NANYANG TECHNOLOGICAL UNIVERSITY

ON SELF-DUAL CYCLIC CODES AND GENERALIZED SELF-DUAL CYCLIC CODES OVER FINITE FIELDS

YAN JIA

Division of Mathematical Sciences

School of Physical and Mathematical Sciences

2011

ON SELF-DUAL CYCLIC CODES AND GENERALIZED SELF-DUAL CYCLIC CODES OVER FINITE FIELDS

YAN JIA

Division of Mathematical Sciences
School of Physical and Mathematical Sciences

A thesis submitted to Nanyang Technological University

in fulfillment of the requirement for the degree of

Doctor of Philosophy in Mathematical Sciences

19 December 2011

Acknowledgement

It is a pleasure to thank the many people who made this thesis possible.

First and foremost, my utmost gratitude to my Ph.D supervisor, Professor San Ling, whose sincerity and encouragement I will never forget. With his enthusiasm, his inspiration, his patience, his academic experience and his great efforts to explain things clearly and simply, he helped to make mathematics fun for me. I want to thank him for teaching me how to do research. I want to thank him for teaching me how to be a good mathematician. I want to thank him for believing in me as I overcome all the obstacles in the completion of this research work. It is difficult to overstate my gratitude to Professor San Ling. I would like to say that I would have been lost without him.

I am deeply grateful to Professors Chaoping Xing, Patrick Solé and Henk D. L. Hollmann for numerous discussion online and in person. I want to thank them for all their help, support, interest and valuable hints.

I wish to express my warm and sincere thanks to Professors Hao Shen, Dexing Kong and Baorui Song from Department of Mathematics, Shanghai Jiao Tong University, China whose letters gave me important guidance during my first steps into coding theory studies.

I am indebted to my many friends in the math division for providing a stimulating and fun environment in which to learn and grow. I am especially grateful to Romar dela Cruz, Martianus Frederic Ezerman, Peng Gao, Somphong Jitman, Jiang Liu, Yin Tan, Jing Yang and Xiande Zhang.

I am grateful to the staff of Nanyang Technological University, for assisting me in many different ways. Claire Lin and Melvin Soh deserve special mention.

I wish to thank the anonymous examiner for suggestions that improved the quality of the work. I also wish to thank the committee of my thesis and all the lecturers during my study. In particular, I would like to thank School of Physical and Mathematical Sciences, Nanyang Technological University for providing opportunity and financial support.

Lastly, and most importantly, I wish to thank my parents. They raised me, supported me, taught me, and loved me. To them I dedicate this thesis.

List of Works

Below is the list of work done, in chronological order, during my PhD studies in NTU.

1. Y. Jia, S. Ling, and C. Xing, *On Self-Dual Cyclic Codes Over Finite Fields*, IEEE Transactions on Information Theory, Vol. 57, No. 4, pp. 2243–2251, April 2011.

2. Y. Jia, *On Quasi-twisted Codes over Finite Fields*, Finite Fields and their Applications, Accepted 1 August 2011, Available online 15 September 2011.

3. Y. Jia, S. Ling, and P. Solé *On Isodual Cyclic Codes over Finite Fields*, Final stage of preparation.

Contents

Abstract

Cyclic codes over finite fields form an important class of codes which has been extensively studied, for their interesting algebraic structure, and many "good" codes are cyclic. Therefore, it is natural to try to generalize the notion, for example in the search of good codes, or to generalize the algebraic properties. The duality of cyclic codes and the algebraic structure of generalized cyclic codes are the main objects of this work.

A cyclic code over a finite field is a vector space over a finite field, and the dual is the orthogonal complement. When this dual code is the same as the original code, we call the code self-dual. When the dual code can be obtained by a certain type of transformation from the original code, then we call the code isodual ("isomorphic" to dual in some sense).

For self-duality, it is shown that self-dual cyclic codes of length n over $\mathbb{F}_q$ exist if and only if n is even and $q = 2^m$ with m a positive integer. The enumeration of such codes is also investigated. When n and q are even, there is always a trivial self-dual cyclic code with generator polynomial $x^{\frac{n}{2}} + 1$. We therefore classify the existence of self-dual cyclic codes, for given n and q, into two cases: when only the trivial one exists and when two or more such codes exist. Given n and m, an easy criterion to

determine which of these two cases occurs is given in terms of the prime factors of n, for most n. It is also shown that, over a fixed field, the latter case occurs more frequently as the length grows.

For isoduality, two classes of isodual cyclic codes are considered: cyclic codes equivalent to their dual codes up to a multiplier permutation and cyclic codes equivalent to their dual codes up to a scalar transformation. The construction as well as the enumeration are given.

Cyclic codes are namely invariant under cyclic shift on their codewords. To generalize the notion, we can define quasi-cyclic codes: the codes that are invariant under l-cyclic shifts on their codewords, for some positive integer l. We can also define constacyclic codes: the codes that are invariant under cyclic shift while multiplying the shifted part of the codewords by a constant. Combining the above two notions, we have quasi-twisted (QT) codes. For generalized cyclic codes, we mainly focus on QT codes since QT codes include cyclic codes, quasi-cyclic codes and constacyclic codes as special cases. We decompose a QT code to a direct sum of component codes – linear codes over rings. Furthermore, given the decomposition of a QT code, we can describe the decomposition of its dual code. We also use the generalized discrete Fourier transform to give the inverse formula for both the so-called nonrepeated-root and so-called repeated-root cases. Then we produce a formula which can be used to construct a QT code given the component codes.

Chapter 1

Introduction

In coding theory, cyclic codes over finite fields form an important class of block codes that has been extensively studied, for their beautiful underlying algebraic structures, fascinating links to other objects such as polynomials and lattices, as well as for practical use. The main objects of this thesis are cyclic codes and generalized cyclic codes – so called quasi-twisted codes. In particular, we investigate issues related to duality of cyclic codes and algebraic structure of generalized cyclic codes including cyclic codes.

In Chapter 3, we discuss self-dual cyclic codes over finite fields. In particular, we investigate issues related to their existence, characterization and enumeration.

It is shown that self-dual cyclic codes of length n over $\mathbb{F}_q$ exist if and only if q is a power of 2 and n is even. When these conditions are met, there is always a *trivial self-dual cyclic code* with generator polynomial $x^{\frac{n}{2}} + 1$. A natural question that then arises is the existence of self-dual cyclic codes other than this trivial one.

One approach to this question is to enumerate all self-dual cyclic codes of length n

over $\mathbb{F}_{2^m}$, for any given n and m. It is well known that cyclic codes of length n over $\mathbb{F}_q$ may be regarded as ideals in the quotient polynomial ring $\frac{\mathbb{F}_q[x]}{(x^n-1)}$, which is a principal ideal ring. Hence each cyclic code is uniquely generated by a generator polynomial in the corresponding ideal – the unique monic polynomial of minimal degree which is also a factor of $x^n - 1$. Based on the irreducible factors of $x^n - 1$, we obtain a characterization of the generator polynomials of the self-dual cyclic codes. Using the characterization, we produce a formula for the desired enumeration of self-dual cyclic codes.

An explicit form of this enumeration formula involves a two-variable function χ defined number-theoretically as follows: $\chi(j, m) = 0$ if j divides $(2^m)^k + 1$ for some $k \geq 0$, and $\chi(j, m) = 1$ otherwise. It turns out that the question on the existence of self-dual cyclic codes other than the trivial one can be directly addressed via the values of this function $\chi(j, m)$, where m is as in the underlying field $\mathbb{F}_{2^m}$ and j runs through all the odd prime factors of the length n. An analysis of the values of $\chi(j, m)$ provides us directly with the answer to the above question for all n without any prime factor congruent to 1 modulo 8. No enumeration formula is needed.

Another natural question that subsequently emerges is the following: over a fixed field $\mathbb{F}_{2^m}$ and as the length n grows, which of the following two cases occurs more frequently – where only the trivial self-dual cyclic code of length n exists, or where there are at least two such codes? By an analysis of the asymptotic behavior of the function χ, we confirm that it is more common to have two or more self-dual cyclic codes of length n as n grows.

Since self-dual cyclic codes only exist over finite fields of characteristic 2, it is natural to consider a class of codes similar to self-dual cyclic codes that exists over

finite fields of odd characteristic, e.g., $\mathbb{F}_3$. Although a cyclic code and its dual code are never equal over a finite field of odd characteristic, they can be equivalent. Therefore, in Chapter 4, we focus on isodual cyclic codes – the cyclic codes which are equivalent to their dual code. There are 3 ways to define the equivalence of codes over finite fields.

Definition 1.0.1. *[20] Two codes over a finite field, say $\mathscr{C}_1$ and $\mathscr{C}_2$, are said to be* equivalent *if $\mathscr{C}_2$ can be obtained from $\mathscr{C}_1$ by one of the following transformations.*

1. *Permutations of the coordinates.*
2. *Scalar transformation (that is, multiplication of the coordinates by nonzero field elements).*
3. *Monomial transformations of the coordinates (that is, a permutation of the coordinates followed by multiplication of the coordinates by nonzero field elements),*

where the scalar transformation is defined as follows.

Definition 1.0.2. *The* scalar transformation*, denoted by Λ, is a transformation defined on the vector space $\mathbb{F}_q^n$ as*

$$\Lambda : \mathbb{F}_q^n \to \mathbb{F}_q^n$$

$$(v_0, v_1, \ldots, v_{n-1}) \mapsto (\lambda_0 v_0, \lambda_1 v_1, \ldots, \lambda_{n-1} v_{n-1}),$$

where $\lambda_i \in \mathbb{F}_q^*$ for $0 \leq i \leq n-1$. Furthermore, Λ is said to be corresponding to the vector $(\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$, denoted by $\Lambda = (\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$.

It is not easy to decide whether two codes are equivalent up to a permutation[19]. Moreover, by Theorem 4.3.17 in [5, p.141], if $\gcd(n, \phi(n)) = 1$, where $\phi(n)$ is the

Euler function, then two cyclic codes of length n are equivalent up to permutations if and only if they are equivalent up to the following particular kind of permutations – multiplier permutations:

Definition 1.0.3. *A multiplier permutation is defined on the n coordinates of a vector over $\mathbb{F}_q$ (indexed from 0 to $n-1$) as:*

$$\mu_e : \mathbb{F}_q^n \to \mathbb{F}_q^n$$

$$(v_0, v_1, \ldots, v_{n-1}) \mapsto (v_0, v_e, v_{2e}, \ldots, v_{(n-1)e}),$$

where all the subscripts are taken modulo n and e is a positive integer coprime to n (to make sure that μ_e permutes the coordinates). The integer e is called the multiplier.

In this case, studying isodual cyclic codes up to all the permutations is equivalent to studying those up to multiplier permutations. Furthermore, since a monomial transformation of the coordinates is a combination of a permutation and a scalar transformation, throughout Chapter 4, we restrict ourselves to the following two types of equivalence:

E1: Multiplier permutation.

E2: Scalar transformation (multiplication of the coordinates by nonzero field elements).

In Chapter 4, we study isodual cyclic codes up to a multiplier permutation and those up to a scalar transformation. To simplify the description, we give the following definition.

Definition 1.0.4. *A code is said to be E1-isodual if the code and its dual code are equivalent up to a multiplier permutation. Furthermore, if a code is isodual up to the multiplier permutation μ_e, then the code is said to be μ_e-isodual.*

A code is said to be E2-isodual if the code and its dual code are equivalent up to a scalar transformation. Furthermore, if a code is isodual up to the scalar transformation $\Lambda = (\lambda_0, \ldots, \lambda_{n-1})$, then the code is said to be Λ-isodual or $(\lambda_0, \ldots, \lambda_{n-1})$-isodual.

Firstly, we discuss the E1-isodual cyclic codes. The main method is analyzing the defining set of a cyclic code over the finite field $\mathbb{F}_q$. We show that if q is odd, no E1-isodual cyclic codes exist over $\mathbb{F}_q$. If q is even and the multiplier permutation μ_e is fixed, we give a construction for all the $[n, \frac{n}{2}]_q$ μ_e-isodual cyclic codes. We can then use this result to enumerate such codes. Since self-dual cyclic codes over a finite field are studied in Chapter 3 and self-dual cyclic codes are also isodual cyclic codes, we give a necessary and sufficient condition for the existence of E1-isodual cyclic codes that are not self-dual.

