the ideals of the transform components, in particular by the ideals of the transform components $A_{x_1}, \cdots, A_{x_k}$. But any ideal of $GR(p^e, mr_x)$ is of the form $p^j GR(p^e, mr_x)$ for some j. So, for any j; $0 \leq j \leq e$, there is a maximal subset $T_j \subseteq G$, such that for all $x \in T_j$, A_x takes values from $p^k GR(p^e, mr_x)$ for some $k \geq j$. Clearly, for any j, T_j is a union of q-cyclotomic cosets, since all the transform components in a particular cyclotomic coset take values from the same ideal. T_j; $0 \leq j \leq e$ are ordered as:

$$T_e \subseteq T_{e-1} \subseteq \cdots \subseteq T_1 \subseteq T_0 = G.$$

Similar to cyclic codes, $(T_1, \cdots, T_a)$ will be called the defining sets of the abelian code. The type of the code $(k_0, \cdots, k_{e-1})$ is given by $k_i = |T_i| - |T_{i+1}|$ for $0 \leq i \leq e-1$.

From Theorem 5.5.1, any codeword $\mathbf{b}$ of the dual code $\mathcal{C}^\perp$ satisfies

$$A_x B_{x^{-1}} = 0 \ \forall x \in G, \ \ \forall \mathbf{a} \in \mathcal{C}.$$

If A_x takes values from $p^k GR(p^e, mr_x)$ for $\mathcal{C}$, then for $\mathcal{C}^\perp$, A_x takes values from $p^{e-k} GR(p^e, mr_x)$. Suppose the defining sets of $\mathcal{C}^\perp$ is $(T_1^\perp, \cdots, T_e^\perp)$. Suppose for $\mathcal{C}$, A_x takes values from $p^k GR(p^e, mr_x)$. Now, In $\mathcal{C}^\perp$, A_x takes values from

$$\begin{aligned} & \{B \in GR(p^e, mr_x) | AB = 0 \ \forall A \in p^k GR(p^e, mr_x)\} \\ = \ & p^{e-k} GR(p^e, mr_x) \end{aligned}$$

So,

$$\begin{aligned} x \in T_j^\perp & \Leftrightarrow e - k \geq j \\ & \Leftrightarrow k \leq e - j \\ & \Leftrightarrow k < e - j + 1 \\ & \Leftrightarrow k \notin T_{e-j+1} \end{aligned}$$

Hence the defining sets of the dual code are given by

$$T_i^\perp = \{x \in G | x^{-1} \notin T_{e-i+1}\}.$$

By using the decomposition (5.2) component-wise, the DFT of any $\mathbf{a} \in (GR(p^e, m))^l$ can be decomposed as

$$\mathbf{A} = \mathbf{A}^{(0)} + p\mathbf{A}^{(1)} + \cdots + p^{e-1}\mathbf{A}^{(e-1)} \tag{5.24}$$

such that for $0 \leq i \leq e-1$, each component of $\mathbf{A}^{(i)}$ is in $\mathcal{T}_{mr}$.

Theorem 5.7.2. *Let $\mathcal{C}$ be an abelian code over $GR(p^e, m)$ on the abelian group G with defining sets $(T_1, \cdots, T_e)$. For any $\mathbf{a} \in \mathcal{C}$, $\mathbf{A}_x^{(i)}$ is nonzero only if $x^{-1} \in T_{e-i}^{\perp}$.*

Proof:

$$\begin{aligned} & \mathbf{A}_x^{(i)} \neq 0 \\ \Rightarrow \quad & \mathbf{A}_x \notin p^{i+1} GR(p^e, mr) \\ \Rightarrow \quad & x \notin T_{i+1} \\ \Rightarrow \quad & x^{-1} \in T_{e-(i+1)+1}^{\perp} = T_{e-i}^{\perp} \end{aligned}$$

■

Any abelian group G can be decomposed as direct sum of some cyclic groups:

$$G = C_{n_1} \oplus \cdots \oplus C_{n_\tau} \simeq \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_\tau}$$

where C_{n_i} is the cyclic group of order n_i. With this decomposition, any element of G has an unique representation as $(i_1, \cdots, i_\tau)$ where $i_j < n_j$ for $1 \leq j \leq \tau$. So the group algebra $GR(p^e, m)G$ is isomorphic to $\frac{GR(p^e,m)[X_1,\cdots,X_\tau]}{(X_1^{n_1}-1,\cdots,X_\tau^{n_\tau}-1)}$. The isomorphism takes $(i_1, \cdots, i_\tau) \in \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_\tau}$ to $X_1^{i_1} \cdots X_\tau^{i_\tau}$. For any $\mathbf{a} \in GR(p^e, m)G$, let us denote the corresponding polynomial as $a(X_1, \cdots, X_\tau)$. We also denote $(i_1, \cdots, i_\tau)$, $(X_1 \cdots X_\tau)$ as $\mathbf{i}$ and $X_1^{i_1} \cdots X_\tau^{i_\tau}$ as $\mathbf{i}$, $\mathbf{X}$ and $\mathbf{X^i}$ respectively.

If $\alpha_1, \cdots, \alpha_\tau$ are respectively $n_1, \cdots, n_\tau$ 'th roots of unity in $GR(p^e, mr)$, then ψ can be chosen as $\psi((i_1, \cdots, i_\tau), (j_1, \cdots, j_\tau)) = \alpha_1^{i_1 j_1} \cdots \alpha_\tau^{i_\tau j_\tau}$. With this ψ, the DFT can be expressed as

$$A_{(j_1,\cdots,j_\tau)} = \sum_{(i_1,\cdots,i_\tau)} \alpha_1^{i_1 j_1} \cdots \alpha_\tau^{i_\tau j_\tau} a_{(i_1,\cdots,i_\tau)} = a(\alpha_1^{j_1}, \cdots, \alpha_\tau^{j_\tau})$$

The Mattson-Solomon (MS) polynomial of $\mathbf{a}$ is defined as

$$A(Z_1, \cdots, Z_\tau) = \sum_{(j_1,\cdots,j_\tau)} A_{(n_1-j_1,\cdots,n_\tau-j_\tau)} Z_1^{i_1} \cdots Z_\tau^{i_\tau}.$$

Theorem 5.7.2 gives the following corrolary, which corresponds to [27, Theorem 3.3] for cyclic codes.

Corollary 5.7.3. *The MS polynomial of any codeword $\mathbf{a} \in \mathcal{C}$ is of the form*

$$\sum_{-\mathbf{i} \in T_e} A_{\mathbf{i}}^{(0)} \mathbf{Z^i} + p \sum_{-\mathbf{i} \in T_{e-1}} A_{\mathbf{i}}^{(1)} \mathbf{Z^i} + \cdots + + p^{e-1} \sum_{-\mathbf{i} \in T_1} A_{\mathbf{i}}^{(e-1)} \mathbf{Z^i}$$

where $-\mathbf{i}$ denotes $(n_1 - i_1, \cdots, n_\tau - i_\tau)$.

5.7.1 Permutation Groups of Abelian Codes

In [27], permutation groups of primitive length cyclic codes over Galois rings were investigated using transform technique. In this subsection, the same approach is generalized for abelian codes on an abelian group G with exponent relatively prime to p.

Any permutation of G acts on any element $GR(p^e, m)G$ naturally. The maximal subgroup of $Per(G)$ which keeps a code $\mathcal{C}$ invariant is called the permutation group $Per(\mathcal{C})$ of $\mathcal{C}$. That is, $Per(\mathcal{C}) = \{\sigma \in Per(G) | \sigma(\mathbf{a}) \in \mathcal{C}\,;\ \forall \mathbf{a} \in \mathcal{C}\}$.

Lemma 5.7.4 ([27]). *If $\mathcal{C}$ is a linear code over $GR(p^e, m)$, then $Per(\mathcal{C}) = Per(\mathcal{C}^{\perp})$.*

The following lemma is stated in [27] for primitive length cyclic codes and is valid by the same argument.

Lemma 5.7.5. *If $m_1|m_2$ and $R_1 = GR(p^e, m_1)$, $R_2 = GR(p^e, m_2)$, $T_e \subseteq T_{e-1} \subseteq \cdots \subseteq T_1 \subseteq G$ are unions of p^{m_1}-cyclotomic cosets, and if $\mathcal{C}_i$ is the abelian code over R_i on the abelian group G with defining sets $(T_1, \cdots, T_e)$ for $i = 1, 2$, then $Per(\mathcal{C}_1) = Per(\mathcal{C}_2)$.*

Note that, $G \simeq Z_{n_1} \oplus \cdots \oplus Z_{n_\tau}$ and Z_{n_i} can also be realized as $\langle \bar{\alpha}_i \rangle$, the cyclic subgroup of $F^*_{p^{mr}}$ of order n_i. Any permutation σ of G has τ component maps $\sigma_i : G \to Z_{n_i}\,;\ 1 \leq i \leq \tau$ such that $\sigma(\alpha_1^{i_1}, \cdots, \alpha_\tau^{i_\tau}) = (\sigma_1(\alpha_1^{i_1}, \cdots, \alpha_\tau^{i_\tau}), \cdots, \sigma_\tau(\alpha_1^{i_1}, \cdots, \alpha_\tau^{i_\tau}))$. Now, σ_i can be described by a unique polynomial f_{σ_i} in $F_{p^{mr}}[X_1, \cdots, X_\tau]/(X_1^{n_1} - 1, \cdots, X_\tau^{n_\tau} - 1)$ so that $f_{\sigma_i}(\alpha_1^{i_1}, \cdots, \alpha_\tau^{i_\tau}) = \sigma_i(\alpha_1^{i_1}, \cdots, \alpha_\tau^{i_\tau})$. So, the τ-tuple $(f_{\sigma_1}, \cdots, f_{\sigma_\tau})$ specifies the permutation σ.

Since $G \simeq \langle \bar{\alpha}_1 \rangle \oplus \cdots \oplus \langle \bar{\alpha}_\tau \rangle$ is isomorphic to $\langle \alpha_1 \rangle \oplus \cdots \oplus \langle \alpha_\tau \rangle$, any permutation σ of G induces a permutation σ' on $\langle \alpha_1 \rangle \oplus \cdots \oplus \langle \alpha_\tau \rangle$. For any $g(X_1, \cdots, X_\tau) \in F_{p^{mr}}[X_1, \cdots, X_\tau]$, define $g^{(L)}(X_1, \cdots, X_\tau) \in \mathcal{T}_{mr}[X_1, \cdots, X_\tau]$ by lifting each co-efficient of $g(X_1, \cdots, X_\tau)$ to it's representative in $\mathcal{T}_{mr}$.

In the following results, like [27], we use the fact that, if $mr + 1 \geq e$, then for any $r \in GR(p^e, mr)$, $r^{p^{mr}} \in \mathcal{T}_{rm}$. Proofs of both the following lemmas and Theorem 5.7.8 are similar to their version (in [27]) for primitive length cyclic codes and thus are omitted.

Lemma 5.7.6. *If $R = GR(p^e, mr)$, $e \leq mr + 1$, and if the map $\sigma \in Per(\langle \bar{\alpha}_1 \rangle \oplus \cdots \oplus \langle \bar{\alpha}_\tau \rangle)$ has the permutation polynomials $(f_{\sigma_1}, \cdots, f_{\sigma_\tau})$, then σ lifts to a permutation σ' of $\langle \alpha_1 \rangle \oplus \cdots \oplus \langle \alpha_\tau \rangle$, which is calculated as*

$$\sigma'(y) = \left(\left(f_{\sigma_i}^{(L)}(y)\right)^{p^{mr}}, \cdots, \left(f_{\sigma_i}^{(L)}(y)\right)^{p^{mr}} \right)\ ,\ \ y \in \langle \alpha_1 \rangle \oplus \cdots \oplus \langle \alpha_\tau \rangle$$

With abuse of notation, we'll let σ act on $\langle\alpha_1\rangle \oplus \cdots \oplus \langle\alpha_\tau\rangle$ directly as $\sigma(y) = \sigma'(y)\,;\ \forall y \in \langle\alpha_1\rangle \oplus \cdots \oplus \langle\alpha_\tau\rangle$.