For the E2-isodual cyclic codes, we first give a necessary and sufficient condition on the scalar transformation for the image of a cyclic code to remain cyclic since in general, the image of an $[n, \frac{n}{2}]_q$ cyclic code under a scalar transformation is not necessarily cyclic again. As a consequence, we obtain a necessary and sufficient condition on the scalar transformation to make a cyclic code isodual. It is also shown that if $\sum_{i=0}^{n-1} \lambda_i \neq 0$, then the $(\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$-isodual cyclic codes are self-dual, which therefore implies q must be even. Therefore, if q is odd, then there is no $(\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$-isodual cyclic code of length n over $\mathbb{F}_q$ with $\sum_{i=0}^{n-1} \lambda_i \neq 0$.

To meet the necessary and sufficient condition on the scalar transformation to

make the image code cyclic again, we consider the $(1, \lambda, \lambda^2, \ldots, \lambda^{n-1})$-isodual cyclic codes, where $\lambda \in \mathbb{F}_q^*$. In order to exclude the self-dual cyclic codes from this class of codes, we set $\lambda \neq 1$ and $\sum_{i=0}^{n-1} \lambda_i = 0$, i.e., $\lambda \neq 1$ and the order r of λ divides n. By dealing with the factorization of $x^{\bar{n}} - 1$, we explicitly describe the generator polynomials of the $(1, \lambda, \lambda^2, \ldots, \lambda^{n-1})$-isodual cyclic codes. As a consequence, we show that when q is even, there always exists a $(1, \lambda, \lambda^2, \ldots, \lambda^{n-1})$-isodual cyclic code. When q is odd, there exists a $(1, \lambda, \lambda^2, \ldots, \lambda^{n-1})$-isodual cyclic code if and only if $\frac{n}{r}$ is odd, where r is the order of λ.

Since for any finite field $\mathbb{F}_q$ with q odd, we always have $-1 \in \mathbb{F}_q$ and $-1 \neq 1$. Therefore, it is natural to further discuss the $(1, \lambda, \lambda^2, \ldots, \lambda^{n-1})$-isodual cyclic codes by letting $\lambda = -1$. Besides a necessary and sufficient condition on the existence of $(1, -1, 1, \ldots, (-1)^{n-1})$-isodual cyclic codes, a construction of the generator polynomials of all such codes is given. Using this result, we enumerate them.

In Chapter 5, we study generalized cyclic codes. It is known that quasi-cyclic codes, constacyclic codes and quasi-twisted codes are all generalizations of cyclic codes. Since quasi-twisted (QT) codes over finite fields include cyclic codes, quasi-cyclic codes and constacyclic codes as special cases, we focus on QT codes. In particular, we investigate issues related to the decomposition and construction of a QT code. The important tool used is so-called generalized discrete Fourier transform.

By decomposing the ring $\mathbb{R}_{\theta,\lambda} := \frac{\mathbb{F}_q[x]}{(x^\theta - \lambda)}$ into a direct sum of coprime component rings, it is shown that a (λ, l)-QT code of length $l\theta$ over $\mathbb{F}_q$ can be decomposed into a direct sum of linear codes $\mathscr{C}_i$ of length l over these component rings.

The decomposition of the ring involves the factorization of the polynomial $x^\theta - \lambda$ over $\mathbb{F}_q$. If $\gcd(\theta, q) = 1$ (nonrepeated-root case), then the polynomial $x^\theta - \lambda$ is

factorized into a product of distinct irreducible polynomials. It is shown that if $\gcd(\theta, q) = p^a$ with $a \geq 1$ (repeated-root case), then all the irreducible factors of the polynomial $x^\theta - \lambda$ have multiplicity p^a. In this thesis, we allow $a \geq 0$ and then both cases are included. When $x^\theta - \lambda = (f_1(x))^{p^a}(f_2(x))^{p^a} \cdots (f_k(x))^{p^a}$, where $f_i(x)$'s are irreducible polynomials over $\mathbb{F}_q$, the ring $\mathbb{R}_{\theta,\lambda}$ is decomposed into a direct sum of the pairwise coprime component rings $\mathbb{R}_i := \frac{\mathbb{F}_q[x]}{\left((f_i(x))^{p^a}\right)}$, $1 \leq i \leq k$.

Since the dual code $\mathscr{C}^\perp$ of a (λ, l)-QT code $\mathscr{C}$ is a (λ^{-1}, l)-QT code, a natural question that then arises is: given the decomposition of $\mathscr{C}$, what is the decomposition of $\mathscr{C}^\perp$? When $\lambda = \pm 1$, $\mathscr{C}$ and $\mathscr{C}^\perp$ are modules over the same ring $\frac{\mathbb{F}_q[x]}{(x^\theta - \lambda)}$ and hence, only in this case, self-dual QT codes make sense. When $\lambda \neq \pm 1$, $\mathscr{C}$ and $\mathscr{C}^\perp$ are modules over different rings: $\mathbb{R}_{\theta,\lambda}$ and $\mathbb{R}_{\theta,\lambda^{-1}}$ respectively. Since the two rings are isomorphic by identifying $x \in \mathbb{R}_{\theta,\lambda}$ with $x^{-1} \in \mathbb{R}_{\theta,\lambda^{-1}}$, we map $\mathscr{C}^\perp$ into the module $\mathbb{R}^l_{\theta,\lambda}$ and get an isomorphic copy of $\mathscr{C}^\perp$ in module $\mathbb{R}^l_{\theta,\lambda^{-1}}$. Based on the dual defined over two modules over the same ring, the decomposition of the dual code over $\mathbb{R}_{\theta,\lambda^{-1}}$ is explicitly described. In particular, the decomposition of self-dual QT codes is given.

An important tool to study algebraic codes is the discrete Fourier transform (DFT). When $\gcd(\theta, p) = 1$, i.e., in the nonrepeated-root case, the classical DFT of $c(x) \in \frac{\mathbb{F}_q[x]}{(x^\theta - \lambda)}$ is defined to be a matrix

$$\hat{c} = [\hat{c}_0, \hat{c}_1, \ldots, \hat{c}_{\theta-1}],$$

where

$$\hat{c}_i = c(\beta\xi^i), \text{ for } 0 \leq i \leq \theta - 1,$$

β is a θ-th root of λ,

and ξ is a primitive θ-th root of unity.

It is well-known that the DFT is invertible. However, in the repeated-root case, the classical DFT is not applicable. Therefore, we adopt the Hasse derivatives to develop the generalized discrete Fourier transform (GDFT). We also give the inverse formula of the GDFT. The GDFT also gives an explicit connection between a QT code and its component codes. Therefore, by the inverse formula of the GDFT, we produce a formula to construct a QT code from linear codes over component rings. It is further shown that the computation can be done in the field $\mathbb{F}_q$ instead of the extension fields.

This thesis is organized as follows. Chapter 2 is an introduction to the key notions and notations. Then the duality of cyclic codes over finite fields is discussed in two chapters: self-dual cyclic codes over finite fields in Chapter 3 and isodual cyclic codes over finite fields in Chapter 4, respectively. Chapter 5 deals with QT codes.

Chapter 2

Preliminaries

In this chapter, we recall necessary definitions and properties concerning cyclic codes and some families of generalized cyclic codes over finite fields.

2.1 Cyclic codes over finite fields

Let $\mathbb{F}_q$ denote the finite field of $q = p^m$ elements where p is a prime, m a positive integer and let $\mathbb{F}_q^*$ denote $\mathbb{F}_q \setminus \{0\}$. Denote by $\mathbb{F}_q[x]$ the polynomial ring in indeterminate x with coefficients from $\mathbb{F}_q$.

Definition 2.1.1. *A* linear code $\mathscr{C}$ *of length n and dimension k over $\mathbb{F}_q$ is a k-dimensional subspace of the vector space $\mathbb{F}_q^n$ over $\mathbb{F}_q$. It is known as an $[n,k]_q$ code. The elements of the subspace are the* codewords *of $\mathscr{C}$ and written as row vectors: $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$.*

For a linear code, the following matrices are important.

Definition 2.1.2. *Let $\mathscr{C}$ be an $[n,k]_q$ linear code. A* generator matrix *of $\mathscr{C}$, denoted*

by G, is a $k \times n$ matrix over $\mathbb{F}_q$ such that the row vectors of G form a basis for $\mathscr{C}$. That is, for each $\mathbf{c} \in \mathscr{C}$, there is a unique $\mathbf{u} \in \mathbb{F}_q^k$ such that

$$\mathbf{c} = \mathbf{u}G$$

and all vectors of this form are codewords.

A parity check matrix *of $\mathscr{C}$, denoted by H, is an $(n-k) \times n$ matrix of row rank $n-k$ over $\mathbb{F}_q$ such that $\mathbf{c}$ is a codeword if and only if $H\mathbf{c}^T = 0$.*

Obviously, either a generator matrix or a parity check matrix can be used to construct a linear code.

Now we give the definition of dual codes as follows.

Definition 2.1.3. *The* dual *$\mathscr{C}^\perp$ of a linear code $\mathscr{C}$ is defined as the dual space of the vector space $\mathscr{C}$ with respect to the Euclidean inner product.*

Obviously, if a linear code $\mathscr{C}$ is an $[n,k]_q$ code, then its dual code $\mathscr{C}^\perp$ is an $[n,n-k]_q$ code. Furthermore, if a linear code $\mathscr{C}$ has parity check matrix H, then its dual code $\mathscr{C}^\perp$ has generator matrix H.

Definition 2.1.4. *A code $\mathscr{C}$ is* cyclic *if it is linear and if any cyclic shift of a codeword is also a codeword, i.e., whenever $(c_0, c_1, \ldots, c_{n-1})$ is in $\mathscr{C}$ then so is $(c_{n-1}, c_0, \ldots, c_{n-2})$.*

2.1.1 Generator polynomials and check polynomials

We associate with the vector $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ in $\mathbb{F}_q^n$ the polynomial $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$. Then a cyclic code of length n over $\mathbb{F}_q$ can be defined as an ideal in the ring of polynomials modulo $x^n - 1$ over $\mathbb{F}_q$. Under this correspondence, a cyclic code has the following properties.

Theorem 2.1.5. *[14, Theorem 1, p. 190] Let $\mathscr{C}$ be a nonzero ideal in $\frac{\mathbb{F}_q[x]}{(x^n-1)}$, i.e., a cyclic code of length n over $\mathbb{F}_q$.*

1. *There is a unique monic polynomial $G(x)$ of minimal degree in $\mathscr{C}$.*

2. *$\mathscr{C} =< G(x) >$, i.e., $G(x)$ is a generator polynomial of $\mathscr{C}$.*

3. *$G(x)$ divides $x^n - 1$.*

4. *Any $c(x) \in \mathscr{C}$ can be written uniquely as $c(x) = k(x)G(x)$ in $\mathbb{F}_q[x]$, where $k(x) \in \mathbb{F}_q[x]$ has degree $< n - \deg G(x)$. The dimension of $\mathscr{C}$ is $n - \deg G(x)$. Thus the message $k(x)$ becomes the codeword $k(x)G(x)$.*

5. *If $G(x) = G_0 + G_1x + \cdots + G_bx^b$, then a generator matrix of $\mathscr{C}$ is*

$$G = \begin{bmatrix} G_0 & G_1 & G_2 & \cdots & G_b & & 0 \\ & G_0 & G_1 & \cdots & G_{b-1} & G_b & \\ & & & \cdots & \cdots & & \\ 0 & & G_0 & \cdots & \cdots & & G_b \end{bmatrix}_{(n-b)\times n},$$

$$= \begin{bmatrix} G(x) & & & & \\ & xG(x) & & & \\ & & & \cdots & \\ & & & & x^{n-b-1}G(x) \end{bmatrix}.$$

using an obvious notation.