Lemma 5.7.7. *Suppose, $e \le mr+1, \sigma \in Per(G)$ and $f_{\sigma_i}(X_1,\cdots,X_\tau) \in F_{p^{mr}}[X_1,\cdots,X_\tau]/(X_1^{n_1}-1,\cdots,X_\tau^{n_\tau}-1)\,;\ 1 \le i \le \tau$ are the corresponding polynomials. If $\mathbf{a} \in GR(p^e,m)G$ has MS polynomial $A(Z_1,\cdots,Z_\tau) \in GR(p^e,mr)[Z_1,\cdots,Z_\tau]/(Z_1^{n_1}-1,\cdots,Z_\tau^{n_\tau}-1)$, then $\sigma(\mathbf{a})$ has MS polynomial $A\left(\left(f_{\sigma_1}^{(L)}(Z_1,\cdots,Z_\tau)\right)^{p^{mr}},\cdots,\left(f_{\sigma_\tau}^{(L)}(Z_1,\cdots,Z_\tau)\right)^{p^{mr}}\right)$ mod $(Z_1^{n_1}-1,\cdots,Z_\tau^{n_\tau}-1)$.*

Theorem 5.7.8. *Let $e \le mr+1$ and $\mathcal{C}$ be an abelian code over $GR(p^e,m)$ with defining sets $(T_1,\cdots,T_e)$. If $\sigma \in Per(G)$ and $(f_{\sigma_1},\cdots,f_{\sigma_\tau})$ are the corresponding polynomials, then $\sigma \in Per(\mathcal{C})$ if and only if for all $j, 1 \le j \le e, \mathbf{s} = (s_1,\cdots,s_\tau) \in T_j$,*

$$p^{e-j}\left(\left(f_{\sigma_1}^{(L)}(Z_1,\cdots,Z_\tau)\right)^{s_1p^{mr}}\cdots\left(f_{\sigma_\tau}^{(L)}(Z_1,\cdots,Z_\tau)\right)^{s_2p^{mr}}\right)$$
$$\equiv \sum_{l=1}^{j} p^{e-l} \sum_{\mathbf{i}=(i_1,\cdots,i_\tau)\in T_l} a_{s,l,\mathbf{i}} Z_1^{i_1}\cdots Z_\tau^{i_\tau} \quad mod\ (Z_1^{n_1}-1,\cdots,Z_\tau^{n_\tau}-1)$$

5.8 Minimum Distance of G-Invariant codes

In the previous chapters, a way was shown to determine minimum Hamming distance of a linear code over a finite field from a set of parity check equations over an extension field. In this section, that result is extended to codes over Galois rings.

Theorem 5.8.1. *Suppose, the components of the vector $\mathbf{v} \in (GR(p^e,mr))^n$ are distinct (q^r-1)-th roots of unity and $T_e \subseteq \cdots \subseteq T_1 \subseteq T_0 = [0,q^r-1]$. If for each $k = k_0,k_1,\cdots,k_{\delta-2}$, the vectors $p^{e-j}\mathbf{v}^k\,;\ j \in T_j$ are in the span of a set of parity check equations over $GR(p^e,mr)$, then the minimum Hamming distance of the code is at least that of the cyclic code of length q^r-1 with defining sets $T_1,\cdots,T_e$.*

This theorem can be generalized like the version Theorem 2.5.2 for finite fields. Though the theorem is stated for Hamming distance only, it remains valid for Lee distance (whenever defined) as well. If a lower bound on the minimum (Hamming or Lee) distance is known for a code using Theorem 5.8.1, then the code can be decoded upto that minimum distance by using a decoder for the corresponding cyclic code (of Theorem 5.8.1). Detailed treatment on decoding can be seen in [15, 19, 97–100]. Decoding algorithms for specific classes of linear quaternary codes were given in [19] and [100] for Lee metric. Decoding algorithm for Reed-Solomon and BCH codes over integer residue rings was given in [15] and the decoding of cyclic codes over $\mathbb{Z}_{p^k}$ was discussed in [62, 101] for Hamming distance. Greferath and Velbinger [97] gave an algorithm to decode spliting codes over $\mathbb{Z}_{p^k}$ (i.e. codes which are free submodules of $\mathbb{Z}_{p^k}^n$) by repeated use of any algorithm to decode codes over the residue field $\mathbb{Z}_p$. Byrne extended this to codes over arbitrary Galois rings and Babu and Zimmermann [98] extended it to any linear code (not necessarily spliting codes) over arbitrary Galois rings.

If $(x_1)^q, \cdots, (x_k)^q$ denote the distinct cyclotomic residue classes, then we know that any G-invariant code $\mathcal{C}$ is specified by the submodules $V_{x_1}, \cdots, V_{x_k}$ of $(GR(p^e, mr_{x_1}))^{e_{x_1}}, \cdots,$ $(GR(p^e, mr_{x_k}))^{e_{x_k}}$ respectively, from which $A_{\widetilde{x_1}}, \cdots, A_{\widetilde{x_k}}$ take values. Now, each of V_x ; $x = x_1, \cdots, x_k$ can be considered as a linear code over $GR(p^e, mr_x)$ of length e_x. It is known that any such code has (upto some co-ordinate permutation) a parity check matrix of the form

$$\begin{bmatrix} I_{k_0} & M_{0,1} & M_{0,2} & \cdots & M_{0,e-1} & M_{0,e} \\ 0 & pI_{k_1} & pM_{1,2} & \cdots & pM_{1,e-1} & pM_{1,e} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & p^{e-1}I_{k_{e-1}} & p^{e-1}M_{e-1,e} \end{bmatrix}. \tag{5.25}$$

Any row of this matrix is of the form $p^j\mathbf{v}$.

Suppose $\widetilde{x} = \{y_1, \cdots, y_l\}$, where $x = y_i$ for some i and $l = e_x$. Let $\sum_{i=1}^{l} v_i A_{y_i} = 0$ be a parity check equation of V_x. Then,

$$\begin{aligned} & \sum_{i=1}^{l} v_i A_{y_i} = 0 \\ \Rightarrow \; & \sum_{i=1}^{l} v_i \sum_{y \in \mathcal{G}} \Psi(y, y_i) a_y = 0 \\ \Rightarrow \; & \sum_{y \in \mathcal{G}} \left(\sum_{i=1}^{l} v_i \Psi(y, y_i) \right) a_y = 0 \end{aligned}$$

Clearly, this gives a parity check equation of $\mathcal{C}$ over $GR(p^e, mr_x)$. The component wise conjugate vectors of the parity check vectors obtained this way and the vectors in their span are also parity check vectors of the code.

Though Theorem 5.8.1 gives a way to get minimum distance bound of any linear code, it's application is at least as difficult as it's version for codes over finite fields.

5.9 Number of Submodules of $(GR(p^e, m))^l$

Any submodule V of $(GR(p^e, m))^l$, upto permutations of columns, has a generator matrix of the form:

$$M = \begin{bmatrix} I_{k_0} & M_{0,1} & M_{0,2} & \cdots & M_{0,e-1} & M_{0,e} \\ 0 & pI_{k_1} & pM_{1,2} & \cdots & pM_{1,e-1} & pM_{1,e} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & p^{e-1}I_{k_{e-1}} & p^{e-1}M_{e-1,e} \end{bmatrix} \quad (5.26)$$

where I_k denotes the $k \times k$ identity matrix over $GR(p^e, m)$ [102]. Such a matrix is said to be of type $(k_0, k_1, \cdots, k_e)$. Moreover, the $(e+1)$-tuple $(k_0, k_1, \cdots, k_e)$ is unique for the submodule, where $k_e = l - \sum_{i=0}^{e-1} k_i$. The submodule V is said to be of type $(k_0, k_1, \cdots, k_e)$. A submodule of type $(k_0, k_1, \cdots, k_e)$ has size $p^{m\eta}$ where

$$\eta = \sum_{i=0}^{e} k_i(e-i). \quad (5.27)$$

Suppose, V is a submodule of $(GR(p^e, m))^l$ of type $(k_0, k_1, \cdots, k_e)$. The following algorithm chooses a matrix, if exists, of type $(k'_0, k'_1, \cdots, k'_e)$ with rows from V.

Algorithm I

1. Let $L = \{0, \cdots, l-1\}$.

2. For $i = 0$ to $e-1$
   2.1: For $j = 0$ to $k'_i - 1$
      2.2: Let W be the submodule of V containing all the elements of V whose all the components outside L are zeros. Check if W has at least one element with at least one component not in $p^{i+1}GR(p^e, m)$.
      If YES,
         then take such an element as a new row after normalizing the first such component to p^{i+1}. Remove the index of that component from L.
      If NO,
         then there is no matrix of type $(k'_0, k'_1, \cdots, k'_e)$ with rows from V.

Generator matrix of the form (5.26) for any submodule V can be chosen in many ways. In fact, many different generator matrices can be obtained by Algorithm I itself by taking $k'_i = k_i$ for $0 \leq i \leq e$. To see how many different generator matrices can be chosen for V, let us consider Step 2.2 at any iteration of the i and j loops. Already $k_0+k_1+\cdots+k_{i-1}+j$ rows are selected for the generator matrix M. Consider all complete standard generator matrices with those rows as the first $k_0+k_1+\cdots+k_{i-1}+j$ rows. Clearly, the last $k_{e-1}+\cdots+k_{i+1}+k_i-j$ rows of any of those generator matrices span the same submodule of type $(0,\cdots,0,k_i-j,k_{i+1},\cdots,k_e)$. This submodule has $p^{m\eta_{i,j}}$ elements, where

$$\eta_{i,j}=(k_i-j)(e-i)+k_{i+1}(e-i-1)+\cdots+k_{e-1} \tag{5.28}$$

and $p^{m((k_i-j)(e-i-1)+k_{i+1}(e-i-1)+\cdots+k_{e-1})}=p^{m(\eta_{i,j}-k_i+j)}$ of them have all the components from $p^{i+1}GR(p^e,m)$. So, an element with at least one component not in $p^{i+1}GR(p^e,m)$ can be chosen in $p^{m\eta_{i,j}}-p^{m(\eta_{i,j}-k_i+j)}$ ways. But by normalization, $p^{(e-i)m}-p^{(e-i-1)m}$ distinct elements will give the same row of the generator matrix. So, the new row can be chosen in $\frac{p^{m\eta_{i,j}}-p^{m(\eta_{i,j}-k_i+j)}}{p^{(e-i)m}-p^{(e-i-1)m}}$ ways. Hence, the number of generator matrices of V that can be chosen by Algorithm I is

$$\prod_{i=0}^{e-1}\left(\frac{1}{\left(p^{(e-i)m}-p^{(e-i-1)m}\right)^{k_i}}\prod_{j=0}^{k_i-1}\left(p^{m\eta_{i,j}}-p^{m(\eta_{i,j}-k_i+j)}\right)\right). \tag{5.29}$$

Similarly, the number of matrices of type $(k_0,k_1,\cdots,k_e)$ that can be chosen with rows from $(GR(p^e,m))^l$ is

$$\prod_{i=0}^{e-1}\left(\frac{1}{\left(p^{(e-i)m}-p^{(e-i-1)m}\right)^{k_i}}\prod_{j=0}^{k_i-1}\left(p^{(e-i)m(l-k'_{i-1}-j)}-p^{(e-i-1)m(l-k'_{i-1}-j)}\right)\right). \tag{5.30}$$

So, the number of submodules of $(GR(p^e,m))^l$ of type $(k_0,k_1,\cdots,k_e)$ is

$$N_{(k_0,k_1,\cdots,k_e)}(p^e,m,l)=\prod_{i=0}^{e-1}\prod_{j=0}^{k_i-1}\frac{p^{(e-i)m(l-k'_{i-1}-j)}-p^{(e-i-1)m(l-k'_{i-1}-j)}}{p^{m\eta_{i,j}}-p^{m(\eta_{i,j}-k_i+j)}}. \tag{5.31}$$

5.10 Discussion

Algebraic structure of codes over Galois rings which are closed under arbitrary abelian group G of permutations is investigated. Dual of G-invariant codes and self-dual G-invariant codes are characterized. Number of self-dual G-invariant codes is expressed in terms of the number of self-dual and Hermitian self-dual codes of certain lengths and the number of submodules of $(GR(p^e,m))^l$. However, unlike the codes over finite fields, these numbers are not known for arbitrary length and any Galois ring. Only the number of self-dual codes of any length over $\mathbb{Z}_4$ is known. The number of submodules of $(GR(p^e,m))^l$ of any type is derived in Section 5.9.

Chapter 6

Affine Invariant Extended Cyclic Codes over Galois Rings

6.1 Introduction

In this chapter the transform technique of Blackford and Ray-Caudhuri is extended to find necessary and sufficient conditions under which cyclic codes over $GR(p^e, m)$ are affine invariant for arbitrary e when $p = 2$ and for arbitrary p when $e = 2$. Two new classes of affine invariant codes are found using these conditions.