From the above theorem, for a cyclic code $\mathscr{C}$ of length n, the generator polynomial $G(x)$ divides $x^n - 1$. Then

$$\begin{aligned} H(x) &= (x^n - 1)/G(x) \\ &= \sum_{i=0}^{k} H_i x^i \text{ (say)}, \; H_k \neq 0, \end{aligned}$$

is called the check polynomial of $\mathscr{C}$. The reason for this name is that $H(x)$ can be used to compute a parity check matrix for $\mathscr{C}$:

$$H = \begin{bmatrix} & & & H_k & \cdots & H_2 & H_1 & H_0 \\ & & H_k & \cdots & H_2 & H_1 & H_0 & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ H_k & \cdots & & H_2 & H_1 & H_0 & & \end{bmatrix}.$$

Furthermore, the check polynomial $H(x)$ of $\mathscr{C}$ is related to the generator polynomial of $\mathscr{C}^\perp$ as follows. To simplify the notation, we give the following definition regarding polynomials.

Definition 2.1.6. *Let $f(x) = f_0 + f_1 x + \cdots + f_i x^i$ with $f_i \neq 0$ be a polynomial in $\mathbb{F}_q[x]$. Then the* reciprocal polynomial *of $f(x)$, denoted by $f^*(x)$, is*

$$\begin{aligned} f^*(x) &:= f_0^{-1} \overleftarrow{f}(x) \\ &= f_0^{-1} x^i f(x^{-1}) \\ &= f_0^{-1}(f_i + f_{i-1}x + \cdots + f_0 x^i). \end{aligned}$$

where $\overleftarrow{f}(x)$ is the polynomial obtained by reversing the order of the coefficients of $f(x)$. In particular, if $f(x) = f^*(x)$, then $f(x)$ is called self-reciprocal.

Note that $f^*(x) = f_0^{-1} x^i f(x^{-1})$ if $i = \deg(f(x))$.

Theorem 2.1.7. *[14, Theorem 4, p. 196] Let $\mathscr{C}$ be a cyclic code of length n with generator polynomial $G(x)$ and check polynomial $H(x) = (x^n - 1)/G(x)$. Then the dual code $\mathscr{C}^\perp$ is cyclic and has generator polynomial*

$$G^\perp(x) = H^*(x).$$

2.1.2 Defining set

Since the unique generator polynomial $G(x)$ of an $[n, k]_q$ cyclic code is a divisor of the polynomial $x^n - 1$, the generator polynomial as well as the corresponding cyclic code can be determined by the zeros of $G(x)$ which are zeros of $x^n - 1$. Write

$$n = p^a \bar{n},$$

where $\gcd(\bar{n}, p) = 1$ and $a \geq 0$. Then

$$x^n - 1 = (x^{\bar{n}} - 1)^{p^a}.$$

Let ξ be an $\bar{n}$-th primitive root of unity. Then all the zeros of $G(x)$ can be written as powers of ξ. Therefore, we define the *defining set* T of a cyclic code as a multiset whose elements are ordered pairs:

$$T = \{(i, m_i) | \xi^i \text{ is a zero of } G(x) \text{ with multiplicity } m_i, i = 0, \ldots, \bar{n} - 1\}. \tag{2.1}$$

By convention, when ξ^j is not a zero of $G(x)$ for some j, set $m_j = 0$. Then the defining set of a cyclic code is identified with the set of the zeros of the generator polynomial of the code. Therefore, a cyclic code can be determined by its defining set. Given the defining set T of the code $\mathscr{C}$, the defining set of its dual code $\mathscr{C}^\perp$, denoted by $T^\perp$ is

$$\{(-i, p^a - m_i) | (i, m_i) \in T, i = 0, \ldots, \bar{n} - 1\}.$$

To simplify the notations, we define the multiset $U = \{(i, p^a)|i = 0, \ldots, \bar{n} - 1\}$ as the universe which is identified with all the zeros of $x^n - 1$. Let $\overline{T}$ be the complement of T with respect to U, i.e.,

$$\overline{T} = \{(i, p^a - m_i)|(i, m_i) \in T, i = 0, \ldots, \bar{n} - 1\}.$$

For an integer j, we define jT as

$$jT = \{(ji, m_i)|(i, m_i) \in T, i = 0, \ldots, \bar{n} - 1\}.$$

Therefore, if the defining set of the cyclic code $\mathscr{C}$ is T, then the defining set of its dual code $\mathscr{C}^\perp$ is

$$T^\perp = -\overline{T}.$$

2.2 Some families of generalized cyclic codes over finite fields

In this section, we introduce constacyclic codes, quasi-cyclic codes and quasi-twisted codes over finite fields. These codes are all generalized from cyclic codes over finite fields.

Definition 2.2.1. *Let $\mathscr{C}$ be a linear code of length n over $\mathbb{F}_q$. Let $\lambda \in \mathbb{F}_q^*$. For each codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ in $\mathscr{C}$, if the vector $(\lambda c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathscr{C}$, then the code $\mathscr{C}$ is called a λ-constacyclic code and λ is called the constant of $\mathscr{C}$.*

By the correspondence between codewords and polynomials, a λ-constacyclic code can be defined as an ideal in $\mathbb{F}_q[x]/(x^n - \lambda)$.

Definition 2.2.2. *Let $\mathscr{C}$ be a linear code of length n over $\mathbb{F}_q$. For each codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ in $\mathscr{C}$, if the vector $\sigma^l(\mathbf{c}) = (c_{n-l}, c_{n-l+1} \ldots, c_{n-1}, c_0, \ldots, c_{n-l-1}) \in \mathscr{C}$ where the subscripts are taken modulo n and l is a positive integer, then the code $\mathscr{C}$ is called an l-quasi-cyclic (QC) code and l is called the index of $\mathscr{C}$.*

It is easy to check that an l-QC code of length n is also a $\gcd(l, n)$-QC code (see [1]). Without loss of generality, we therefore assume that the index l always divides the length n. Let $\theta = \frac{n}{l}$. Properly permuting the coordinates of a codeword $(c_0, c_1, \ldots, c_{n-1})$ in the l-QC code to the vector

$$\mathbf{c}' = (c_0, c_l \ldots, c_{(\theta-1)l}, c_1, c_{l+1}, \ldots, c_{(\theta-1)l+1}, \ldots, c_{l-1}, \ldots, c_{\theta l-1}),$$

we divide $\mathbf{c}'$ to l parts and each part consists of θ consecutive coordinates.

It is observed that each part can be regarded as a codeword in a cyclic code of length θ over $\mathbb{F}_q$. Therefore, representing each part of $\mathbf{c}'$ by a polynomial in $\mathbb{F}_q[x]/(x^\theta - 1)$, the codeword $\mathbf{c}$ is equivalent to the vector in $(\mathbb{F}_q[x]/(x^\theta - 1))^l$ up to a permutation:

$$(c_0 + c_l x + \cdots + c_{(\theta-1)l} x^{\theta-1}, c_1 + \cdots + c_{(\theta-1)l+1} x^{\theta-1}, \ldots, c_{l-1} + c_{2l-1} x + \cdots + c_{\theta l-1} x^{\theta-1}).$$

Then an l-QC code is equivalent to a submodule of $(\mathbb{F}_q[x]/(x^\theta - 1))^l$ over the ring $\mathbb{F}_q[x]/(x^\theta - 1)$.

Definition 2.2.3. *Let $\mathscr{C}$ be a linear code of length n over $\mathbb{F}_q$. Let $\lambda \in \mathbb{F}_q^*$ and let l be a positive integer. For each codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ in $\mathscr{C}$, if the vector*

$$(\lambda c_{n-l}, \lambda c_{n-l+1} \ldots, \lambda c_{n-1}, c_0, \ldots, c_{n-l-1}) \in \mathscr{C},$$

where the subscripts are taken modulo n, then the code $\mathscr{C}$ is called a (λ, l)-quasi-twisted (QT) code.

We define the following action $\mathscr{L}_{\lambda,l}$ on the vector space $\mathbb{F}_q^n$.

Definition 2.2.4. *Let $\mathscr{L}_{\lambda,l}$ be a map as*

$$\mathscr{L}_{\lambda,l} : \mathbb{F}_q^n \to \mathbb{F}_q^n(v_0, v_1, \ldots, v_{n-1}) \quad \mapsto (\lambda v_{n-l}, \lambda v_{n-l+1} \ldots, \lambda v_{n-1}, v_0, \ldots, v_{n-l-1}).$$

We call $\mathscr{L}_{\lambda,l}$ is l cyclic shifts with constant λ. In particular, when $\lambda = 1$, we call $\mathscr{L}_{1,l}$ is l cyclic shifts, and when $\lambda = l = 1$, we call $\mathscr{L}_{\lambda,l}$ is a cyclic shift.

A (λ, l)-QT code is invariant as a set under the action $\mathscr{L}_{\lambda,l}$.

It is easy to check that a (λ, l)-QT code of length n is also a $(\lambda, \gcd(l, n))$-QT code. Thus we always assume l divides n. Let $\theta = \frac{n}{l}$. When $\lambda = 1$, a (λ, l)-QT code is an l-QC code. When $l = 1$, a (λ, l)-QT code is a λ-constacyclic code. When $\lambda = l = 1$, a (λ, l)-QT code is a cyclic code. From the above discussion about constacyclic codes and QC codes, a (λ, l)-QT code of length n is a submodule of $(\mathbb{F}_q[x]/(x^\theta - \lambda))^l$ over the ring $\mathbb{F}_q[x]/(x^\theta - \lambda)$. For convenience, we use the same notation for both the code over $\mathbb{F}_q$ and its corresponding submodule of $(\mathbb{F}_q[x]/(x^\theta - \lambda))^l$ over the ring $\mathbb{F}_q[x]/(x^\theta - \lambda)$.

Chapter 3

Self-dual cyclic codes over finite fields

The main objects of study in this chapter are self-dual cyclic codes over finite fields. We investigate issues related to their existence, characterization and enumeration.

This chapter is organized as follows. The conditions for the existence of self-dual cyclic codes are given in Section 3.1. In Section 3.2 , we give a characterization of the generator polynomials of self-dual cyclic codes, which is then used in Section 3.3 for the enumeration formula. Section 3.4 deals with the asymptotic occurrence problem explained above. A summary and a brief discussion of open problems conclude the chapter in Section 3.5.

3.1 Existence of self-dual cyclic codes

By Theorem 2.1.7, we immediately get the following proposition.

Proposition 3.1.1. *A cyclic code $\mathscr{C}$ of length n is self-dual if and only if*

$$G(x) = H^*(x),$$

where $G(x)$ is the generator polynomial of $\mathscr{C}$, $H(x)$ is the check polynomial and $H^*(x)$ is the reciprocal polynomial of $H(x)$.

Clearly, self-dual codes of odd lengths over $\mathbb{F}_q$ do not exist. It is natural to ask for the conditions required of q and the length n in order for $[n, \frac{n}{2}]_q$ self-dual cyclic codes to exist. The following result provides an answer to this question.

Theorem 3.1.2. *There exists at least one self-dual cyclic code of length n over $\mathbb{F}_q$ if and only if q is a power of 2 and n is even.*

Proof. Suppose that $\mathscr{C}$ is a self-dual cyclic code of length n over $\mathbb{F}_q$. Then n must be even and $\deg G = \deg H = \frac{n}{2}$. As $G(x)H(x) = x^n - 1$, we have $G_0H_0 = -1$, where G_0 and H_0 are the constant terms of $G(x)$ and $H(x)$, respectively. Therefore,

$$\begin{aligned} & & G(x^{-1})H(x^{-1}) &= x^{-n} - 1, \\ &\Rightarrow\quad & (G_0G^*(x))(H_0H^*(x)) &= 1 - x^n, \\ &\Rightarrow & G^*(x)H^*(x) &= x^n - 1. \end{aligned} \tag{3.1}$$

By Proposition 3.1.1, we have

$$\begin{aligned} & G(x) &= H^*(x), \\ \Rightarrow\quad & \overleftarrow{G}(x) &= H_0^{-1}H(x), \\ \Rightarrow\quad & G_0G^*(x) &= H_0^{-1}H(x), \\ \Rightarrow\quad & G^*(x) &= -H(x). \end{aligned} \tag{3.2}$$

Therefore, we have $G^*(x)H^*(x) = -H(x)G(x) = -(x^n - 1)$. Then by (3.1) and (3.2), we have

$$x^n - 1 = -(x^n - 1).$$

Hence, the following identity holds:

$$2(x^n - 1) = 0,$$

which implies that the characteristic of the field $\mathbb{F}_q$ is 2, i.e., q is a power of 2.