6.2 Preliminaries

Let n be a positive integer relatively prime to p. If any $\mathbf{c} = (c_0, \cdots, c_{n-1}) \in (GR(p^e, m))^n$ is associated with a polynomial $c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$, then a cyclic code of length n over $GR(p^e, m)$ is an ideal of the modular algebra $\frac{GR(p^e,m)[X]}{(X^n-1)}$. Any cyclic code of length n over $GR(p^e, m)$ is [14] of the form $(f_0, pf_1, \cdots, p^{e-1}f_{e-1})$, where f_j are monic irreducible divisors of $X^n - 1$ and $f_0|f_1|\cdots|f_{e-1}$. If r is the smallest positive integer such that n divides $p^{mr} - 1$, then $GR(p^e, mr)$ is the smallest extension ring of $GR(p^e, m)$ where there is a primitive n-th root ζ of 1 and over which $X^n - 1$ factors into distinct linear factors. The defining sets $T_1, \cdots, T_e$ of the code are defined as

$$T_j = \{s \in [0, n-1] | f_{j-1}(\zeta^s) = 0\}$$

By definition, $T_e \subseteq \cdots \subseteq T_2 \subseteq T_1$. It is also easy to see that each defining set is union of p^m-cyclotomic cosets modulo n.

For any $\mathbf{c} = (c_0, \cdots, c_{n-1}) \in (GR(p^e, m))^n$, the Mattson-Solomon (MS) polynomial of $\mathbf{c}$ is defined [27] as

$$C(Z) = \sum_{i=0}^{n-1} \hat{c}(n-i) Z^i$$

where

$$\hat{c}(i) = c(\zeta^i) = \sum_{j=0}^{n-1} c_j \zeta^{ij}$$

for $0 \leq i \leq n$.

If $\hat{T}_e \subseteq \cdots \subseteq \hat{T}_1 \subseteq [0, n]$ are unions of q-cyclotomic cosets (where $q = p^m$) modulo n, then the extended cyclic code $\hat{\mathcal{C}}$ over $GR(p^e, m)$ of length $n+1$ with defining sets $(\hat{T}_1, \cdots, \hat{T}_e)$ is the set of vectors $\mathbf{a} \in (GR(p^e, m))^{p^m}$, such that

$$\sum_{x \in \mathcal{T}_m} a_x x^s \equiv 0 \bmod p^j \ ; \ \forall s \in \hat{T}_j$$

Clearly if $0 \in T_e$, then $\hat{\mathcal{C}}$ is the extension of the cyclic code $\mathcal{C}$ via a parity check, where $\mathcal{C}$ has defining sets

$$T_j = \{s \bmod n | s \in \hat{T}_j \setminus \{0\}\}$$

Let us assume $n \notin T_1$, since otherwise the code is over $pGR(p^e, m)$. The MS polynomial of a codeword is defined to be that of the corresponding codeword of the cyclic code.

In the following, two important classes of cyclic (and extended cyclic) codes are discussed.

BCH Codes: BCH codes over $\mathbb{Z}_{p^e}$ was first defined by Shankar [10]. Generalization to BCH codes over Galois rings is very straight forward and natural. But Blackford and Ray-Chaudhuri [27] gave a more general definition of BCH codes over Galois rings. For $(n, p) = 1$, suppose $1 \leq \delta_e \leq \delta_{e-1} \leq \cdots \leq \delta_1 \leq n-1$. Then the BCH code $B(n, \delta_1, \cdots, \delta_e)$ of length n over $GR(p^e, m)$ with designed distances $\delta_1, \cdots, \delta_e$ is defined to be the cyclic code with defining sets

$$T_j = \cup_{i \in [1, \delta_j - 1]} [i]^q.$$

Similarly, extended BCH code $\hat{B}(n, \delta_1, \cdots, \delta_e)$ of length $n+1$ is defined as the extended cyclic code with defining sets

$$\hat{T}_j = \{0\} \cup T_j$$

Shankar's definition of BCH code is obtained by assuming $\delta_1 = \delta_2 = \cdots = \delta_e$. Note that, if $p = 2$, we can always take each designed distance to be odd, since if $\delta_i - 1 \in \hat{T}_i$ is odd, then δ_i is also in $\hat{T}_i$ and so we can take $\delta_i + 1$ to be the i'th designed distance as well.

Generalized Reed-Muller Codes over $\mathbb{Z}_{p^e}$: Suppose $0 \le r_1 \le r_2 \le \cdots \le r_e \le (p-1)m$. The Generalized Reed-Muller code of length p^m and orders $(r_1, \cdots, r_e)$ over $\mathbb{Z}_{p^e}$ is defined [27] as the extended cyclic code with defining sets

$$\hat{T}_j = \{s \in [0, p^m - 1] : wt_p(s) < m(p-1) - r_j\}$$

where $wt_p(s)$ denotes the p-adic weight of s: $wt_p(s) = \sum_{i=0}^{m-1} s_i$. GRM codes of length p^m and orders $(r, \cdots, r)$ were well known as the Hensel lifts of GRM codes of order r over $\mathbb{Z}_p$ [19, 34].

For any permutation σ of F_q, there is a unique polynomial $f_\sigma(X)$ over F_q of degree at most $q-1$. Clearly, there is an 1-1 correspondence between F_q and $\mathcal{T}_m$ via the canonical homomorphism of $GR(p^e, m)$ onto F_q. For each polynomial $f(X) \in GR(p^e, m)[X]$, the lifted polynomial $f^{(L)}(X) \in \mathcal{T}_m(X)$ is obtained by lifting each coefficient of $f(X)$ to it's representative in $\mathcal{T}_m$. If $m \ge e-1$, then for any $u \in GR(p^e, m)$, $u^q \in \mathcal{T}_m$. So, any permutation σ of F_q has a corresponding permutation σ' induced by the polynomial $f_\sigma^{(L)}(X)$ as

$$\sigma'(u) = \left(f_\sigma^{(L)}(u)\right)^q \ , \ \ \forall u \in \mathcal{T}_m$$

Clearly, the lifted permutation polynomial corresponding to any affine permutation of $\mathcal{T}_m$ is of the form $aX + b$ where $a, b \in \mathcal{T}_m$ and $a \neq 0$.

The following result from [27] will be very useful in the later sections.

Theorem 6.2.1. *[27, Theorem 4.2] Let $n = p^m - 1$, where $m \ge e-1$. Let $\hat{\mathcal{C}}$ be the extended cyclic code over any subring of $GR(p^e, m)$ of length n with defining sets $(\hat{T}_1, \cdots, \hat{T}_a)$, with $0 \in \hat{T}_a$. If $\sigma \in Sym(p^m)$, and $f_\sigma(X) \in F_q[X]$ is the corresponding permutation polynomial, then $\sigma \in Per(\hat{\mathcal{C}})$ if and only if for all j, $1 \le j \le a$, $s \in \hat{T}_j$,*

$$p^{e-j}\left(f_\sigma^{(L)}(X)\right)^{sp^m} \equiv \sum_{l=1}^{j} p^{e-l} \sum_{i \in \hat{T}_l} a_{s,l,i} X^i \quad (mod\ X^n - 1)$$

where $a_{s,l,i} \in \mathcal{T}_m$.

6.3 Affine Invariant Codes over Galois Rings

In [30], a partial order $\preceq_p$ for the set $[0, p^m - 1]$ was defined. For any two elements $s, t \in [0, p^m - 1]$, they can be uniquely decomposed as $s = \sum_{i=0}^{m-1} s_i p^i$ and $t = \sum_{i=0}^{m-1} t_i p^i$, with $0 \le s_i, t_i \le p-1$. Then $s \preceq_p t$ if $s_i \le t_i$ for $0 \le i \le m-1$. The m-tuples $(s_{m-1}, \cdots, s_0)$ and $(t_{m-1}, \cdots, t_0)$ are called the p-ary representations of the integers s and t respectively. It should be noted that for any $s \in [0, p^m - 2]$, $ps \mod (p^m - 1)$ has the p-ary representation $(s_{m-2}, \cdots, s_0, s_{m-1})$. Any subset $T \subseteq S$ is called a lower ideal of S if $t \in T$, $s \preceq_p t \Rightarrow s \in T$. It is known that $\binom{s}{t} = \binom{s_0}{t_0} \cdots \binom{s_{m-1}}{t_{m-1}}$. So,

Lemma 6.3.1 (Lucas). *for $s, i \in [0, p^m - 2]$, $\binom{s}{i} \not\equiv 0 \mod p$ if and only if $i \preceq_p s$.*

6.3.1 $p = 2$ and Arbitrary e

Let us consider $p = 2$ and define $M_{m,2}^{(i)}(s, k)$; $i \ge 0$, $s, k \in [0, 2^m - 2]$ recursively as

$$M_{m,2}^{(0)}(s,k) = \begin{cases} 1 & \text{if } k \preceq_2 s \\ 0 & \text{otherwise} \end{cases}$$
$$M_{m,2}^{(i)}(s,k) * M_{m,2}^{(j)}(s,k) = \sum_{\substack{0 \le k_1, k_2 \le n-1 \\ 2^j k_1 + 2^i k_2 \equiv k \bmod n \\ k_1 < k_2 \text{ if } i=j}} M_{m,2}^{(i)}(s,k_1) M_{m,2}^{(j)}(s,k_2)$$

$$\text{and} \quad M_{m,2}^{(i)}(s,k) = \begin{cases} \sum_{\substack{(i_1,i_2) \\ 0 \le i_1 \le i_2 \le i-1 \\ i_1+i_2=i-1}} M_{m,2}^{(i_1)}(s,k) * M_{m,2}^{(i_2)}(s,k) & \text{if } i \text{ is odd} \\ \sum_{\substack{(i_1,i_2) \\ 0 \le i_1 \le i_2 \le i-1 \\ i_1+i_2=i-1}} M_{m,2}^{(i_1)}(s,k) * M_{m,2}^{(i_2)}(s,k) + \left(M_{m,2}^{(\frac{i}{2})}(s, 2^{m-\frac{i}{2}}k)\right)^2 & \text{if } i \text{ is even} \end{cases}$$

By this definition, $M_{m,2}^{(1)}(s,k)$ is same as $M_m(s,k)$ in [27], i.e.,

$$M_{m,2}^{(1)}(s,k) = |\{(i,j) | i < j; i, j \preceq_2 s; i + j \equiv k \bmod n\}|.$$

Let us also define the following numbers for $i \ge 0$, $s, k \in [0, 2^m - 2]$.

$$K_{m,2}^{(0)}(s,k) = M_{m,2}^{(0)}(s,k)$$
$$\text{and} \quad K_{m,2}^{(i)}(s,k) = M_{m,2}^{(i)}(s,k) + \lfloor \frac{1}{2} K_{m,2}^{(i-1)}(s, k.2^{m-1}) \rfloor \text{ for } i \ge 1$$

Here $\lfloor . \rfloor$ denotes the largest integer less than or equal to the number inside.

Parity of any integer i is defined as

$$P(i) = \begin{cases} 0 & \text{if } i \text{ is even} \\ 1 & \text{if } i \text{ is odd} \end{cases}$$

Lemma 6.3.2. *If* $m \geq e-1$ *and* $s, k \in [0, 2^m - 2]$, *then*

1. *For* $i \geq 0,\ 0 \leq j < m,\ M_{m,2}^{(i)}(s,k) = M_{m,2}^{(i)}(2^j s, 2^j k)$
2. *For* $i \geq 0,\ 0 \leq j < m,\ K_{m,2}^{(i)}(s,k) = K_{m,2}^{(i)}(2^j s, 2^j k)$
3. $M_{m,2}^{(i)}(s,k) \neq 0 \Rightarrow k \leq 2^i s - 1$ *for* $i > 0$
4. $K_{m,2}^{(i)}(s,k) \neq 0 \Rightarrow k \leq 2^i s - 1$ *for* $i > 0$

Proof: 1) For $i = 0$, the result is obvious. For $i > 0$ also, the proof is trivial by induction.
2) Trivial using the definition of $K_{m,2}^{(i)}(s,k)$ and the first part of this lemma.
3) First, note that for $i = 0$, $M_{m,2}^{(i)}(s,k) \neq 0 \Rightarrow k \leq 2^i s = s$. For $i = 1$, the result is same as [27, Lemma 5.1(3)]. Suppose it is true for $(i-1)$ and smaller integers (where $i \geq 2$) and $M_{m,2}^{(i)}(s,k) \neq 0$. Then either of the following cases hold.
Case I: $\exists i_1, i_2;\ i_1 \leq i_2;\ i_1 + i_2 + 1 = i$, such that $\exists k_1, k_2$, satisfying $2^{i_2}k_1 + 2^{i_1}k_2 = k \bmod n$, $M_{m,2}^{(i_1)}(s,k_1) \neq 0$ and $M_{m,2}^{(i_2)}(s,k_2) \neq 0$. Clearly, $i_2 \neq 0$. By induction hypotheses,

$$k_1 \leq 2^{i_1}s$$
$$k_2 \leq 2^{i_2}s - 1$$

So,

$$\begin{aligned} k &= 2^{i_2}k_1 + 2^{i_1}k_2 \\ &\leq 2^{i-1}s + 2^{i-1}s - 2^{i_1} \\ &= 2^i s - 2^{i_1} \\ &\leq 2^i s - 1 \end{aligned}$$

Case II: i is even and

$$\begin{aligned} & M_{m,2}^{(\frac{i}{2})}(s, 2^{m-\frac{i}{2}}k) \neq 0 \\ \Rightarrow\ & M_{m,2}^{(\frac{i}{2})}(2^{\frac{i}{2}}s, k) \neq 0 \\ \Rightarrow\ & k \leq 2^{\frac{i}{2}}.2^{\frac{i}{2}}s - 1 = 2^i s - 1 \end{aligned}$$

4) For $i = 1$, $K_{m,2}^{(1)}(s,k) = M_{m,2}^{(1)}(s,k)$. So, the claim is true for $i = 1$. Suppose it is true for $i-1$ and $K_{m,2}^{(i)}(s,k) \neq 0$. Then either $M_{m,2}^{(i)}(s,k) \neq 0$ or $K_{m,2}^{(i-1)}(s, 2^{m-1}k) \neq 0$. In the first case, the claim follows from third part of this lemma. In the second case, $K_{m,2}^{(i-1)}(2s,k) \neq 0 \Rightarrow k \leq 2^{i-1}.2s - 1 = 2^i s - 1$. ■

Lemma 6.3.3. *Suppose* $m \geq e-1$ *and* $x, y \in GR(2^e, m)$. *Then* $(x+2y)^{2^m} = x^{2^m}$.

Proof:

$$\begin{aligned}
(x+2y)^{2^m} &= (x^2 + 2^2 f_1(x,y))^{2^{m-1}} \text{ where } f_1(x,y) = xy + y^2 \\
&= (x^{2^2} + 2^3 f_2(x,y))^{2^{m-2}} \text{ where } f_2(x,y) = x^2 f_1(x,y) + 2f_1^2(x,y) \\
&\quad \ldots \\
&= (x^{2^m} + 2^{m+1} f_m(x,y))^{2^{m-2}} \text{ where } f_m(x,y) = x^{2^{m-1}} f_{m-1}(x,y) + 2^{m-1} f_{m-1}^2(x,y) \\
&= x^{2^m} \text{ in } GR(p^e, m)
\end{aligned}$$

Lemma 6.3.4. *If* $m \geq e-1$ *and* $x, b \in \mathcal{T}_m \subset GR(2^e, m)$, *then*

$$(x+b)^{s.2^m} = \left(\sum_{\substack{0 \leq i \leq s \\ i \preceq_2 s}} x^i b^{s-i} \right)^{2^m}$$

Proof: Taking binomial expansion, we have

$$(x+b)^{s.2^m} = \left(\sum_{0 \leq i \leq s} \binom{s}{i} x^i b^{s-i} \right)^{2^m}$$

If $i \preceq_2 s$, then $\binom{s}{i} \equiv 1 \bmod 2$. Otherwise $\binom{s}{i} \equiv 0 \bmod 2$. So the result follows by Lemma 6.3.3. ∎

Lemma 6.3.5. *Suppose* $x, b \in GR(2^e, m)$. *Then*

$$\left(\sum_{\substack{0 \leq i \leq s \\ i \preceq_2 s}} x^i b^{s-i} \right)^{2^{m_1}} \equiv \sum_{i=0}^{m_2} 2^i \sum_{k=0}^{n-1} M_{m,2}^{(i)}(s,k) x^{k.2^{m_1-i}} b^{2^{m_1}s - k.2^{m_1-i}} \quad mod\ 2^{m_2+1}$$

for any $m_1 \geq 0,\ m_2 \leq m_1$.

Proof: By induction on m_1. Clearly, the result is true for $m_1 = 0$. Suppose it is true for $m_1 - 1$ for some $m_1 \geq 1$. Then we need to prove it for m_1.

Obviously, the result is true for $m_2 = 0$. Suppose $m_1 \geq m_2 > 0$. By induction hypotheses,

$$\left(\sum_{\substack{0 \leq i \leq s \\ i \preceq_2 s}} x^i b^{s-i} \right)^{2^{m_1-1}} \equiv \sum_{i=0}^{m_2-1} 2^i \sum_{k=0}^{n-1} M_{m,2}^{(i)}(s,k) x^{k.2^{m_1-1-i}} b^{2^{m_1-1}s - k.2^{m_1-1-i}} \bmod 2^{m_2}$$

since $m_2 - 1 \leq m_1 - 1$. So, $\left(\sum_{\substack{0\leq i\leq s\\ i\preceq_2 s}} x^i b^{s-i}\right)^{2^{m_1-1}}$ can be expanded in the form

$$\left(\sum_{\substack{0\leq i\leq s\\ i\preceq_2 s}} x^i b^{s-i}\right)^{2^{m_1-1}} \equiv \sum_{i=0}^{m_2-1} 2^i \sum_{k=0}^{n-1} M^{(i)}_{m,2}(s,k) x^{k.2^{m_1-1-i}} b^{2^{m_1-1}s-k.2^{m_1-1-i}} + 2^{m_2} u$$

for some $u \in GR(2^e, m)$. By squaring both sides, we get

$$\left(\sum_{\substack{0\leq i\leq s\\ i\preceq_2 s}} x^i b^{s-i}\right)^{2^{m_1}} \equiv \left(\sum_{i=0}^{m_2-1} 2^i \sum_{k=0}^{n-1} M^{(i)}_{m,2}(s,k) x^{k.2^{m_1-1-i}} b^{2^{m_1-1}s-k.2^{m_1-1-i}}\right)^2 \mod 2^{m_2+1}$$

$$\equiv \sum_{i=0}^{m_2} 2^i \sum_{\substack{0\leq i_1\leq i_2\leq i-1\\ i_1+i_2+1=i}} \sum_{\substack{0\leq k_1,k_2\leq n-1\\ k_1<k_2 \text{ if } i_1=i_2}} M^{(i_1)}_{m,2}(s,k_1) M^{(i_2)}_{m,2}(s,k_2) x^{k_1.2^{m_1-1-i_1}+k_2.2^{m_1-1-i_2}} b^{2^{m_1}s-\left(k_1.2^{m_1-1-i_1}+k_2.2^{m_1-1-i_2}\right)}$$

$$+ \sum_{i=0}^{m_2-1} 2^{2i} \sum_{k=0}^{n-1} \left(M^{(i)}_{m,2}(s,k)\right)^2 x^{k.2^{m_1-i}} b^{2^{m_1}s-k.2^{m_1-i}} \mod 2^{m_2+1}$$

$$\equiv \sum_{i=0}^{m_2} 2^i \sum_{\substack{0\leq i_1\leq i_2\leq i-1\\ i_1+i_2+1=i}} \sum_{\substack{0\leq k_1,k_2\leq n-1\\ k_1<k_2 \text{ if } i_1=i_2}} M^{(i_1)}_{m,2}(s,k_1) M^{(i_2)}_{m,2}(s,k_2) x^{2^{m_1-i}(k_1.2^{i_2}+k_2.2^{i_1})} b^{2^{m_1}s-2^{m_1-i}(k_1.2^{i_2}+k_2.2^{i_1})}$$

$$+ \sum_{i=0}^{m_2-1} 2^{2i} \sum_{k=0}^{n-1} \left(M^{(i)}_{m,2}(s,k)\right)^2 x^{k.2^{m_1-i}} b^{2^{m_1}s-k.2^{m_1-i}} \mod 2^{m_2+1}$$

$$\equiv \sum_{i=0}^{m_2} 2^i \sum_{\substack{0\leq i_1\leq i_2\leq i-1\\ i_1+i_2+1=i}} \sum_{k=0}^{n-1} \left(M^{(i_1)}_{m,2}(s,k) * M^{(i_2)}_{m,2}(s,k)\right) x^{2^{m_1-i}k} b^{2^{m_1}s-2^{m_1-i}k}$$

$$+ \sum_{\substack{0\leq i\leq m_2-1\\ i \text{ even}}} 2^i \sum_{k=0}^{n-1} \left(M^{(\frac{i}{2})}_{m,2}(s,k)\right)^2 x^{k.2^{m_1-\frac{i}{2}}} b^{2^{m_1}s-k.2^{m_1-\frac{i}{2}}} \mod 2^{m_2+1}$$

$$\equiv \sum_{i=0}^{m_2} 2^i \sum_{k=0}^{n-1} \left(\sum_{\substack{0\leq i_1\leq i_2\leq i-1\\ i_1+i_2+1=i}} \left(M^{(i_1)}_{m,2}(s,k) * M^{(i_2)}_{m,2}(s,k)\right)\right) x^{2^{m_1-i}k} b^{2^{m_1}s-2^{m_1-i}k}$$

$$+ \sum_{\substack{0\leq i\leq m_2-1\\ i \text{ even}}} 2^i \sum_{k'=0}^{n-1} \left(M^{(\frac{i}{2})}_{m,2}(s, 2^{m-\frac{i}{2}}k')\right)^2 x^{k'.2^{m_1-i}} b^{2^{m_1}s-k'.2^{m_1-i}} \mod 2^{m_2+1}$$

where $k' = k.2^{\frac{i}{2}} \mod n$

$$\equiv \sum_{i=0}^{m_2} 2^i \sum_{k=0}^{n-1} M^{(i)}_{m,2}(s,k) x^{2^{m_1-i}k} b^{2^{m_1}s-2^{m_1-i}k} \mod 2^{m_2+1}$$

■

Theorem 6.3.6. *If $m \geq e-1$, $x, b \in \mathcal{T}_m \subset GR(2^e, m)$, $n = 2^m - 1$ and $s \in [0, n-1]$,* *then*

$$(x+b)^{s.2^m} = \sum_{i=0}^{e-1} 2^i \sum_{k=0}^{n-1} M_{m,2}^{(i)}(s,k) x^{2^{m-i}k} b^{2^m s - 2^{m-i}k}$$

Proof: Trivial using Lemma 6.3.4 and Lemma 6.3.5. ■

Lemma 6.3.7. *Suppose $m \geq e-1$, $x, b \in \mathcal{T}_m \subset GR(2^e, m)$, $n = 2^m - 1$ and $s \in [0, n-1]$. Then for any j; $0 \leq j \leq e-1$,*

$$\begin{aligned}(x+b)^{s.2^m} \quad = \quad & \sum_{i=0}^{j-1} 2^i \sum_{k=0}^{n-1} P(K_{m,2}^{(i)}(s,k)) x^{2^{m_1-i}k} b^{2^{m_1}s - 2^{m_1-i}k} \\ & + 2^j \sum_{k=0}^{n-1} K_{m,2}^{(j)}(s,k) x^{2^{m_1-j}k} b^{2^{m_1}s - 2^{m_1-j}k} \\ & + \sum_{i=j+1}^{e-1} 2^i \sum_{k=0}^{n-1} M_{m,2}^{(i)}(s,k) x^{2^{m_1-i}k} b^{2^{m_1}s - 2^{m_1-i}k}\end{aligned}$$

Proof: By induction on j.

Clearly the statement is true for $j = 0$. Suppose it is true for $j (< e-1)$. Then it needs to be proved for $j+1$. It is trivial by using the fact:

$$K_{m,2}^{(j)}(s,k) = P\left(K_{m,2}^{(j)}(s,k)\right) + 2\lfloor \frac{1}{2} K_{m,2}^{(j)}(s,k) \rfloor.$$

■

Taking $j = e-1$, we get the following corollary.