Conversely, if q is a power of 2 and n is even, then the polynomial $x^n - 1$ can be written as follows over $\mathbb{F}_q$:

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

By Proposition 3.1.1, it is easy to check that the cyclic code with generator polynomial $x^{\frac{n}{2}} + 1$ is self-dual. □

Theorem 3.1.2 gives a necessary and sufficient condition for the existence of self-dual cyclic codes.

The final part of the proof of Theorem 3.1.2 reveals the existence of the self-dual cyclic code with generator polynomial $x^{\frac{n}{2}} + 1$ whenever n and q are even. This leads us to introduce the following definition.

Definition 3.1.3. *For n even, the $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic code $\mathscr{C}$ with generator polynomial $x^{\frac{n}{2}} + 1$ is called the* trivial self-dual cyclic code*, denoted by $\bar{\mathscr{C}}[n]_{2^m}$, or simply $\bar{\mathscr{C}}$ without specifying the length n and the field $\mathbb{F}_{2^m}$ if no confusion arises.*

Throughout the rest of this chapter, in view of Theorem 3.1.2, we assume that the integer n is even and $q = 2^m$ for some positive integer m.

3.2 Generator polynomials of $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic codes

Each cyclic code over $\mathbb{F}_{2^m}$ is uniquely determined by its generator polynomial, a monic divisor of $x^n + 1$ over $\mathbb{F}_{2^m}$. In order to describe the generator polynomials of $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic codes, we need to know the factorization of the polynomial $x^n + 1$ over $\mathbb{F}_{2^m}$. Write

$$n = 2^{\nu(n)}\bar{n}, \tag{3.3}$$

where $\bar{n}$ is an odd integer and $\nu(n)$ is a positive integer depending on n. Then

$$x^n + 1 = (x^{\bar{n}} + 1)^{2^{\nu(n)}}.$$

For any irreducible polynomial dividing $x^{\bar{n}} + 1$ over $\mathbb{F}_{2^m}$, its reciprocal polynomial also divides $x^{\bar{n}} + 1$ over $\mathbb{F}_{2^m}$ and is also irreducible over $\mathbb{F}_{2^m}$. Since $\gcd(\bar{n}, 2^m) = 1$, the polynomial $x^{\overline{n}} + 1$ can be factorized into distinct irreducible polynomials as follows [10, p. 2753]:

$$x^{\bar{n}} + 1 = f_1(x) \cdots f_s(x) h_1(x) h_1^*(x) \cdots h_t(x) h_t^*(x), \tag{3.4}$$

where $f_i(x)$ $(1 \leq i \leq s)$ are monic irreducible self-reciprocal polynomials over $\mathbb{F}_{2^m}$ while $h_j(x)$ and its reciprocal polynomial $h_j^*(x)$ $(1 \leq j \leq t)$ are both monic irreducible polynomials over $\mathbb{F}_{2^m}$. We say that $h_j(x)$ and $h_j^*(x)$ form a *reciprocal polynomial pair*. Note that s and t both depend on n and m. Therefore, we regard them as two functions of the pair (n, m).

Definition 3.2.1. *Let n be an even positive integer and let m be a positive integer. Define $s(n, m)$ to be the number of self-reciprocal polynomials in the factorization*

of $x^{\bar{n}}+1$ *over* $\mathbb{F}_{2^m}$*, and* $t(n,m)$ *the number of reciprocal polynomial pairs in the factorization of* $x^{\bar{n}}+1$ *over* $\mathbb{F}_{2^m}$*, where* $\bar{n}$ *is defined as in* (3.3)*.*

Therefore,

$$x^n+1 = f_1(x)^{2^{\nu(n)}}\cdots f_{s(n,m)}(x)^{2^{\nu(n)}} h_1(x)^{2^{\nu(n)}} h_1^*(x)^{2^{\nu(n)}}\cdots h_{t(n,m)}(x)^{2^{\nu(n)}} h_{t(n,m)}^*(x)^{2^{\nu(n)}}. \tag{3.5}$$

We can describe the generator polynomials for the $[n,\frac{n}{2}]_{2^m}$ self-dual cyclic codes as soon as we know the factorization of x^n+1 over $\mathbb{F}_{2^m}$.

Theorem 3.2.2. *Let* x^n+1 *be factorized as in* (3.5)*. A cyclic code* $\mathscr{C}$ *of length* n *is self-dual over* $\mathbb{F}_{2^m}$ *if and only if its generator polynomial is of the form*

$$f_1(x)^{2^{\nu(n)-1}}\cdots f_s(x)^{2^{\nu(n)-1}} h_1(x)^{\beta_1} h_1^*(x)^{2^{\nu(n)}-\beta_1}\cdots h_t(x)^{\beta_t} h_t^*(x)^{2^{\nu(n)}-\beta_t}, \tag{3.6}$$

where $s=s(n,m)$*,* $t=t(n,m)$ *and* $0\le\beta_i\le 2^{\nu(n)}$ *for each* $1\le i\le t$*.*

Proof. Let $\mathscr{C}$ be a cyclic code of length n over $\mathbb{F}_{2^m}$ and let $G(x)$ be its generator polynomial. We need to show that $\mathscr{C}$ is self-dual if and only if $G(x)$ is of the form as in (3.6).

To simplify the notation in the proof, let ν, s and t be $\nu(n), s(n,m)$ and $t(n,m)$, respectively. Since the generator polynomial $G(x)$ of a cyclic code of length n is monic and divides x^n+1, we may assume that

$$G(x) = f_1(x)^{\alpha_1}\cdots f_s(x)^{\alpha_s} h_1(x)^{\beta_1} h_1^*(x)^{\gamma_1}\cdots h_t(x)^{\beta_t} h_t^*(x)^{\gamma_t},$$

where $0\le\alpha_i\le 2^\nu$ for each $1\le i\le s$, and $0\le\beta_j,\gamma_j\le 2^\nu$ for each $1\le j\le t$.

Then the check polynomial is

$$H(x) = f_1(x)^{2^\nu-\alpha_1}\cdots f_s(x)^{2^\nu-\alpha_s} h_1(x)^{2^\nu-\beta_1} h_1^*(x)^{2^\nu-\gamma_1}\cdots h_t(x)^{2^\nu-\beta_t} h_t^*(x)^{2^\nu-\gamma_t}.$$

Hence

$$H^*(x) = f_1(x)^{2^\nu-\alpha_1} \cdots f_s(x)^{2^\nu-\alpha_s} h_1^*(x)^{2^\nu-\beta_1} h_1(x)^{2^\nu-\gamma_1} \cdots h_t^*(x)^{2^\nu-\beta_t} h_t(x)^{2^\nu-\gamma_t},$$

since $f_i(x)$ $(1 \leq i \leq s)$ are self-reciprocal while $h_j(x)$ and $h_j^*(x)$ $(1 \leq j \leq t)$ are reciprocal polynomial pairs over $\mathbb{F}_{2^m}$.

By Proposition 3.1.1, $\mathscr{C}$ is self-dual if and only if $G(x) = H^*(x)$, i.e.,

$$\begin{cases} \alpha_i = 2^\nu - \alpha_i, & \text{for each } 1 \leq i \leq s \\ \gamma_j = 2^\nu - \beta_j, & \text{for each } 1 \leq j \leq t, \end{cases}$$

or, equivalently,

$$\begin{cases} \alpha_i = 2^{\nu-1}, & \text{for each } 1 \leq i \leq s \\ \gamma_j = 2^\nu - \beta_j, & \text{for each } 1 \leq j \leq t. \end{cases}$$

Therefore, $\mathscr{C}$ is self-dual if and only if its generator polynomial $G(x)$ is of the form as in (3.6). □

From the above discussion, it is clear that in order to construct the generator polynomial of an $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic code, we just need to determine the exponents associated with the irreducible factors of x^n+1 over $\mathbb{F}_{2^m}$. Theorem 3.2.2 says that the exponents of the irreducible self-reciprocal polynomials in the factorization should be $2^{\nu(n)-1}$ while the exponents of each reciprocal polynomial pair should sum up to $2^{\nu(n)}$ without other restrictions. Therefore, the number of distinct $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic codes is exactly the number of choices of the exponents of the reciprocal pairs, i.e., the number of choices of β_j's for $1 \leq j \leq t(n, m)$. Thus we immediately have the following corollary.

Corollary 3.2.3. *Let $x^n + 1$ be factorized over $\mathbb{F}_{2^m}$ as in* (3.5)*. Then the number of $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic codes is exactly $(2^{\nu(n)} + 1)^{t(n,m)}$. In particular, if $t(n, m) = 0$, i.e., all monic irreducible factors of $x^{\bar{n}} + 1$ are self-reciprocal, then there is a unique $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic code.*

Example 3.2.4. Consider the case: $n = 14$ and $q = 2$. Now $\bar{n} = 7$. The factorization of $x^{14} + 1$ over $\mathbb{F}_2$ is

$$x^{14} + 1 = (x + 1)^2(x^3 + x + 1)^2(x^3 + x^2 + 1)^2.$$

It is observed that the polynomial $x + 1$ is a self-reciprocal polynomial and $x^3 + x + 1$ is the reciprocal polynomial of $x^3 + x^2 + 1$ over $\mathbb{F}_2$. There are 3 binary self-dual cyclic codes of length 14 with the following generator polynomials respectively:

$$\begin{aligned} (x + 1)(x^3 + x + 1)^2 &= x^7 + x^6 + x^3 + x^2 + x + 1, \\ (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1) &= x^7 + 1, \\ (x + 1)(x^3 + x^2 + 1)^2 &= x^7 + x^6 + x^5 + x^4 + x + 1. \end{aligned}$$

The one with generator polynomial $x^7 + 1$ is the trivial self-dual cyclic code.

Table 3.1 lists all binary self-dual cyclic codes of lengths up to 46. In the table, only the coefficients of the generator polynomials are listed in ascending order. For example, $1^4 0^2 1^2$ in the column labeled by $G(x)$ means that the generator polynomial is $1 + x + x^2 + x^3 + x^6 + x^7$. The column labeled by 'No.' gives the values of $(2^{\nu(n)} + 1)^{t(n,1)}$. For example, there are 3 self-dual cyclic codes of length 14 over $\mathbb{F}_2$.

Table 3.2 lists all self-dual cyclic codes of lengths up to 28 over $\mathbb{F}_4$. In Table 3.2, w is a primitive element in $\mathbb{F}_4$ with $w^2 + w + 1 = 0$. The coordinates of the vector in the column labeled by $G(x)$ are the coefficients of the generator polynomial in ascending

Table 3.1: Self-Dual Cyclic Codes over $\mathbb{F}_2$ of Lengths up to 46

n	$\bar{n}$	No.	$G(x)$	n	$\bar{n}$	No.	$G(x)$
2	1	1	1^2	30	15	3	$1^2 0^1 1^4 0^3 1^1 0^2 1^3$
4	1	1	$1^1 0^1 1^1$				$1^1 0^{14} 1^1$
6	3	1	$1^1 0^2 1^1$				$1^3 0^2 1^1 0^3 1^4 0^1 1^2$
8	1	1	$1^1 0^3 1^1$	32	1	1	$1^1 0^{15} 1^1$
10	5	1	$1^1 0^4 1^1$	34	17	1	$1^1 0^{16} 1^1$
12	3	1	$1^1 0^5 1^1$	36	9	1	$1^1 0^{17} 1^1$
14	7	3	$1^4 0^2 1^2$	38	19	1	$1^1 0^{18} 1^1$
			$1^1 0^6 1^1$	40	5	1	$1^1 0^{19} 1^1$
			$1^2 0^2 1^4$	42	21	9	$1^1 0^2 1^1 0^8 1^1 0^2 1^1 0^2 1^1 0^2 1^1$
16	1	1	$1^1 0^7 1^1$				$1^4 0^2 1^1 0^1 1^3 0^2 1^1 0^1 1^3 0^2 1^2$
18	9	1	$1^1 0^8 1^1$				$1^1 0^1 1^4 0^1 1^2 0^1 1^2 0^1 1^1 0^2 1^1 0^1 1^2 0^1 1^1$
20	5	1	$1^1 0^9 1^1$				$1^2 0^1 1^1 0^1 1^3 0^1 1^1 0^4 1^4 0^1 1^3$
22	11	1	$1^1 0^{10} 1^1$				$1^1 0^{20} 1^1$
24	3	1	$1^1 0^{11} 1^1$				$1^3 0^1 1^4 0^4 1^1 0^1 1^3 0^1 1^1 0^1 1^2$
26	13	1	$1^1 0^{12} 1^1$				$1^1 0^1 1^2 0^1 1^1 0^2 1^1 0^1 1^2 0^1 1^2 0^1 1^4 0^1 1^1$
28	7	5	$1^1 0^1 1^1 0^1 1^1 0^1 1^1 0^5 1^1 0^1 1^1$				$1^2 0^2 1^3 0^1 1^1 0^2 1^3 0^1 1^1 0^2 1^4$
			$1^4 0^2 1^1 0^1 1^3 0^2 1^2$				$1^1 0^2 1^1 0^2 1^1 0^2 1^1 0^8 1^1 0^2 1^1$
			$1^1 0^{13} 1^1$	44	11	1	$1^1 0^{21} 1^1$
			$1^2 0^2 1^3 0^1 1^1 0^2 1^4$	46	23	3	$1^4 0^6 1^6 0^2 1^2 0^2 1^2$
			$1^1 0^1 1^1 0^5 1^1 0^1 1^1 0^1 1^1 0^1 1^1$				$1^1 0^{22} 1^1$
							$1^2 0^2 1^2 0^2 1^6 0^6 1^4$

order. For example, $[w, w, 1, 1]$ means the generator polynomial is $w + wx + x^2 + x^3$. The column labeled by 'No.' gives the values of $(2^{\nu(n)} + 1)^{t(n,1)}$. For example, there are 3 self-dual cyclic codes of length 6 over $\mathbb{F}_4$.

Table 3.2: Self-Dual Cyclic Codes over $\mathbb{F}_4$ of Length up to 28

n	$\bar{n}$	No.	$G(x)$
2	1	1	$[1, 1]$
4	1	1	$[1, 0, 1]$
6	3	3	$[w^2, w^2, 1, 1]$, $[1, 0, 0, 1]$, $[w, w, 1, 1]$
8	1	1	$[1, 0, 0, 0, 1]$
10	5	1	$[1, 0, 0, 0, 0, 1]$
12	3	5	$[w, 0, w, 0, 1, 0, 1]$, $[w^2, w^2, 1, w, w^2, 1, 1]$, $[1, 0, 0, 0, 0, 0, 1]$
			$[w, w, 1, w^2, w, 1, 1]$, $[w^2, 0, w^2, 0, 1, 0, 1]$
14	7	3	$[1, 1, 1, 1, 0, 0, 1, 1]$, $[1, 0, 0, 0, 0, 0, 0, 0, 1]$, $[1, 1, 0, 0, 1, 1, 1, 1]$
16	1	1	$[1, 0, 0, 0, 0, 0, 0, 0, 0, 1]$
18	9	9	$[w, w, w^2, w^2, 0, 0, w^2, w^2, 1, 1]$, $[w^2, w^2, 1, w, w^2, 1, w, w^2, 1, 1]$, $[1, 1, w, w, 0, 0, w^2, w^2, 1, 1]$
			$[w^2, 0, 0, w^2, 0, 0, 1, 0, 0, 1]$, $[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1]$, $[w, 0, 0, w, 0, 0, 1, 0, 0, 1]$
			$[1, 1, w^2, w^2, 0, 0, w, w, 1, 1]$, $[w, w, 1, w^2, w, 1, w^2, w, 1, 1]$, $[w^2, w^2, w, w, 0, 0, w, w, 1, 1]$
20	5	1	$[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1]$
22	11	3	$[1, 1, w, w, 1, 1, 1, 1, w^2, w^2, 1, 1]$, $[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1]$, $[1, 1, w^2, w^2, 1, 1, 1, 1, w, w, 1, 1]$
24	3	9	$[w^2, 0, 0, 0, w^2, 0, 0, 0, 1, 0, 0, 0, 1]$, $[1, 1, w^2, w, 0, w, 1, w^2, 0, w^2, w, 1, 1]$
			$[w, 0, w, 0, 1, 0, w^2, 0, w, 0, 1, 0, 1]$, $[w^2, w^2, 1, w, w^2, 1, w, w^2, 1, w, w^2, 1, 1]$
			$[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1]$, $[w, w, 1, w^2, w, 1, w^2, w, 1, w^2, w, 1, 1]$
			$[w^2, 0, w^2, 0, 1, 0, w, 0, w^2, 0, 1, 0, 1]$, $[1, 1, w, w^2, 0, w^2, 1, w, 0, w, w^2, 1, 1]$
			$[w, 0, 0, 0, w, 0, 0, 0, 1, 0, 0, 0, 1]$
26	13	1	$[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1]$
28	7	5	$[1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1]$, $[1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1]$
			$[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1]$, $[1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1]$
			$[1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1]$

3.3 Enumeration of self-dual cyclic codes

Recall that $n = 2^{\nu(n)}\bar{n}$, $q = 2^m$ and $t(n,m)$ is the number of irreducible reciprocal polynomial pairs in the factorization of $x^{\bar{n}}+1$ over $\mathbb{F}_{2^m}$. In order to know the number of distinct $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic codes, by Corollary 3.2.3, we need to know the values of $\nu(n)$ and $t(n,m)$. For given n and q, it is easy to compute the value of $\nu(n)$. However, it is hard to obtain a general formula for the value of $t(n,m)$.

In this section, we fix n and m. Now, we briefly state some well-known facts regarding the factorization of $x^{\bar{n}}+1$ over $\mathbb{F}_{2^m}$. For further details, [8] can be referred to. We adopt the same definitions and notations as in [8]. Let $\overline{\mathbb{F}}$ be the algebraic closure of $\mathbb{F}_{2^m}$. Thus $\overline{\mathbb{F}}$ contains all the $\bar{n}$ roots of $x^{\bar{n}}+1$.

It is well known that

$$x^{\bar{n}}+1 = \prod_{j|\bar{n}} Q_j(x),$$

where $Q_j(x)$ is the jth *cyclotomic polynomial* over $\mathbb{F}_{2^m}$, i.e., the polynomial whose roots in $\overline{\mathbb{F}}$ are all of order j. Notice that $Q_j(x)$ is in $\mathbb{F}_{2^m}[x]$. In order to describe the factorization of $Q_j(x)$, we need the following definitions.

Definition 3.3.1. *Let i and j be any two positive integers with* $\gcd(i,j) = 1$. *The* order *of i in the multiplicative group $(\mathbb{Z}/j\mathbb{Z})^*$, denoted by* $\mathrm{ord}_j(i)$, *is defined to be the smallest integer k such that j divides $i^k - 1$.*

Definition 3.3.2. *Let j be an odd positive integer and m positive integer. We say the pair (j,m) is* good *if j divides $(2^m)^k + 1$ for some integer $k \geq 0$ and* bad *otherwise.*

Definition 3.3.3. *Let χ be a function defined on the pair (j,m), with j odd, as*

follows:

$$\chi(j,m) = \begin{cases} 0, & \textit{if } (j,m) \textit{ is good,} \\ 1, & \textit{otherwise.} \end{cases}$$

With the help of the above definitions and notations, we have the following lemma.

Lemma 3.3.4. *Let j be an odd positive integer. The jth cyclotomic polynomial $Q_j(x)$ factors into $\frac{\phi(j)}{\mathrm{ord}_j(2^m)}$ distinct monic irreducible polynomials over $\mathbb{F}_{2^m}$ of the same degree $\mathrm{ord}_j(2^m)$, where ϕ is the Euler function.*

Moreover, if (j,m) is good, then all the irreducible polynomials in the factorization of $Q_j(x)$ are self-reciprocal. Otherwise, all of them form reciprocal polynomial pairs.

Proof. The first part is just Theorem 2.47 in [8, p. 65]. Hence we only show the second part.

Let $f(x)$ be any irreducible polynomial of degree d in the factorization of $Q_j(x)$ over $\mathbb{F}_{2^m}$, where d is the same as in the statement of the lemma. Then its reciprocal polynomial $f^*(x)$ is also irreducible and of degree d. Let ξ be any root of $f(x)$ in $\overline{\mathbb{F}}$. By the definition of cyclotomic polynomials, the order of ξ in $\overline{\mathbb{F}}$ is j. Moreover, the set

$$\{\xi^{2^{mi}} \ : \ 0 \le i \le d-1\}$$

comprises all distinct roots of $f(x)$. Notice that even if $i > d-1$, $\xi^{2^{mi}}$ is also a root of $f(x)$. Here, we restrict i between 0 and $d-1$ so that the elements in the set are distinct.

Suppose that the pair (j,m) is good, i.e., $j \mid (2^m)^k + 1$ for some $k \ge 0$. Then $\xi^{(2^m)^k+1} = 1$ since j is the order of ξ. Therefore, we have $\xi^{-1} = \xi^{(2^m)^k}$. This means that ξ^{-1} is a root of $f(x)$, too. Since ξ^{-1} is also a root of $f^*(x)$, all the $\frac{\phi(j)}{\mathrm{ord}_j(2^m)}$ roots

of $f(x)$ are the $\frac{\phi(j)}{\mathrm{ord}_j(2^m)}$ roots of $f^*(x)$. Therefore, we have $f(x) = f^*(x)$, i.e., all the irreducible polynomials in the factorization of $Q_j(x)$ are self-reciprocal.

Next, suppose that the pair (j, m) is bad. Then ξ^{-1} is a root of $f^*(x)$ but not a root of $f(x)$. Otherwise, we can express ξ^{-1} as $\xi^{-1} = \xi^{(2^m)^k}$ for some $k \geq 0$, which implies (j, m) is good, contradicting the assumption. Therefore the polynomial $f(x)$ is not equal to its reciprocal polynomial $f^*(x)$. Since the roots of $f(x)$ and $f^*(x)$ have the same order j, $f^*(x)$ is an irreducible polynomial in the factorization of $Q_j(x)$ and different from $f(x)$. It follows that, if (j, m) is bad, all the irreducible polynomials in the factorization of $Q_j(x)$ form reciprocal polynomial pairs. □

By Lemma 3.3.4, if the pair (j, m) is good, then $Q_j(x)$ contributes nothing to the number of reciprocal pairs $t(n, m)$ in the factorization of $x^{\bar{n}} + 1$ over $\mathbb{F}_{2^m}$. Otherwise, $Q_j(x)$ contributes $\frac{\phi(j)}{2\mathrm{ord}_j(2^m)}$ reciprocal polynomial pairs to $t(n, m)$. Hence, we get the following theorem.

Theorem 3.3.5. *Assume that $n = 2^{\nu(n)}\bar{n}$ and $x^n + 1$ is factorized as in (3.5). Then the number of reciprocal polynomial pairs $t(n, m)$ is*

$$t(n, m) = \frac{1}{2} \sum_{j|\bar{n}} \chi(j, m)\phi(j)/\mathrm{ord}_j(2^m),$$

and the number of $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic codes is

$$(1 + 2^{\nu(n)})^{\frac{1}{2}\sum_{j|\bar{n}} \chi(j,m)\phi(j)/\mathrm{ord}_j(2^m)}.$$

In particular, if and only if the pair $(\bar{n}, m)$ is good, $t(n, m) = 0$ and there is only the trivial self-dual cyclic code $\bar{\mathscr{C}}[n]_{2^m}$, i.e., the $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic code with generator polynomial $x^{\frac{n}{2}} + 1$.