Corollary 6.3.8. *Suppose $m \geq e-1$, $x, b \in \mathcal{T}_m \subset GR(2^e, m)$, $n = 2^m - 1$ and $s \in [0, n-1]$. Then*

$$(x+b)^{s.2^m} = \sum_{i=0}^{e-1} 2^i \sum_{k=0}^{n-1} P(K_{m,2}^{(i)}(s,k)) x^{2^{m_1-i}k} b^{2^{m_1}s - 2^{m_1-i}k}.$$

Theorem 6.3.9. *If $m \geq e-1$, then an extended cyclic code over any subring of $GR(2^e, m)$ of length $n+1 = 2^m$ with defining sets $\hat{T}_1, \cdots, \hat{T}_e$ is affine invariant if and only if for all $i = 1, 2, \cdots, e$; $j = 1, 2, \cdots, i$,*

$$s \in \hat{T}_i, P\left(K_{m,2}^{(i-j)}(s,k)\right) = 1 \Rightarrow 2^{m-(i-j)}.k \in \hat{T}_j. \tag{6.1}$$

Proof: By Theorem 6.2.1, the code is affine invariant if and only if for $i = 1, \cdots, e$ and $\sigma \in AGL(1, 2^m)$, each polynomial in the set

$$\left\{ 2^{e-i} \left(f_\sigma^{(L)}(Z)\right)^{s.2^m} | s \in \hat{T}_i \right\}$$

is of the form

$$\sum_{j=1}^{i} 2^{e-j} \sum_{k\in\hat{T}_j} a_{s,j,k} Z^k \qquad \text{mod } Z^n - 1$$

where $a_{s,j,k} \in \mathcal{T}_m$. Since the code is extended cyclic, it is sufficient to consider the polynomials $f_\sigma^{(L)}(Z) = Z + b;\ \ b \in \mathcal{T}_m$. Now, by Corollary 6.3.8, for any $i = 1, \cdots, e,\ b \in \mathcal{T}_m,\ s \in \hat{T}_i$,

$$2^{e-i}(x+b)^{s,2^m} = \sum_{j=1}^{i} 2^{e-j} \sum_{k=0}^{n-1} P\left(K_{m,2}^{(i-j)}(s,k)\right) b^{\left(2^{(i-j)}s-k\right)2^{m-(i-j)}} Z^{k.2^{m-(i-j)}} \qquad \text{mod } Z^n - 1.$$

So, the code is affine invariant if and only if for all $i = 1, 2, \cdots, e;\ j = 1, 2, \cdots, i,$

$$s \in \hat{T}_i, P\left(K_{m,2}^{(i-j)}(s,k)\right) = 1 \Rightarrow 2^{m-(i-j)}.k \in \hat{T}_j.$$

■

For $i < e$, the necessary and sufficient conditions can also be put as

$$s \in \hat{T}_i \setminus \hat{T}_{i+1}, P\left(K_{m,2}^{(i-j)}(s,k)\right) = 1 \Rightarrow 2^{m-(i-j)}.k \in \hat{T}_j$$

since for $s \in \hat{T}_{i+1} \subseteq \hat{T}_i$, $P\left(K_{m,2}^{(i-j)}(s,k)\right) = 1 \Rightarrow P\left(K_{m,2}^{((i+1)-(j+1))}(s,k)\right) = 1 \Rightarrow 2^{m-(i-j)}.k = 2^{m-((i+1)-(j+1))}.k \in \hat{T}_{(j+1)} \subseteq \hat{T}_j$.

For $j = i$, the necessary and sufficient condition in the Theorem 6.3.9 says, $\hat{T}_1, \cdots, \hat{T}_e$ are lower ideals in $[0, n]$. For $i = 2, j = 1$, the condition is equivalent to

$$s \in \hat{T}_2,\ \ M_{m,2}^{(1)}(s,k) \not\equiv 0 \text{ mod } 2 \Rightarrow 2^{m-1}.k \in \hat{T}_1$$

So, for $e = 2$, the theorem gives [27, Theorem 5.1] as a special case.

Note that if the code is over the subring $GR(2^e, m_1)$ of $GR(2^e, m)$, then $2^{m-l}.k \in \hat{T}_j \Leftrightarrow 2^{(m-l) \text{ mod } m_1} k \in \hat{T}_j$ by conjugacy constraints. So, if $m_1 = 1$, then $2^{m-l}.k \in \hat{T}_j \Leftrightarrow k \in \hat{T}_j$.

Theorem 6.3.10. *Let $\hat{B}(n, \delta_1, \cdots, \delta_e)$ be the extended BCH codes of length $n+1 = 2^m$ over $\mathbb{Z}_{2^e}$ with designed distances $\delta_1, \cdots, \delta_e$. If for $i = 1, \cdots, e$, $l = 0, \cdots, i-1$, $\delta_{i-l} \geq 2^l(\delta_i - 2)$, then $\hat{B}(n, \delta_1, \cdots, \delta_e)$ is affine-invariant.*

Proof: As mentioned earlier, without loss of generality, we can assume each designed distance to be odd. We need to prove that, under the conditions, for $i = 1, \cdots, e$, $l = 0, \cdots, i-1$,

$$s \leq \delta_i - 1 \text{ and } K_{m,2}^{(l)}(s,k) \neq 0 \Rightarrow k \leq \delta_{i-l} - 1$$

By Lemma 6.3.2(2), it sufficient to check only for the odd values of s. Since $\delta_i - 1$ is even, it is sufficient to consider $s \leq \delta_i - 2$. For $l = 0$, it is trivial. For $l \neq 0$, $s \leq \delta_i - 2$ and $K_{m,2}^{(l)}(s,k) \neq 0 \Rightarrow k \leq 2^l s - 1 \leq 2^l(\delta_i - 2) - 1 \leq \delta_{i-l} - 1$. ■

The following corollary gives stronger conditions for pairs of the consecutive designed distances, under which a BCH code is affine invariant. If these stronger conditions are satisfied by the designed distances, then one need not check for the other conditions required by Theorem 6.3.10, since, then they are automatically satisfied.

Corollary 6.3.11. *Let $\hat{B}(n, \delta_1, \cdots, \delta_e)$ be the extended BCH codes of length $n+1 = 2^m$ over $\mathbb{Z}_2^e$ with designed distances $\delta_1, \cdots, \delta_e$. If $\delta_{i-1} \geq 2\delta_i - 2$ for $1 < i \leq e$, then the code $\hat{B}(n, \delta_1, \cdots, \delta_e)$ is affine invariant.*

Proof: We shall show that if $\hat{B}(n, \delta_1, \cdots, \delta_e)$ satisfies these conditions, then it also satisfies the conditions of Theorem 6.3.10. For $i = 1, \cdots, e$, $l = 0, \cdots, i-1$.

$$\begin{aligned}
\delta_{i-l} &\geq 2\delta_{i-l+1} - 2 \\
&\geq 2(2\delta_{i-l+2} - 2) - 2 \\
&\cdots \\
&\geq 2(2(\cdots 2(2\delta_i - 2) - 2)\cdots 2) - 2 \\
&= 2^l\delta_i - 2(1 + 2 + \cdots + 2^{l-1}) \\
&= 2^l\delta_i - 2(2^l - 1) = 2^l(\delta_i - 2) + 2 > 2^l(\delta_i - 2)
\end{aligned}$$

■

The GRM codes over $\mathbb{Z}_4$ were proved to be affine invariant in [27]. However, it was pointed out with an example that the same is not true for GRM codes over $\mathbb{Z}_e$ for $e > 2$. In the following, we proceed towards finding a class of affine invariant GRM codes over $\mathbb{Z}_{2^e}$.

Lemma 6.3.12.

$$K_{m,2}^{(i)} \neq 0 \Rightarrow \begin{cases} wt_2(k) \leq 2^{i-1} wt_2(s) & \text{for } i > 0 \\ wt_2(k) \leq wt_2(s) & \text{for } i = 0 \end{cases}$$

Proof: Proof by induction on i: For $i = 0$, obvious. For $i = 1$, $K_{m,2}^{(i)} \neq 0 \Rightarrow$ there are integers $k_1, k_2 \preceq_2 s$ such that $k_1 + k_2 \equiv k \bmod n$. So, $wt_2(k) \leq wt_2(s)$.

Suppose the claim is true for i and smaller integers, where $i > 0$. Then it needs to be proved for $i+1$.

$$K_{m,2}^{(i+1)}(s,k) \neq 0 \Rightarrow M_{m,2}^{(i+1)}(s,k) \neq 0 \text{ or } K_{m,2}^{(i)}(s, 2^{m-1}k) \neq 0 \tag{6.2}$$

If $K_{m,2}^{(i)}(s, 2^{m-1}k) \neq 0$, then by induction hypotheses, $wt_2(k) \leq 2^{i-1}wt_2(s) \leq 2^i wt_2(s)$. If $M_{m,2}^{(i+1)}(s,k) \neq 0$, then either $\exists i_1, i_2, k_1, k_2;\ i_1 + i_2 = i, i_1 \leq i_2, 2^{i_2}k_1 + 2^{i_1}k_2 \equiv k \bmod n$, such that $M_{m,2}^{(i_1)}(s,k_1) \neq 0$ and $M_{m,2}^{(i_2)}(s,k) \neq 0$ or $(i+1)$ is even and $M_{m,2}^{\frac{(i+1)}{2}}(s, 2^{m-\frac{(i+1)}{2}}k) \neq 0 \Leftrightarrow M_{m,2}^{\frac{(i+1)}{2}}(2^{\frac{(i+1)}{2}}s, k) \neq 0$. In the second case, by induction hypotheses, $wt_2(k) \leq 2^{\frac{(i-1)}{2}} wt_2(2^{\frac{(i+1)}{2}} s \bmod n) = 2^{\frac{(i-1)}{2}} wt_2(s) \leq 2^i wt_2(s)$. In the first case, the following sub-cases can hold.

Case I: $i_1 = 0$:

$$\begin{aligned} wt_2(k) &= wt_2(2^{i_2}k_1 + 2^{i_1}k_2) \\ &\leq wt_2(2^{i_2}k_1) + wt_2(2^{i_1}k_2) \\ &= wt_2(k_1) + wt_2(k_2) \\ &\leq (2^{i_2-1}+1)wt_2(s) \\ &\leq (2^{i-1}+1)wt_2(s) \leq 2^i wt_2(s) \end{aligned}$$

Case II: $i_1 \neq 0$:

$$\begin{aligned} wt_2(k) &= wt_2(2^{i_2}k_1 + 2^{i_1}k_2) \\ &\leq wt_2(2^{i_2}k_1) + wt_2(2^{i_1}k_2) \\ &= wt_2(k_1) + wt_2(k_2) \\ &\leq 2^{i_1-1}wt_2(s) + 2^{i_2-1}wt_2(s) \\ &\leq 2^{i-1}wt_2(s) + 2^{i-1}wt_2(s) \\ &\leq 2^i wt_2(s) \end{aligned}$$

■

Theorem 6.3.13. *A GRM code $GRM(r_1, \cdots, r_e, m)$ is affine invariant if either $e = 1$ or for $i = 2, \cdots, e;\ l = 1, \cdots, i-1,\ r_{i-l} \leq m - 2^{l-1}(m - r_i)$.*

Proof: Clearly for $i = 1, \cdots, e$, $\hat{T}_i$ is a lower ideal. This completes the proof for $e = 1$. Now, we need to prove (6.1) for $i = 1, \cdots, e;\ l = i - j = 1, \cdots, i-1$. For these values of

i and l,

$$\begin{aligned} & s \in \hat{T}_i \text{ and } K_{m,2}^{(l)}(s,k) \neq 0 \\ \Rightarrow\ & wt_2(s) \leq m - r_i \text{ and } wt_2(k) \leq 2^{l-1} wt_2(s) \\ \Rightarrow\ & wt_2(k) \leq 2^{l-1}(m - r_i) \\ \Rightarrow\ & wt_2(k) \leq m - r_{i-l} \\ \Rightarrow\ & k \in \hat{T}_{i-l} \end{aligned}$$

So, the code is affine invariant. ■

Example 6.3.1. For any $e \geq 1$, let us consider the code $GRM(r_1, \cdots, r_a, m)$ over $\mathbb{Z}_{2^e}$ with $r_e = m - 1$ and $r_i = m - 2^{e-i-1}$ for $i < e$. For $i = 2, \cdots, e$,

$$\begin{aligned} & r_i \geq m - 2^{a-i} \\ \Rightarrow\ & 2^{a-i} \geq m - r_i \\ \Rightarrow\ & m - 2^{l-1}.2^{a-i} \leq m - 2^{l-1}(m - r_i) \end{aligned}$$

So, for $l = 1, \cdots, i-1$,

$$\begin{aligned} r_{i-l} &= m - 2^{a-(i-l)-1} \\ &= m - 2^{l-1}.2^{a-i} \\ &\leq m - 2^{l-1}(m - r_i) \end{aligned}$$

So, the code is an affine invariant code.