Proof. The first part is immediately deduced from Lemma 3.3.4 and the second part is from Corollary 3.2.3. Hence we only show the third part. Suppose that $(\bar{n}, m)$ is good. Then $\bar{n}$ divides $(2^m)^k + 1$ for some integer $k \geq 0$. Therefore, for any $j \mid \bar{n}$, the integer j also divides $(2^m)^k + 1$ for the same k. Thus, the pair (j, m) is good and $\chi(j, m) = 0$ for each $j \mid \bar{n}$. By the first part of this theorem, we have $t(n, m) = 0$. □

Tables 3.3 and 3.4 list the numbers of self-dual cyclic codes over $\mathbb{F}_2$ and $\mathbb{F}_4$ for lengths up to 200, respectively.

By Theorem 3.3.5, the function χ is therefore very important to the enumeration of self-dual cyclic codes. Hence, we focus next on the study of the behavior of the function χ.

Definition 3.3.6. *Let $i \geq 0$ and $j \geq 1$ be integers. We say 2^i* exactly divides *j, denoted by $2^i \parallel j$, when 2^i divides j but 2^{i+1} does not divide j.*

Definition 3.3.7. *For each $r \geq 0$, let S_r^m be defined as $S_r^m := \{p : p$ is an odd prime and $2^r \parallel \mathrm{ord}_p(2^m)\}$.*

With the help of the above definitions, we characterize the good pairs (j, m) with j an odd prime. A necessary and sufficient condition is given in [18, Theorem 1]. The following theorem follows immediately from [18, Theorem 1] when $a = 2^m$ and $b = 1$.

Theorem 3.3.8. *Let j be an odd positive integer and m a positive integer. Then $\chi(j, m) = 0$ if and only if there exists $r \geq 1$ such that $p \in S_r^m$ for every prime p dividing j. In particular, for an odd prime p, then $\chi(p, m) = 0$ if and only if $p \in S_r^m$ for some $r \geq 1$, i.e., $\mathrm{ord}_p(2^m)$ is even.*

Table 3.3: The Number of Self-Dual Cyclic Codes over $\mathbb{F}_2$ of Fixed Lengths up to 200

n	$\bar{n}$	$(2^{\nu(n)}+1)^{t(n,1)}$	n	$\bar{n}$	$(2^{\nu(n)}+1)^{t(n,1)}$	n	$\bar{n}$	$(2^{\nu(n)}+1)^{t(n,1)}$
46	23	3	98	49	9	150	75	9
48	3	1	100	25	1	152	19	1
50	25	1	102	51	9	154	77	9
52	13	1	104	13	1	156	39	5
54	27	1	106	53	1	158	79	3
56	7	9	108	27	1	160	5	1
58	29	1	110	55	3	162	81	1
60	15	5	112	7	17	164	41	1
62	31	27	114	57	1	166	83	1
64	1	1	116	29	1	168	21	81
66	33	1	118	59	1	170	85	81
68	17	1	120	15	9	172	43	1
70	35	9	122	61	1	174	87	3
72	9	1	124	31	125	176	11	1
74	37	1	126	63	243	178	89	81
76	19	1	128	1	1	180	45	25
78	39	3	130	65	1	182	91	81
80	5	1	132	33	1	184	23	9
82	41	1	134	67	1	186	93	729
84	21	25	136	17	1	188	47	5
86	43	1	138	69	9	190	95	3
88	11	1	140	35	25	192	3	1
90	45	9	142	71	3	194	97	1
92	23	5	144	9	1	196	49	25
94	47	3	146	73	81	198	99	1
96	3	1	148	37	1	200	25	1

Table 3.4: The Number of Self-Dual Cyclic Codes over $\mathbb{F}_4$ of Fixed Lengths up to 200

n	$\bar{n}$	$(2^{\nu(n)}+1)^{t(n,2)}$	n	$\bar{n}$	$(2^{\nu(n)}+1)^{t(n,2)}$	n	$\bar{n}$	$(2^{\nu(n)}+1)^{t(n,2)}$
32	1	1	90	45	729	146	73	81
34	17	1	92	23	5	148	37	1
36	9	25	94	47	3	150	75	243
38	19	3	96	3	33	152	19	9
40	5	1	98	49	9	154	77	81
42	21	81	100	25	1	156	39	125
44	11	5	102	51	243	158	79	3
46	23	3	104	13	1	160	5	1
48	3	17	106	53	1	162	81	81
50	25	1	108	27	125	164	41	1
52	13	1	110	55	27	166	83	3
54	27	27	112	7	17	168	21	6561
56	7	9	114	57	81	170	85	6561
58	29	1	116	29	1	172	43	125
60	15	125	118	59	3	174	87	27
62	31	27	120	15	729	176	11	17
64	1	1	122	61	1	178	89	81
66	33	81	124	31	125	180	45	15625
68	17	1	126	63	177147	182	91	2187
70	35	27	128	1	1	184	23	9
72	9	81	130	65	1	186	93	59049
74	37	1	132	33	625	188	47	5
76	19	5	134	67	3	190	95	27
78	39	27	136	17	1	192	3	65
80	5	1	138	69	81	194	97	1
82	41	1	140	35	125	196	49	25
84	21	625	142	71	3	198	99	2187
86	43	27	144	9	289	200	25	1
88	11	9						

By Theorem 3.3.8, if $p \in S_0^m$, then $\chi(p, m) = 1$. Moreover, we have

$$\chi(p^i, m) = \chi(p, m),$$

where p is a prime and i is a positive integer.

Generally, for every prime p, there exists $r_p \geq 0$, dependent on p, such that $p \in S_{r_p}^m$. We have $\chi(j, m) = 0$ if and only if these r_p's are all equal and positive for each prime p dividing j. Thus, by Theorem 3.3.8, we can determine the value of $\chi(j, m)$ as soon as we know the value of r_p for each prime factor p of j. Given any m, the following proposition characterizes the r_p's for all odd primes p except for those congruent to 1 modulo 8.

Proposition 3.3.9. *Let p be an odd prime.*

1. *Let $p \equiv 3 \pmod 8$.*
   (a) *If m is odd, then $p \in S_1^m$ and $\chi(p, m) = 0$.*
   (b) *If m is even, then $p \in S_0^m$ and $\chi(p, m) = 1$.*
2. *Let $p \equiv 5 \pmod 8$.*
   (a) *If m is odd, then $p \in S_2^m$ and $\chi(p, m) = 0$.*
   (b) *If $m \equiv 2 \pmod 4$, then $p \in S_1^m$ and $\chi(p, m) = 0$.*
   (c) *If $m \equiv 0 \pmod 4$, then $p \in S_0^m$ and $\chi(p, m) = 1$.*
3. *Let $p \equiv 7 \pmod 8$. Then $p \in S_0^m$ and $\chi(p, m) = 1$.*

Proof. For each case, we only show the value of r such that $p \in S_r^m$. Then the value of $\chi(p, m)$ follows immediately by Theorem 3.3.8. In this proof, we mainly use Euler's

criterion:

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p},$$

where p is an odd prime. Therefore, we have

$$2^{\frac{p-1}{2}} \equiv \begin{cases} -1 \pmod{p}, & \text{if } p \equiv 3, 5 \pmod{8}, \\ 1 \pmod{p}, & \text{if } p \equiv 7 \pmod{8}. \end{cases} \tag{3.7}$$

1. Case 1a: Let $p \equiv 3 \pmod{8}$ and let m be odd. By (3.7), we have

   $$2^{m\frac{p-1}{2}} \equiv (-1)^m \equiv -1 \pmod{p}.$$

   From this, we find that $\mathrm{ord}_p(2^m)$ divides $p-1$ but not $\frac{p-1}{2}$. Since $2 \parallel p-1$, we have $2 \parallel \mathrm{ord}_p(2^m)$. Therefore, we have $p \in S_1^m$.

2. Case 1b: Let $p \equiv 3 \pmod{8}$ and let m be even. By (3.7), we have

   $$2^{m\frac{p-1}{2}} \equiv (-1)^m \equiv 1 \pmod{p}.$$

   Then $\mathrm{ord}_p(2^m)$ divides $\frac{p-1}{2}$. Since $\frac{p-1}{2}$ is odd, by Theorem 3.3.8, we have $p \in S_0^m$.

3. Case 2a: Let $p \equiv 5 \pmod{8}$ and let m be odd. By (3.7), we have

   $$2^{m\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

   From this congruence, we find that $\mathrm{ord}_p(2^m)$ divides $p-1$ but not $\frac{p-1}{2}$. Since $4 \parallel p-1$, we have $4 \parallel \mathrm{ord}_p(2^m)$. Therefore, we have $p \in S_2^m$.

4. Case 2b: Let $p \equiv 5 \pmod{8}$ and $m \equiv 2 \pmod{4}$. By (3.7), we have $2^{\frac{p-1}{2}\frac{m}{2}} \equiv -1 \pmod{p}$ because $\frac{m}{2}$ is odd. Hence we have $(2^m)^{\frac{p-1}{4}} \equiv -1 \pmod{p}$. Therefore, $\mathrm{ord}_p(2^m)$ divides $\frac{p-1}{2}$ but not $\frac{p-1}{4}$. Since $2 \parallel \frac{p-1}{2}$, we have $2 \parallel \mathrm{ord}_p(2^m)$. Hence, we have $p \in S_1^m$.

5. Case 2c: Let $p \equiv 5 \pmod 8$ and $m \equiv 0 \pmod 4$. We have

$$2^{m\frac{p-1}{4}} \equiv 1 \pmod p,$$

for $\frac{m}{2}$ is even. Then $\mathrm{ord}_p(2^m)$ divides $\frac{p-1}{4}$. Since $\frac{p-1}{4}$ is odd, we have $p \in S_0^m$.

6. Case 3: Let $p \equiv 7 \pmod 8$. By (3.7), we have

$$2^{m\frac{p-1}{2}} \equiv 1^m \equiv 1 \pmod p,$$

for any m. Then $\mathrm{ord}_p(2^m)$ divides $\frac{p-1}{2}$. Since $\frac{p-1}{2}$ is odd, we have $p \in S_0^m$.

□

Proposition 3.3.9 covers the cases for odd primes $p \equiv 3, 5, \text{or } 7 \pmod 8$. For these cases, it is easy to determine the value of $\chi(p, m)$ for any given m.

The values of $\chi(p, m)$ for primes $p \equiv 1 \pmod 8$ and $m = 1$ are determined in [18, Theorem 6]. We quote the result here without proof.

Proposition 3.3.10. *Let p be a prime satisfying $p \equiv 1 \pmod 8$ and let $2^r \parallel (p-1)$.*

1. *If $r = 3$ and p is represented by the quadratic form $A^2 + 64(A + 2B)^2$ with variables A and B, then $p \in S_0^1$.*

2. *If $r = 3$ and p is represented by the quadratic form $A^2 + 256B^2$ with variables A and B, then $p \in S_1^1$.*

3. *If $r \geq 4$ and p is represented by the quadratic form $A^2 + 64(A + 2B)^2$ with variables A and B, then $p \in S_{r-2}^1$.*

4. *If p is represented by the quadratic form $A^2 + 16(A + 2B)^2$ with variables A and B, then $p \in S_{r-1}^1$.*

It is stated in [18] that when $m = 1$, i.e. in the binary case, the smallest odd prime that is not covered by the cases in Propositions 3.3.9 and 3.3.10 is 337 and the density of the primes not covered is 1/32.

By Proposition 3.3.9, since the sets $S_{r_p}^m$'s are given, it is easy to determine the value of $\chi(j, m)$ for any odd positive integer j with no prime factor congruent to 1 modulo 8. Therefore, we obtain the following theorem from Theorem 3.3.8 and Proposition 3.3.9.

Theorem 3.3.11. *Let j be an odd positive integer with no prime factor congruent to 1 modulo 8.*

1. *Let m be odd. Then $\chi(j, m) = 0$ if and only if all the prime factors of j are congruent to 3 modulo 8 or all of them are congruent to 5 modulo 8.*

2. *Let $m \equiv 2 \pmod 4$. Then $\chi(j, m) = 0$ if and only if all the prime factors of j are congruent to 5 modulo 8.*

3. *Let $m \equiv 0 \pmod 4$. Then $\chi(j, m) = 1$.*

From Theorems 3.3.5 and 3.3.11, we immediately derive the following corollary.