6.3.2 Arbitrary p and $e = 2$

In this subsection, extended cyclic codes over $GR(p^2, m)$ is considered for arbitrary p and investigate the affine invariant codes among them. For any $i_1, i_2, \cdots, i_k$ with $i_1 + i_2 + \cdots + i_k \leq s$, let us define the quantity $\begin{pmatrix} & s & \\ i_1\ i_2 & \cdots & i_k \end{pmatrix}$ to be the number of ways the disjoint subsets $S_1, S_2, \cdots, S_k \subset [0, n-1]$ can be chosen with $|S_j| = i_j$ for $1 \leq j \leq k$. It's value is given by

$$\begin{pmatrix} & s & \\ i_1\ i_2 & \cdots & i_k \end{pmatrix} = \begin{pmatrix} s \\ i_1 \end{pmatrix} \begin{pmatrix} s - i_1 \\ i_2 \end{pmatrix} \cdots \begin{pmatrix} s - i_1 - \cdots - i_{k-1} \\ i_k \end{pmatrix}$$

Lemma 6.3.14. *Suppose $s, i_1, \cdots, i_k \in [0, p^m - 2]$ have the p-ary representations $(s_0, \cdots s_{m-1}), (i_{1,0}, \cdots, i_{1,m-1}), \cdots, (i_{k,0}, \cdots, i_{k,m-1})$ respectively. Then*

$$\begin{pmatrix} & s & \\ i_1\ i_2 & \cdots & i_k \end{pmatrix} = \prod_{j=0}^{m-1} \begin{pmatrix} & s_j & \\ i_{1,j}\ i_{2,j} & \cdots & i_{k,j} \end{pmatrix}$$

This gives the following generalization of Lucas' lemma.

Lemma 6.3.15 (Generalized Lucas Lemma). *Suppose $s, i_1, \cdots, i_k \in [0, p^m - 2]$ have the p-ary representations $(s_0, \cdots s_{m-1}), (i_{1,0}, \cdots, i_{1,m-1}), \cdots, (i_{k,0}, \cdots, i_{k,m-1})$ respectively. Then $\binom{s}{i_1\ i_2\ \cdots\ i_k} \not\equiv 0 \bmod p$ if and only if $i_{1,j} + \cdots + i_{k,j} \leq s_j$ for $0 \leq j \leq m-1$.*

For any $s, k \in [0, p^m - 2]$, let us define the quantity

$$M_{m,p}(s,k) = \frac{1}{p} \sum_{\substack{(i_0, \cdots, i_s) \\ \sum_{j=0}^{s} i_j = p;\ i_j \neq p\,\forall j \\ j \preceq_p s \text{ whenever } i_j \neq 0 \\ \sum_{j=0}^{s} j i_j \equiv k \bmod p^m - 2}} \binom{p}{i_0\ \cdots\ i_{s-1}} \binom{s}{1}^{i_1} \cdots \binom{s}{s-1}^{i_{s-1}}$$

For $p = 2$, it reduces to $M_m(s,k)$ as defined in [27]: $M_{m,2}(s,k) = M_m(s,k) = |\{(i,j) | i < j; i, j \preceq_2 s; i + j \equiv k \bmod n\}|$.

Lemma 6.3.16. *If $n = p^m - 1$, $1 \leq i \leq m$ and $s, k \in [0, n-1]$, then*

1. $M_{m,p}(s,k) = M_{m,p}(p^i s, p^i k)$
2. $M_{m,p}(p^i s, k) = M_{m,p}(s, p^{(m-i)} k)$
3. $M_{m,p}(s,k) \neq 0 \Rightarrow k \leq ps - 1$

Proof: 1) It is sufficient to assume $i = 1$. For any $s, k \in [0, n-1]$, let us define the set $S_{(s,k)} \triangleq \{((i_0, \cdots, i_s) | \sum_{j=0}^{s} i_j = p;\ i_j \neq p\,\forall j; j \preceq_p s \text{ whenever } i_j \neq 0; \sum_{j=0}^{s} j i_j \equiv k \bmod p^m - 1\}$. By definition,

$$M_{m,p}(s,k) = \frac{1}{p} \sum_{(i_0,\cdots,i_s) \in S_{(s,k)}} \binom{p}{i_0\ \cdots\ i_{s-1}} \binom{s}{1}^{i_1} \cdots \binom{s}{s-1}^{i_{s-1}} \tag{6.3}$$

$$M_{m,p}(ps,pk) = \frac{1}{p} \sum_{(i'_0,\cdots,i'_{ps}) \in S_{(ps,pk)}} \binom{p}{i_0\ \cdots\ i_{ps-1}} \binom{ps}{1}^{i_1} \cdots \binom{ps}{ps-1}^{i_{s-1}} \tag{6.4}$$

where multiplication by p is modulo n. Note that multiplication modulo n by p cyclically shifts the p-ary representation of any integer. The inverse operation is multiplication modulo n by $p^{(m-1)}$.

For any $(i_0, \cdots, i_s) \in S_{(s,k)}$, whenever $i_j \neq 0$, $j \preceq_p s \Rightarrow pj(\bmod n) \preceq_p ps(\bmod n)$ and so $pj(\bmod n) \leq ps(\bmod n)$. This gives a 1-1 correspondence

$$\begin{aligned} S_{(s,k)} &\rightarrow S_{(ps,pk)} \\ (i_0, \cdots, i_s) &\mapsto (i'_0, \cdots, i'_{ps \bmod n}) \end{aligned}$$

given by

$$\begin{aligned} &i'_{pj \bmod n} = i_j \text{ whenever } i_j \neq 0 \\ &i'_j = 0 \text{ otherwise }. \end{aligned}$$

Such a $(i'_0, \cdots, i'_{ps \bmod n})$ satisfies all the conditions to be in $M_{m,p}(ps, pk)$.

Clearly, under this 1-1 correspondence, the corresponding terms in (6.3) and (6.4) are same. So, $M_{m,p}(s,k) = M_{m,p}(ps, pk)$.

2) Directly follows from (1).

3)

$$\begin{aligned} & M_{m,p}(s,k) \neq 0 \\ \Rightarrow\ & (i_0, \cdots, i_s) \in M_{m,p}(s,k) \\ \Rightarrow\ & k = \sum_{j=0}^{s} j i_j \bmod n \\ \Rightarrow\ & k \leq (s-1).1 + s.(p-1) \quad \text{since } \sum_{j=0}^{s} j i_j \text{ is maximum when } i_s = p-1,\ i_{s-1} = 1 \\ \Rightarrow\ & k \leq ps - 1 \end{aligned}$$

■

In [33], the authors proved that, an extended cyclic code of length p^m over F_{p^m} is affine invariant if and only if it's defining set is a lower ideal of $[0, p^m - 1]$. It was shown in [27] that an extended cyclic code of length p^m over $GR(4, m)$ is affine invariant if and only if $\hat{T}_1, \hat{T}_2$ are lower ideals in $[0, 2^m - 1]$ and $s \in \hat{T}_2, M_{m,p}(s,k) \not\equiv 0 \bmod 2 \Rightarrow 2^{(m-1)}k \in \hat{T}_1$. In the following, we show that the same conditions are valid for codes over $GR(p^2, m)$ for any prime p.

Lemma 6.3.17. *If $x, b \in \mathcal{T}_m \subseteq R = GR(p^2, m)$, $m \geq 1$ and $s \in [0, n], n = p^m - 1$, then*

$$(x+b)^{sp^m} = \sum_{j \preceq_p s} \binom{s}{i}^{p^m} x^j b^{s-j} + p \sum_{k=0}^{n-1} M_{m,p}(s,k) x^{kp^{(m-1)}} b^{(ps-k)p^{(m-1)}}$$

Proof: Let $x, b \in \mathcal{T}_m$. Then

$$
\begin{aligned}
(x+b)^{sp^m} &= \left(\sum_{i=0}^{s} \binom{s}{i} x^i b^{s-i}\right)^{p^m} \\
&= \sum_{i=0}^{s} \left[\binom{s}{i} x^i b^{s-i}\right]^{p^m} \\
&+ \sum_{\substack{(i_0,\cdots,i_s) \\ \sum_{j=0}^{s} i_j = p;\; i_j \neq p\,\forall j \\ j \preceq_p s \text{ whenever } i_j \neq 0}} \binom{p}{i_0 \;\cdots\; i_{s-1}} \binom{s}{0}^{i_0} \binom{s}{1}^{i_1} \cdots \binom{s}{s}^{i_{s-1}} \left[x^{\sum_{j=0}^{s} j i_j} b^{\sum_{j=0}^{s} i_j (s-j)}\right]^{p^{(m-1)}} \\
&= \sum_{j \preceq_p s} \binom{s}{i}^{p^m} x^i b^{s-i} \\
&+ \sum_{\substack{(i_0,\cdots,i_s) \\ \sum_{j=0}^{s} i_j = p;\; i_j \neq p\,\forall j \\ j \preceq_p s \text{ whenever } i_j \neq 0}} \binom{p}{i_0 \;\cdots\; i_{s-1}} \binom{s}{1}^{i_1} \cdots \binom{s}{s-1}^{i_{s-1}} \left[x^{\sum_{j=0}^{s} j i_j} b^{ps-\sum_{j=0}^{s} i_j j}\right]^{p^{(m-1)}} \\
&= \sum_{j \preceq_p s} \binom{s}{i}^{p^m} x^j b^{s-j} + p \sum_{k=0}^{n-1} M_{m,p}(s,k) x^{kp^{(m-1)}} b^{(ps-k)p^{(m-1)}}
\end{aligned}
$$

■

Theorem 6.3.18. *Let $\hat{\mathcal{C}}$ be an extended cyclic code over a subring $GR(p^2, m_1)$ of $GR(p^2, m)$ of length p^m with defining sets $(\hat{T}_1, \hat{T}_2)$. $\hat{\mathcal{C}}$ is affine invariant if and only if*

1. *$\hat{T}_1, \hat{T}_2$ are lower ideals in $[0, n]$.*

2. *$s \in \hat{T}_2, M_{m,p}(s,k) \not\equiv 0 \ mod\ p \Rightarrow p^{(m-1)}k \in \hat{T}_1$*

Proof:

Case I: $0 \notin \hat{T}_2$: Let $\mathcal{C}_2$ be the extended cyclic code of length p^m over $\mathbb{Z}_p$ with defining set $\hat{T}_2$. Then

$$p\mathcal{C}_2 = \{\mathbf{a} \in \hat{\mathcal{C}} |\text{ all components of } \mathbf{a} \text{ are in } p\mathbb{Z}_{p^2}\}$$

So,

$$
\begin{aligned}
& Per(\mathcal{C}_2) \subseteq Per(\hat{\mathcal{C}}) \\
\Rightarrow\ & \mathcal{C}_2 \text{ is affine invariant} \\
\Rightarrow\ & \hat{T}_2 \text{ is a lower ideal} \\
\Rightarrow\ & \hat{T}_2 \text{ is empty since } 0 \notin \hat{T}_2
\end{aligned}
$$

The code $\mathcal{C}_1 \subseteq F_{p^{m_1}}^{n+1}$ obtained from $\hat{\mathcal{C}}$ by taking component-wise image under the canonical homomorphism $R \to \frac{R}{pR} \simeq F_{p^{m_1}}$ has defining set $\hat{T}_1$. Clearly, $\mathcal{C}_1$ is also affine invariant if $\hat{\mathcal{C}}$ is affine invariant. So, $\hat{T}_1$ is a lower ideal. Hence the condition (1) holds and condition (2) holds vacuously. Case II: $0 \in \hat{T}_2$: By [27, Theorem 4.2], $\hat{\mathcal{C}}$ is affine invariant if and only if the polynomials in the set

$$\{(f_\sigma^{(L)}(Z))^{sp^m} | s \in \hat{T}_2\} \cup \{p(f_\sigma^{(L)}(Z))^{sp^m} | s \in \hat{T}_1\}$$

are MS polynomials of $\hat{\mathcal{C}}$ $\forall \sigma \in AGL(1,p^m)$. Since $\hat{\mathcal{C}}$ is extended cyclic, it is sufficient to check this only for permutations given by $f_\sigma^{(L)}(Z) = Z + b,\ b \in \mathcal{T}_m \setminus \{0\}$.

If $s \in \hat{T}_1$, then

$$p(Z+b)^{sp^m} \equiv p \sum_{i \preceq_p s} \left(\begin{array}{c} s \\ i \end{array} \right)^{p^m} b^{s-i} Z^i \mod Z^n - 1$$

This is an MS polynomial of $\hat{\mathcal{C}}$ if $i \in \hat{T}_1\ \forall i \preceq_p s$, i.e. $\hat{T}_1$ must be a lower ideal.

If $s \in \hat{T}_2$, then by Lemma 6.3.17,

$$\begin{aligned} (Z+b)^{sp^m} &= \sum_{i \preceq_p s} \left(\begin{array}{c} s \\ i \end{array} \right)^{p^m} b^{s-i} Z^i \\ &\quad + p \sum_{k=0}^{n-1} M_{m,p}(s,k) b^{(ps-k)p^{(m-1)}} Z^{kp^{(m-1)}} \mod (Z^n - 1) \end{aligned}$$

This will be an MS polynomial of $\hat{\mathcal{C}}$ if $i \in \hat{T}_2$ whenever $i \preceq_p s$ (i.e. $\hat{T}_2$ is a lower ideal) and if $M_{m,p}(s,k) \not\equiv 0 \mod p \Rightarrow kp^{(m-1)} \in \hat{T}_1$. Thus conditions (1) and (2) must hold for $\hat{\mathcal{C}}$ to be affine invariant and vice versa. ■

The following theorem gives some sufficient conditions under which extended BCH codes of length p^m over $\mathbb{Z}_{p^2}$ are affine invariant.

Theorem 6.3.19. *Let $\hat{B}(n,\delta_1,\delta_2)$ be an extended BCH code of length p^m. If either (i) $p|(\delta_2 - 1)$ and $\delta_1 \geq p(\delta_2 - 2)$ or (ii) $\delta_1 \geq p(\delta_2 - 1)$, then $\hat{B}(n,\delta_1,\delta_2)$ is affine invariant.*

Proof: The defining sets of the code are

$$\hat{T}_1 = \cup_{i \in [0,\delta_1)} [i]^q$$

$$\hat{T}_2 = \cup_{i \in [0,\delta_2)} [i]^q$$

Clearly, both these are lower ideals. We need to check that, $k \in T_1$ whenever $M_{m,p}(s,k) \not\equiv 0 \bmod p$ and $s \in T_2$. By Lemma 6.3.16(2), it is sufficient to consider $s \leq \delta_2 - 1$ which are not divisible by p.

Suppose condition (ii) holds and $s \in T_2$, $M_{m,p}(s,k) \not\equiv 0 \bmod p$. Then

$$
\begin{aligned}
& s \leq \delta_2 - 1 \\
\Rightarrow\quad & ps - 1 \leq p(\delta_2 - 1) - 1 = p\delta_2 - p - 1 \\
\Rightarrow\quad & k \leq p\delta_2 - p - 1 \text{ whenever } M_{m,p}(s,k) \not\equiv 0 \bmod n \text{ (by Lemma 6.3.16(3))} \\
\Rightarrow\quad & k \leq \delta_1 - 1 \text{ whenever } M_{m,p}(s,k) \not\equiv 0 \bmod n \\
\Rightarrow\quad & k \in \hat{T}_1 \text{ whenever } M_{m,p}(s,k) \not\equiv 0 \bmod n
\end{aligned}
$$

If condition (i) holds, then it is sufficient to consider $s \leq \delta_2 - 2$ since by Lemma 6.3.16(2), we need not consider s, which are divisible by p. Then

$$
\begin{aligned}
& s \leq \delta_2 - 2 \\
\Rightarrow\quad & ps - 1 \leq p(\delta_2 - 2) - 1 = p\delta_2 - 2p - 1 \\
\Rightarrow\quad & k \leq p\delta_2 - 2p - 1 \text{ whenever } M_{m,p}(s,k) \not\equiv 0 \bmod n \text{ (by Lemma 6.3.16(3))} \\
\Rightarrow\quad & k \leq \delta_1 - 1 \text{ whenever } M_{m,p}(s,k) \not\equiv 0 \bmod n \\
\Rightarrow\quad & k \in \hat{T}_1 \text{ whenever } M_{m,p}(s,k) \not\equiv 0 \bmod n
\end{aligned}
$$

■

6.4 Conclussion

A set of necessary and sufficient conditions were derived for extended cyclic codes of length p^m over any subring of $GR(p^e, m)$ to be affine invariant for $p = 2$ with arbitrary e and for $e = 2$ with arbitrary p. Classes of affine invariant BCH codes and GRM codes over $\mathbb{Z}_{2^e}$ and over $\mathbb{Z}_{p^2}$ are found using these conditions. However, necessary and sufficient conditions for any BCH or GRM code to be affine invariant remain open.

Chapter 7

Conclusion

In chapter 4 and 5, the permutation groups considered are abelian. Though it covers many important classes of codes, this approach does not apply to the cases when G is nonabelian. As example, famous class of affine invariant codes are not tractable by this approach. Another limitation of this approach is the restriction that the exponent of G has to be relatively to prime to q.

Though Chapter 2 shows one way to investigate algebraic structure of F_qLC codes, it does not give the much wanted information on minimum Hamming distance of these codes. Even the bound on the minimum Hamming distance of the corresponding quasi-cyclic codes is also not easy enough to apply for long codes.

The necessary and sufficient conditions for extended cyclic codes over Galois rings to be affine invariant was derived in Chapter 6. Some necessary and sufficient conditions were first derived in group algebra method by Abdukhalikov [34] for the more general alphabet of p-adic integers. Though the conditions derived in Chapter 6 or those derived in [27] don't appear to be same as those derived by Abdukhalikov, a few example calculations showed the restrictions on the defining sets required by those sets of conditions to be same for those examples. The classes of affine invariant codes found using the conditions derived in this thesis are however completely new.

7.1 Scope for Further Work

All F_{q^m}-linear cyclic codes over F_{q^m} are F_qLC codes and not conversely. It is worth investigating to obtain a criteria/conditions under which a code can be seen as a linear code over F_{q^m} w. r. t. a different multiplication structure in F_{q^m}. In particular, this problem, when special ized to the class of group cyclic codes over elementary abelian groups is important since MDS group cyclic codes which are not linearizable have been reported [74, 75].

It would be interesting to investigate the best choice of basis for a given F_qLC code for maximizing the minimum distance (or it's bound) of the corresponding quasi-cyclic code.

All the transform techniques discussed in this thesis are valid only when the characteristic of the alphabet field or Galois ring is relatively prime to the exponent of the defining permutation group for the particular class of codes. Works on transform technique for the general case (i.e. when the above condition is not necessarily satisfied) is very limited. The resulting class of cyclic codes over finite fields is known as repeated root cyclic codes. Satisfactory structural analysis is done on this class of codes [47–50, 103, 104]. Though the technique using Groebner basis [7] handles the general case for quasi-cyclic codes, the suitable transform domian technique may give interesting insights. More generally, codes closed under arbitrary abelian group G of permutations, when G's exponent is not necessarily relatively prime to the characteristic of the alphabet field (and Galois ring in general) is untouched and is an interesting direction to persue.

In chapter 2, 3, 4, 5, the defining permutation group of the classes of codes considered are abelian groups. Available work on non-abelian codes and codes closed under non-abelian group of permutations is very limited. MacWilliams [105] investigated algebraic structure of codes defined over dihedral groups using group algebra method. This suggests that, codes closed under at least some nonabelian groups G of permutations may be tractable with some suitably defined DFT.

Bibliography

[1] Y. Edel and J. Bierbrauer, "Twisted BCH codes," *Jl. of Comb. Designs*, vol. 5, pp. 377–389, 1997.

[2] M. Hattori, R. J. McEliece, and G. Solomon, "Subspace subcodes of Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1861–1880, 1998.

[3] C. L. Chen, W. W. Peterson, and E. J. Weldon, "Some results on quasic-cyclic codes," *Information and Control*, vol. 15, pp. 407–423, 1969.

[4] T. Kasami, "A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2," *IEEE Trans. Inform. Theory*, vol. 24, pp. 627–628, 1978.

[5] J. Conan and G. Seguin, "Structural properties and enumeration of quasi cyclic codes," *Applicable Algebra in Engineering Communication and Computing*, pp. 25–39, 1993.

[6] G. E. Seguin and G. Drolet, "The trace description of irreducible quasi-cyclic codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1463–1466, 1990.

[7] K. Lally and P. Fitzpatrick, "Algebraic structure of quasi-cyclic codes," *Discrete Appl. Math.*, vol. 111, pp. 157–175, 2001.

[8] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes I: Finite fields," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 2751–2760, 2001.

[9] S. K. Wasan, "Quasi abelian codes," *Publ. de L'Institute Mathematique*, vol. 21, pp. 201–206, 1977.

[10] P. Shankar, "On BCH codes over arbitrary integer rings," *IEEE Trans. Inform. Theory*, vol. 25, no. 4, pp. 480–483, 1979.

[11] S. K. Wasan, “On codes over $\mathbb{Z}_m$,” *IEEE Trans. Inform. Theory*, vol. 28, pp. 117–120, 1982.

[12] G. H. Norton and A. Sălăgean, “On the Hamming distance of linear codes over a finite chain ring,” *IEEE Trans. Inform. Theory*, vol. 46, no. 3, pp. 1060–1067, 2000.

[13] G. H. Norton and A. Sălăgean, “On the structure of linear and cyclic codes over a finite chain ring,” *Applicable algebra in engineering, communication and computing*, vol. 10, pp. 489–506, 2000.

[14] A. R. Calderbank and N. J. A. Sloane, “Modular and p-adic codes,” *Design, Codes and Cryptography*, vol. 6, pp. 21–35, 1995.

[15] J. C. Interlando, R. Palazzo, and M. Elia, “On the decoding of Reed-Solomon and BCH codes over integer residue rings,” *IEEE Trans. Inform. Theory*, vol. 43, pp. 1013–1021, 1997.

[16] A. Bonnecaze, P. Solé, C. Bachoc, and B. Mourrain, “Type II codes over $\mathbb{Z}_4$,” *IEEE Trans. Inform. Theory*, vol. 43, pp. 969–976, 1997.

[17] A. R. Calderbank, G. McGuire, P. V. Kumar, and T. Helleseth, “Cyclic codes over $\mathbb{Z}_4$, locator polynomials and Newton’s identities,” *IEEE Trans. Inform. Theory*, vol. 42, pp. 217–226, 1996.

[18] V. S. Pless and Z. Qian, “Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$,” *IEEE Trans. Inform. Theory*, vol. 42, pp. 1594–1600, 1996.

[19] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, “The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes,” *IEEE Trans. Inform. Theory*, vol. 40, no. 2, pp. 301–319, 1994.

[20] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, 1988.

[21] H. Chabanne, “Permutation decoding of abelian codes,” *IEEE Trans. Inform Theory*, vol. 38, no. 6, pp. 1826–1829, 1992.

[22] F. J. MacWilliams, “Permutation decoding of systematic codes,” *Bell Sys. Tech. Jl.*, pp. 485–505, 1964.

[23] W. C. Huffman, "Codes and groups," in *Handbook of Coding Theory* (V. S. Pless and W. C. Huffman, eds.), vol. 2, ch. 17, pp. 1345–1440, New York, NY, USA: Elsevier Science, 1998.

[24] L. M. G. M. Tolhuizen and W. J. V. Gils, "A large automorphism group decreases the computations in the construction of an optimal encoder/decoder pair for a linear block code," *IEEE Trans. Inform. Theory*, vol. 34, no. 2, pp. 333–337, 1988.

[25] D. M. Gordon, "Minimal permutation sets for decoding the binary golay codes," *IEEE Trans. Inform. Theory*, vol. 28, pp. 541–543, 1982.

[26] J. Wolfman, "A permutation decoding of the (24,12,8) golay code," *IEEE Trans. Inform. Theory*, vol. 29, pp. 748–750, 1983.

[27] J. T. Blackford and D. K. Ray-Chaudhuri, "A transform approach to permutation groups of cyclic codes over galois rings," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2350–2358, 2000.

[28] A. Dur, "The automorphism groups of Reed-Solomon codes," *Jl. Comb. Theory, Series A*, vol. 44, pp. 69–82, 1987.

[29] T. P. Berger, "On the automorphism groups of affine-invariant codes," *Design, Codes and Cryptography*, vol. 7, pp. 215–221, 1996.

[30] T. P. Berger and P. Charpin, "The permutation group of affine-invariant extended cyclic codes," *IEEE Trans. Inform. Theory*, vol. 42, no. 6, pp. 2194–2209, 1996.

[31] T. P. Berger and P. Charpin, "The automorphism group of generalized Reed-Muller codes," *Discrete Math.*, vol. 117, no. 6, pp. 1–17, 1993.

[32] T. P. Berger and P. Charpin, "The automorphism groups of BCH codes and of the affine-invariant codes over extension fields," *Design, Codes and Cryptography*, vol. 18, pp. 29–53, 1999.

[33] T. Kasami, S. Lin, and W. W. Perterson, "Some result on cyclic codes which are invariant under the affine group and their applications," *Information and Control*, vol. 11, pp. 475–496, 1968.

[34] K. S. Abdukhalikov, "Affine invariant and cyclic codes over p-adic numbers and finite rings," *Design, Codes and Cryptography*, vol. 23, no. 3, pp. 343–370, 2001.