Corollary 3.3.12. *Let $n = 2^{\nu(n)}\bar{n}$ as in (3.3). Suppose that $\bar{n}$ has no prime factor congruent to 1 modulo 8.*

1. *Let m be odd. Then there is exactly one $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic code if and only if all the prime factors of $\bar{n}$ are congruent to 3 modulo 8 or all of them are congruent to 5 modulo 8.*

2. *Let $m \equiv 2 \pmod 4$. Then there is exactly one $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic code if and only if all the prime factors of $\bar{n}$ are congruent to 5 modulo 8.*

3. *Let $m \equiv 0 \pmod 4$. Then there are always at least two $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic codes.*

3.4 Distribution of n with a unique $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic code

Recall that the trivial self-dual cyclic code $\bar{\mathscr{C}}[n]_{2^m}$ is the $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic code with generator polynomial $x^{\frac{n}{2}} + 1$. In the proof of Theorem 3.1.2, we know that, when n is even, the trivial self-dual cyclic code always exists. From Theorem 3.3.5, we know that, given an even length n and the field $\mathbb{F}_{2^m}$, exactly one of the following two cases happens:

1. If $\chi(\bar{n}, m) = 0$, then there is a unique $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic code, i.e., the trivial self-dual cyclic code $\bar{\mathscr{C}}[n]_{2^m}$.

2. If $\chi(\bar{n}, m) = 1$, then there is at least another $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic code besides the trivial self-dual cyclic code $\bar{\mathscr{C}}[n]_{2^m}$.

We define the first case as the *unique case* and the second one as the *nonunique case*. For a given field $\mathbb{F}_{2^m}$, we next discuss the distribution of the unique case as n varies.

Definition 3.4.1. *Let $S^m(y)$ be the number of unique cases with $\bar{n}$ not exceeding y.*

We give an asymptotic formula for $S^m(y)$ for a given m.

The following theorem, quoted from [18, Theorems 2 and 5] without proof here, is a more general result concerning the function $S^m(y)$.

Theorem 3.4.2. *Let a and b be two coprime positive integers. Let S denote the set of integers $j > 1$ such that j divides $a^i + b^i$ for some $i \geq 1$. Let $S(y)$ be the number of elements in S not exceeding y. Then, for an integer $N > 1$, there exist positive constants $d_1, \cdots, d_N$ such that*

$$S(y) = \frac{y}{\log y}(d_1 \log^{\delta_1} y + d_2 \log^{\delta_2} y + \ldots + d_N \log^{\delta_N} y + O(\log^{\delta_{N+1}} y)),$$

where the constants $d_1, \cdots, d_N$ and $\delta_1, \cdots, \delta_{N+1}$ depend on a and b. Furthermore, the constants $\delta_1, \cdots, \delta_{N+1}$ are given as follows.

Put $\psi = a/b$. Let k' be the largest number such that $\psi = v^{2^{k'}}$, where v is a rational number. If $v = 2v_1^2$ with rational v_1 and $k' = 0$, then

$$\delta_i = \begin{cases} \frac{7}{24}, & \text{if } i = 1 \text{ or } 2, \\ \frac{8}{24}, & \text{if } i = 3, \\ \frac{1}{24} \cdot \frac{1}{2^{i-4}}, & \text{if } i \geq 4. \end{cases} \tag{3.8}$$

If $v = 2v_1^2$ with rational v_1 and $k' = 1$, then

$$\delta_i = \begin{cases} \frac{7}{12}, & \text{if } i = 1, \\ \frac{8}{24}, & \text{if } i = 2, \\ \frac{1}{24} \cdot \frac{1}{2^{i-3}}, & \text{if } i \geq 3. \end{cases} \tag{3.9}$$

If $v = 2v_1^2$ with rational v_1 and $k' \geq 2$, then

$$\delta_i = \begin{cases} 1 - \frac{1}{3} \cdot \frac{1}{2^{k'}}, & \text{if } i = 1, \\ \frac{1}{3} \cdot \frac{1}{2^{k'+i-1}}, & \text{if } i \geq 2. \end{cases} \tag{3.10}$$

We apply the above theorem to our case.

Theorem 3.4.3. *Let m be a positive integer and let k be the integer such that $2^k \parallel m$. Then, for an integer $N > 1$, there exist positive constants $d_1, \cdots, d_N$ such that*

$$S^m(y) = \frac{y}{log\ y}(d_1 log^{\delta_1} y + d_2 log^{\delta_2} y + \ldots + d_N log^{\delta_N} y + O(log^{\delta_{N+1}} y)),$$

where the constants $d_1, \cdots, d_N$ *and* $\delta_1, \cdots, \delta_{N+1}$ *depend on* m. *Furthermore, the constants* $\delta_1, \cdots, \delta_{N+1}$ *are given as in Theorem 3.4.2: if* $k = 0$, *then they are given in* (3.8); *if* $k = 1$, *then they are given in* (3.9); *if* $k \geq 2$, *then they are given in* (3.10).

Proof. This theorem is just an application of Theorem 3.4.2 with $a = 2^m$ and $b = 1$. The function $S^m(y)$ here is just the function $S(y)$ in Theorem 3.4.2.

Suppose that k' is the largest integer such that

$$2^m = v^{2^{k'}}, \tag{3.11}$$

with rational $v = \frac{w_1}{w_2}$, where $\gcd(w_1, w_2) = 1$. Now it remains to show that k' defined here is just the integer k in the statement of this theorem, and v can be expressed as $2v_1^2$ with rational v_1. Then the result immediately follows from Theorem 3.4.2. From (3.11), we have

$$2^m w_2^{2^{k'}} = w_1^{2^{k'}}.$$

Then 2^m divides $w_1^{2^{k'}}$ and hence 2 divides w_1. Since $\gcd(w_1, w_2) = 1$, w_2 is not divisible by 2. Put $w_1 = 2^i w_1'$ with w_1' odd. Then

$$2^m w_2^{2^{k'}} = 2^{2^{k'} i} (w_1')^{2^{k'}}.$$

Comparing the powers of the prime 2 on both sides, we have the following identities

$$m = 2^{k'} i,$$

$$w_2 = w_1'.$$

Since $\gcd(w_1', w_2) = 1$ for $\gcd(w_1, w_2) = 1$, we have $w_1' = w_2 = 1$ and thus $v = w_1 = 2^i$. By (3.11), the following holds:

$$2^m = (2^i)^{2^{k'}} = 2^{2^{k'} i}.$$

We claim that the integer i is odd, for otherwise, we can write $2^m = (2^{\frac{i}{2}})^{2^{k'+1}}$, contradicting the maximality of k'. Therefore, the integer k defined in this theorem is the same as the integer k' defined in Theorem 3.4.2. Let $v_1 = 2^{\frac{i-1}{2}}$ for i is odd. Then $v = 2(v_1)^2$. This completes the proof. □

This theorem implies that, for any fixed m, as $\bar{n}$ grows, $\chi(\bar{n}, m) = 1$ for almost all $\bar{n}$. It means that the non-unique case, i.e., the case where there are at least two $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic codes, occurs more frequently over the fixed field $\mathbb{F}_{2^m}$ as n runs over all positive even integers.

3.5 Conclusion and open problems

In this chapter, we have given a necessary and sufficient condition for the existence of self-dual cyclic codes of length n over $\mathbb{F}_q$, namely, n is even and $q = 2^m$ with m a positive integer. Given n and m, a formula to enumerate $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic codes has been provided. Furthermore, when n has no prime factor congruent to 1 modulo 8, precise necessary and sufficient conditions in terms of the prime factors of n have been given for the nonexistence of $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic codes other than the one with generator polynomial $x^{\frac{n}{2}} + 1$. Over a fixed finite field $\mathbb{F}_{2^m}$, we also demonstrated that, as the length n grows, the cases where there exist two or more $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic codes occur more frequently (than the cases where there is a unique $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic code). Part of the results in this chapter was also obtained in [7].

In this chapter, we have restricted our investigations to the finite field case. Self-dual cyclic codes over finite rings are also interesting and worth a study. The necessary and sufficient condition for the existence of such codes can be expected to be different

from the finite field case. For instance, the length-1 code $\{0, 2\}$ is a self-dual cyclic code over $\mathbb{Z}_4$, but the length is not even. Other possible generalizations include the use of dualities obtained through other inner products, such as the Hermitian inner product.

Another interesting open problem is to extend Proposition 3.3.9 to cover the primes congruent to 1 modulo 8 (for which only some results in the binary case, i.e., $m = 1$, are known). With such an extension, the constraints on n in Corollary 3.3.12 can then be removed. In other words, given any n and m, one can directly determine whether there is a unique $[n, \frac{n}{2}]_{2^m}$ self-dual cyclic code by simply looking at the prime factors of n.

Apart from the problems mentioned above, there could be many other interesting problems associated with self-dual cyclic codes. For instance, one can ask for which n and even $q > 2$ there exist q-ary "Type II" self-dual cyclic codes of length n ([22]). Note that there are no binary "Type II" self-dual cyclic codes (see [25, Corollary 2]).

Chapter 4

Isodual cyclic codes over finite fields

Definition 4.0.1. *If a linear code $\mathscr{C}$ is equivalent to its dual code $\mathscr{C}^{\perp}$, then $\mathscr{C}$ is called an* isodual *code.*

Recall that equivalence of codes is defined as in Definition 1.0.1, E1-equivalence is defined as in Definitions 1.0.3 and 1.0.4, and E2-equivalence is defined as in Definitions 1.0.2 and 1.0.4.

The main objects of study in this chapter are E1-isodual cyclic codes and E2-isodual cyclic codes.

Since two equivalent codes share the same dimension, an isodual code $\mathscr{C}$ over $\mathbb{F}_q$ must be an $[n, \frac{n}{2}]_q$ code. Therefore, the length n of an isodual code must be even.

Throughout this chapter, the length n of a code is always assumed to be even.

This chapter is organized as follows. The E1-isodual cyclic codes are discussed in Section 4.1. In Section 4.2, the E2-isodual cyclic codes are discussed. A particular

class of $(1, \lambda, \ldots, \lambda^{n-1})$-isodual cyclic codes is considered in Section 4.3 and the case when $\lambda = -1$ is considered separately in Section 4.4. Section 4.5 concludes the chapter.

4.1 E1-isodual cyclic codes

In this section, we discuss E1-isodual cyclic codes which are not self-dual. Throughout this section, let $\mathscr{C}$ be an $[n,k]_q$ cyclic code with generator polynomial $G(x)$ and defining set T. Write $n = p^a\bar{n}$ with $\gcd(p,\bar{n}) = 1$. Let μ_e be a multiplier permutation defined as in Definition 1.0.3.

In the following, we study the criteria for a cyclic code $\mathscr{C}$ to be μ_e-isodual.