[35] H. F. Mattson and G. Solomon, "A new treatment of Bose-Chaudhuri codes," *Jl. SIAM*, vol. 9, no. 4, pp. 654–669, 1961.

[36] R. E. Blahut, "Transform techniques for error-control codes," *IBM Jl. Res. Develop.*, vol. 23, pp. 299–315, 1979.

[37] P. Delsarte, "Automorphisms of abelian codes," *Philips Research Reports*, vol. 25, pp. 389–402, 1970.

[38] R. E. Blahut, *Theory and Practice of Error Control Codes.* Addison Wesley, 1983.

[39] R. Tolimieri, "The algebra of the finite Fourier transform and coding theory," *Trans. of the AMS*, vol. 287, pp. 253–273, 1985.

[40] S. V. Kanetkar and M. D. Wagh, "Group character tables in discrete transform theory," *Jl. of Computer and System Sciences*, vol. 19, pp. 211–221, 1979.

[41] H. B. Kekre, M. D. Wagh, and S. V. Kanetkar, "On group theoretic transforms and the automorphism groups," *Information and Control*, vol. 41, pp. 147–155, 1979.

[42] V. S. Pless and W. C. Huffman, eds., *Handbook of Coding Theory.* Reading, Mass.: Elsevier Science, 1998.

[43] V. S. Pless, *Introduction to the Theory of Error-Correcting Codes.* New York: Wiley, 1989.

[44] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes.* Cambridge, Massachusetts: MIT Press, 1972.

[45] E. R. Berlekamp, *Algebraic coding theory.* Laguna Hills, California: Aegean Park Press, 1984.

[46] R. J. McEliece, *The Theory of Information and Coding.* Cambridge: Cambridge University Press, 1984.

[47] P. Mathys, "Frequency domain description of repeated-root cyclic codes," in *Proceedings of 1994 IEEE International Symposium on Information Theory, Trondheim, Norway*, p. 47, 1994.

[48] G. Gunther, “A finite field Fourier trnasform for vectors of arbitrary length,” in *Communications and Cryptography: Two Sides of One Tapestry* (R. E. Blahut, D. J. Costello, U. Maurer, and T. Mittelholzer, eds.), pp. 141–153, Kluwer Academic Pub., 1994.

[49] G. Castagnoli, J. L. Massey, P. A. Schoeller, and V. von Semann, “On repeated-root cyclic codes,” *IEEE Trans. Inform. Theory*, vol. 37, pp. 337–342, 1991.

[50] J. H. Van Lint, “Repeated-root cyclic codes,” *IEEE Trans. Inform. Theory*, vol. 37, pp. 343–345, 1991.

[51] T. A. Gulliver and V. K. Bhargava, “Two new rate 2/p binary quasi-cyclic codes,” *IEEE Trans. Inform. Theory*, vol. 40, pp. 1667–1668, 1994.

[52] T. A. Gulliver and V. K. Bhargava, “Some best rate 1/p and rate (p-1)/p systematic quasi-cyclic codes,” *IEEE Trans. Inform. Theory*, vol. 37, pp. 552–555, 1991.

[53] T. A. Gulliver and V. K. Bhargava, “Nine good rate (m-1)/pm quasi-cyclic codes,” *IEEE Trans. Inform. Theory*, vol. 38, pp. 1366–1369, 1992.

[54] T. A. Gulliver and V. K. Bhargava, “Some best rate 1/p and rate (p-1)/p systematic quasi-cyclic codes over GF(3) and GF(4),” *IEEE Trans. Inform. Theory*, vol. 38, pp. 1369–1374, 1992.

[55] T. A. Gulliver and V. K. Bhargava, “Twelve good rate (m-r)/pm quasi-cyclic codes,” *IEEE Trans. Inform. Theory*, vol. 39, pp. 1750–1751, 1993.

[56] J. M. Stein, V. K. Bhargava, and S. E. Tavares, “Weight distribution of some ”Best” (3m, 2m) binary quasi-cyclic codes,” *IEEE Trans. Inform. Theory*, vol. 21, pp. 708–711, 1975.

[57] Z. Chen, “New results on binary quasi-cyclic codes,” in *Proceedings of 2000 IEEE International Symposium on Information Theory, Sorrento, Italy*, p. 197, 2000.

[58] I. F. Blake, “Codes over certain rings,” *Inform. Contr.*, vol. 20, pp. 296–404, 1972.

[59] I. F. Blake, “Codes over integer residue rings,” *Inform. Contr.*, vol. 29, pp. 295–300, 1975.

[60] E. Spiegel, “Codes over $\mathbb{Z}_m$,” *Inform. Contr.*, vol. 35, pp. 48–51, 1977.

[61] E. Spiegel, "Codes over $\mathbb{Z}_m$, revisited," *Inform. Contr.*, vol. 37, pp. 100–104, 1978.

[62] B. S. Rajan and M. U. Siddiqi, "Transform domain characterization of cyclic codes over Z_m," *Applicable Algebra in Engineering, Communication and Computing*, vol. 40, no. 5, pp. 261–276, 1994.

[63] B. S. Rajan and M. U. Siddiqi, "A generalized DFT for abelian codes over Z_m," *IEEE Trans. on Inform. Theory*, vol. 40, no. 5, pp. 2082–2090, 1994.

[64] M. Karlin, "Decoding of circulant codes," *IEEE Trans. Inform. Theory*, vol. 16, pp. 797–802, 1970.

[65] P. Heijnen and H. C. A. van Tilborg, "The decoding of binary quasi-cyclic codes," in *Communications and Coding* (M. Darnell and B. Honary, eds.), pp. 146–159, Taunton: Research Studies Press, 1998.

[66] C. L. Chen, "Byte-oriented error-correcting codes for semiconductor memory systems," *IEEE Trans. on Computers*, vol. 35, pp. 646–648, 1986.

[67] C. L. Chen and L. E. Grosbach, "Fault-tolerant memory design in the ibm application system/400," pp. 393–400, 1991.

[68] C. L. Chen and M. Y. Hsiao, "Error-correcting codes for semiconductor memory applications: a state-of-the-art review," *IBM Jl. of Res. Dev.*, vol. 2, pp. 124–134, 1984.

[69] C. L. Chen, "Symbol error-correcting codes for computer memory systems," *IEEE trans. on Comp.*, vol. 35, pp. 646–648, 1986.

[70] C. L. Chen and L. E. Grosbach, "Switching codes for delta-i noise reduction," *IEEE trans. on Comp.*, vol. 45, pp. 1017–1021, 1996.

[71] G. D. Forney, Jr., "Geometrically uniform codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1241–1260, 1991.

[72] G. D. Forney, Jr., "On the hamming distance properties of group codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1797–1801, 1992.

[73] M. Isaksson and L. H. Zetterberg, "Block-coded m-PSK modulation over $gf(m)$," *IEEE Trans. Inform. Theory*, vol. 39, pp. 337–346, 1993.

[74] M. Ran and J. Snyders, "A cyclic [6,5,4] group code and the hexacode over $gf(4)$," *IEEE Trans. on Inform. Theory*, vol. 42, pp. 1250–1253, 1996.

[75] A. A. Zain and B. S. Rajan, "Algebraic characterization of MDS group codes over cyclic groups," *IEEE Trans. Inform. Theory*, vol. 37, pp. 343–345, 1991.

[76] J. M. Jensen, "Subgroup subcodes," *IEEE Trans. Inform. Theory*, vol. 41, pp. 781–785, 1995.

[77] F. J. MacWilliams, "Decomposition of cyclic codes of block lengths 3p, 5p, 7p," *IEEE Trans. Inform. Theory*, vol. 25, pp. 112–118, 1979.

[78] J. Bierbrauer, "The theory of cyclic codes and a generalization to additive codes," 2000. Downloadable manuscript from http://www.math.mtu.edu/ jbierbra/.

[79] J. Bierbrauer, "Direct constructions of additive codes," 2000. Downloadable manuscript from http://www.math.mtu.edu/ jbierbra/.

[80] R. M. Tanner, "A transform theory for a class of group-invariant codes," *IEEE Trans. Inform. Theory*, vol. 34, no. 4, pp. 752–775, 1988.

[81] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20. Reading, Mass.: Addison Wesley, 1983.

[82] G. Seroussi and A. Lempel, "Factorization of symmetric matrices and trace-orthogonal bases in finite fields," *SIAM Jl. Computing*, vol. 9, pp. 758–767, 1980.

[83] G. Solomon and H. van Tilborg, "A connection between block and convolutional codes," *SIAM J. Appl. Math.*, vol. 37, pp. 358–4369, 1979.

[84] M. Esmaeili, T. A. Gulliver, N. P. Secord, and S. A. Mahmoud, "A link between quasi-cyclic codes and convolutional codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 431–435, 1998.

[85] V. K. Bhargava, G. E. Seguin, and J. M. Stein, "Some (mk, k) cyclic codes in quasi-cyclic form," *IEEE Trans. Inform. Theory*, vol. 24, no. 6, pp. 630–632, 1978.

[86] J. M. Stein and V. K. Bhargava, "Equivalent rate $\frac{1}{2}$ quasi-cyclic codes," *IEEE Trans. Inform. Theory*, vol. 21, pp. 588–589, 1975.

[87] S. E. Tavares, V. K. Bhargava, and S. G. S. Shiva, "Some rate-p/(p+1) quasi-cyclic codes," *IEEE Trans. Inform. Theory*, vol. 20, pp. 133–135, 1974.

[88] H. van Tilborg, "On quasi-cyclic codes with rate 1/m," *IEEE Trans. Inform. Theory*, vol. 24, pp. 628–630, 1978.

[89] M. Karlin, "New binary coding results by circulants," *IEEE Trans. Inform. Theory*, vol. 15, pp. 81–92, 1969.

[90] A. R. Calderbank, G. D. Forney, Jr., and A. Vardy, "Minimal tail-biting trellises: the golay codes and more," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1435–1255, 1999.

[91] B. S. Rajan and M. U. Siddiqi, "Transform domain characterization of abelian codes," *IEEE Trans. on Inform. Theory*, vol. 38, pp. 1871–1821, 1992.

[92] S. Ling and P. Solé, "Decomposing quasi-cyclic codes," *Private Communication*, 2001.

[93] V. Pless, "On the uniqueness of the Golay codes," *J. Comb. Th.*, vol. 5, pp. 215–228, 1968.

[94] E. M. Rains and N. J. A. Sloane, "Self-dual codes," in *Handbook of Coding Theory* (V. S. Pless and W. C. Huffman, eds.), ch. 3, pp. 177–294, New York, NY, USA: Elsevier Science, 1998.

[95] B. R. McDonald, *Finite Rings with Identity.* New York: Marcel Dekker, 1974.

[96] P. Gaborit, "Mass formulas for self-dual codes over Z_4 and $F_q + uF_q$ rings," *PGIT*, vol. 42, pp. 1222–1228, 1996.

[97] M. Greferath and U. Vellbinger, "Efficient decoding of $\mathbb{Z}_{p^k}$-linear codes," *IEEE Trans. Inform. Theory*, vol. 44, no. 3, pp. 1288–1291, 1998.

[98] N. S. Babu and K. Zimmermann, "Decoding of linear codes over Galois rings," *IEEE Trans. Inform. Theory*, vol. 47, no. 4, pp. 1599–1603, 2001.

[99] E. Byrne, "Lifting decoding schemes over a Galois rings," in *Proceedings of AAECC-14 (LNCS vol. 2227), RMIT University, Melbourne, Australia, Nov. 26-30*, pp. 323–332, 2001.

[100] T. Helleseth and P. V. Kumar, "The algebraic decoding of the $\mathbb{Z}_4$-linear Goethals code," *IEEE Trans. Inform. Theory*, vol. 41, pp. 2040–2048, 1995.

[101] B. S. Rajan and M. U. Siddiqi, "Transform decoding of BCH codes over $\mathbb{Z}_m$," *Int. J. Electron.*, vol. 75, pp. 1043–1054.

[102] W. C. Huffman, "Decompositions and extremal type II codes over $\mathbb{Z}_4$," *IEEE Trans. Inform. Theory*, vol. 44, pp. 334–352, 1998.

[103] S. D. Berman, "On the theory of group codes," *Kibernetika*, vol. 3, no. 1, pp. 25–31, 1967.

[104] S. D. Berman, "Semisimple cyclic and abelian codes II," *Kibernetika*, vol. 3, no. 3, pp. 17–23, 1967.

[105] F. J. MacWilliams, "Codes and ideals in group algebras," in *Combinatorial Mathematics and its Applications* (R. C. Bose and T. Dowling, eds.), pp. 317–328, Chapel Hill, NC: University of North Carolina Press, 1969.