Lemma 4.1.1. *Let $\mathscr{C}$ be an $[n,k]_q$ cyclic code with generator polynomial $G(x)$ and defining set T. Let e be an integer coprime to n and let μ_e be a multiplier permutation defined as in Definition 1.0.3. Then $\mu_e(\mathscr{C})$ is an $[n,k]_q$ cyclic code with generator polynomial $G'(x) = \gcd(G(x^{e^{-1}}), x^n - 1)$, where e^{-1} is the inverse of e in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$ and* gcd *is the monic greatest common divisor. Moreover, the defining set T' of $\mu_e(\mathscr{C})$ is eT.*

Proof. Let $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mu_e(\mathscr{C})$ and let $\mathscr{L}_{1,1}$ be the cyclic shift as in Definition 2.2.4. Since

$$\mathscr{L}_{1,1}(\mathbf{c}) = (c_{n-1}, c_0, c_1, \ldots, c_{n-2}),$$

and

$$\mu_e(\mathbf{c}) = (c_0, c_e, c_{2e}, \ldots, c_{(n-1)e}),$$

we have

$$(\mathscr{L}_{1,1}(\mathbf{c}))_i = c_{i-1},$$

$$(\mu_e(\mathbf{c}))_i = c_{ie},$$

for all $i \in \mathbb{Z}_n$, where $(\mathscr{L}_{1,1}(\mathbf{c}))_i$ and $(\mu_e(\mathbf{c}))_i$ are the i-th coordinates (indexed from 0 to $n-1$) of the vector $\mathscr{L}_{1,1}(\mathbf{c})$ and the vector $\mu_e(\mathbf{c})$, respectively. Now it easily verifies that

$$\mathscr{L}_{1,1}\mu_e = \mu_e\mathscr{L}_{1,1}^e,$$

from which it is immediate that the image code $\mu_e(\mathscr{C})$ is invariant as a set under the cyclic shift $\mathscr{L}_{1,1}$. Since μ_e is also $\mathbb{F}_q$-linear and invertible, the image code $\mu_e(\mathscr{C})$ is also linear, of the same dimension as $\mathscr{C}$. Then, identifying vectors $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ and polynomials $\sum_{i=0}^{n-1} c_i x^i$, we have that

$$(\mu_e(\mathbf{c}))(x) = c(x^{e^{-1}}),$$

where e^{-1} is the inverse in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$. Therefore, we see immediately that eT is the set of zeros of $\mu_e(\mathscr{C})$. Finally, let $G(x)$ be the generator polynomial of $\mathscr{C}$. Then the set of zeros of the polynomial $G'(x) = \gcd(G(x^{e^{-1}}), x^n - 1)$ is eT. Therefore, $G'(x)$ generates $\mu_e(\mathscr{C})$. □

Lemma 4.1.1 says that for any $[n,k]_q$ cyclic code $\mathscr{C}$ and any integer e with $\gcd(e,n) = 1$, the code $\mu_e(\mathscr{C})$ is always cyclic and the defining set is eT, where T is the defining set of $\mathscr{C}$. Since any cyclic code can be uniquely determined by its defining set and the defining set of the dual code $\mathscr{C}^\perp$ is $-\overline{T}$, the following lemma immediately follows.

Lemma 4.1.2. *Let $\mathscr{C}$ be an $[n, \frac{n}{2}]_q$ cyclic code with defining set T. Let e be an integer coprime to n and let μ_e be a multiplier permutation defined as in Definition 1.0.3. Then the cyclic code $\mathscr{C}$ is μ_e-isodual if and only if $\overline{T} = -eT$.*

This lemma gives a necessary and sufficient condition for a cyclic code to be μ_e-isodual. However, the following theorem tells us this condition is never satisfied for any μ_e when q is odd.

Theorem 4.1.3. *If q is odd, then there exists no E1-isodual cyclic code over $\mathbb{F}_q$.*

Proof. We prove the theorem by contradiction. Assume that $\mathscr{C}$ is an $[n, \frac{n}{2}]_q$ μ_e-isodual cyclic code with defining set T. Then there is a special element $(0, m_0) \in T$ with $0 \leq m_0 \leq p^a$. Then $(0, m_0) \in -eT$ for any e and $(0, p^a - m_0) \in \overline{T}$. Then $-eT = \overline{T}$ implies $2m_0 = p^a$ and hence $p = 2$, contradicting the assumption that q is odd. □

By Theorem 4.1.3, *throughout the rest of this section, we set $q = 2^m$, i.e., $p = 2$.* Since self-duality is a special case of isoduality, there exists at least one E1-isodual cyclic code of length n over $\mathbb{F}_q$ if q is even and n is even (see Theorem 3.1.2). Next we focus on the existence of $[n, \frac{n}{2}]_q$ E1-isodual cyclic codes that are not self-dual.

For our purpose, assume that the length of the code n, the finite field $\mathbb{F}_q = \mathbb{F}_{2^m}$ and the multiplier e are fixed.

Definition 4.1.4. *The operation of multiplying by q divides the integers modulo $\bar{n}$ into sets. These sets are called the q-cyclotomic cosets modulo $\bar{n}$, or simply cyclotomic cosets. The q-cyclotomic coset modulo $\bar{n}$ containing z is $\{z, zq, zq^2, \ldots, zq^{d-1}\}$ where d is the smallest integer such that $zq^d \equiv z \pmod{\bar{n}}$.*

Suppose that there are s q-cyclotomic cosets modulo $\bar{n}$:

$$C_{z_i} = \{z_i, z_i q, z_i q^2, \ldots, z_i q^{d_i - 1}\}, \text{ for } i = 1, 2, \ldots, s,$$

where z_i are the representatives of these cosets and d_i is the smallest positive integer such that $z_i q^{d_i} \equiv z_i \pmod{\bar{n}}$, respectively. Then $-ez_i, 1 \leq i \leq s$, are also the representatives for s cyclotomic cosets, respectively, because e is coprime to n. Therefore, the action of $-e$ on the representatives z_i's can be regarded as a permutation of the cyclotomic cosets, denoted by π_{-e}. Then denote the cyclotomic coset C_{-ez_i} by $C_{z_{\pi_{-e}(i)}}$. Therefore, π_{-e} can also be regarded as a permutation of the subscripts of the representatives $\{1, 2, \ldots, s\}$. We shall express the necessary and sufficient condition in Lemma 4.1.2 in further details in the following lemma, which can be used to construct all the μ_e-isodual cyclic codes (including self-dual cyclic codes) of length n over $\mathbb{F}_q$ by describing their defining sets. In the lemma, we regard a defining set as a union of q-cyclotomic cosets C_{z_i}'s with their multiplicities m_i's, respectively, because $(z_i, m_i) \in T$ implies that $(qz_i, m_i) \in T$. We write T in the following form:

$$T = m_1 C_{z_1} \bigcup m_2 C_{z_2} \bigcup \cdots \bigcup m_s C_{z_s}, \tag{4.1}$$

where C_{z_i} is the q-cyclotomic coset containing z_i and $m_i \geq 0$ is the multiplicity of z_i in T.

Lemma 4.1.5. *Let $\mathscr{C}$ be an $[n, \frac{n}{2}]_{2^m}$ cyclic code with defining set T as in* (4.1)*. Let e be an integer coprime to n and let π_{-e} be the permutation of the subscripts of the representatives $\{1, 2, \ldots, s\}$ such that $C_{-ez_i} = C_{z_{\pi_{-e}(i)}}$. Then $\mu_e(\mathscr{C}) = \mathscr{C}^{\perp}$ if and only if*

$$m_{\pi_{-e}(i)} + m_i = 2^a, \text{ for each } 1 \leq i \leq s, \tag{4.2}$$

where m_i's are as in (4.1).

Proof. Since

$$T = m_1 C_{z_1} \bigcup m_2 C_{z_2} \bigcup \cdots \bigcup m_s C_{z_s},$$

where C_{z_i} is the 2^m-cyclotomic coset containing z_i and $m_i \geq 0$ is the multiplicity of z_i in T, we have

$$\begin{aligned}\overline{T} =&(2^a - m_1)C_{z_1} \bigcup (2^a - m_2)C_{z_2} \bigcup \cdots \bigcup (2^a - m_s)C_{z_s} \\ =&(2^a - m_{\pi_{-e}(1)})C_{z_{\pi_{-e}(1)}} \bigcup (2^a - m_{\pi_{-e}(2)})C_{z_{\pi_{-e}(2)}} \bigcup \cdots \bigcup (2^a - m_{\pi_{-e}(s)})C_{z_{\pi_{-e}(s)}},\end{aligned}$$

and

$$\begin{aligned}-eT &= m_1 C_{-ez_1} \bigcup m_2 C_{-ez_2} \bigcup \cdots \bigcup m_s C_{-ez_s} \\ &= m_1 C_{z_{\pi_{-e}(1)}} \bigcup m_2 C_{z_{\pi_{-e}(2)}} \bigcup \cdots \bigcup m_s C_{z_{\pi_{-e}(s)}}.\end{aligned}$$

By Lemma 4.1.2, we get the necessary and sufficient condition (4.2). □

Lemma 4.1.5 also gives a necessary and sufficient condition to determine whether a given cyclic code is μ_e-isodual. Note that Lemma 4.1.1 and Lemma 4.1.5 are similar but in different expressions. If e is fixed, then by Lemma 4.1.5, a μ_e-isodual cyclic code can be determined by the values of m_i's in its defining set. Notice that, given any μ_e, $m_i = 2^{a-1}$, for $1 \leq i \leq s$, always satisfy Equation (4.2), which gives the trivial self-dual cyclic code with generator polynomial $x^{\frac{n}{2}} - 1$.

Since π_{-e} is a permutation of $\{1, \ldots, s\}$, π_{-e} can be expressed by its cycle decomposition. Suppose that there are θ disjoint cycles in the cycle decomposition of π_{-e}, say O_1, O_2,...,O_θ. For each cycle O_i, we can choose a representative, say w_i. Then the other elements in O_i are $\pi_{-e}(w_i), \pi_{-e}^2(w_i), \ldots, \pi_{-e}^{|O_i|-1}(w_i)$, where $|O_i|$ is the

cardinality of O_i. Then Equation (4.2) can be written as

$$m_{\pi_{-e}^{\alpha_i}(w_i)} + m_{\pi_{-e}^{\alpha_i+1}(w_i)} = 2^a, \text{ for } 0 \leq \alpha_i \leq |O_i| - 1 \text{ and } 1 \leq i \leq \theta, \tag{4.3}$$

where $\pi_{-e}^0(w_i) = \pi_{-e}^{|O_i|}(w_i) = w_i$. Therefore, we have the following corollary about the enumeration of $[n, \frac{n}{2}]_{2^m}$ μ_e-isodual cyclic codes.

Corollary 4.1.6. *Let n be an even positive integer and let $q = 2^m$. Write $n = 2^a\bar{n}$ with $\bar{n}$ odd. Suppose that there are s q-cyclotomic cosets modulo $\bar{n}$, say C_{z_i}, $1 \leq i \leq s$. Let e be an integer coprime to n and let π_{-e} be the permutation defined as above. Then the number of $[n, \frac{n}{2}]_q$ μ_e-isodual cyclic codes is*

$$(2^a + 1)^\sigma, \tag{4.4}$$

where σ is the number of the cycles of even length in the cycle decomposition of π_{-e}.

Proof. Since the defining set can completely determine the cyclic code, the number of $[n, \frac{n}{2}]_q$ μ_e-isodual cyclic codes is the number of solutions to Equation (4.3). Assume that $m_{w_i} = d$ for some d with $0 \leq d \leq 2^a$. Then by Equation (4.2),

$$m_{\pi_{-e}^{\alpha}(w_i)} = \begin{cases} d, & \text{if } \alpha \text{ is even,} \\ 2^a - d, & \text{if } \alpha \text{ is odd.} \end{cases}$$

Therefore, if $|O_i|$ is odd, we have $m_{\pi_{-e}^{|O_i|}(w_i)} = 2^a - d$, and if $|O_i|$ is even, we have $m_{\pi_{-e}^{|O_i|}(w_i)} = d$. On the other hand, we have $\pi_{-e}^{|O_i|}(w_i) = w_i$. Therefore, if $|O_i|$ is odd, we have $d = 2^{a-1}$, and if $|O_i|$ is even, there is no restriction on d. Therefore, the number of isodual cyclic codes depends on the number of the cycles of even length and hence we get (4.4). □

In particular if $e = 1$, then $\mu_e = \mu_1$ is the identity permutation map, which is an automorphism of a cyclic code. Suppose there are r self-reciprocal polynomials and t reciprocal pairs in the factorization of $x^n - 1$ (see [10]). Then there are $r + t$ cycles in the cycle decomposition of π_{-1}: r cycles of length 1 whose elements are the cyclotomic cosets corresponding to the r self-reciprocal polynomials, respectively, and t cycles of length 2 whose elements are the cyclotomic cosets of the t reciprocal pairs, respectively. By the above corollary, there are $(2^a + 1)^t$ μ_1-isodual cyclic codes. Since μ_1 is an automorphism of a cyclic code $\mathscr{C}$, the fact that $\mathscr{C}$ is μ_1-isodual implies that $\mathscr{C}$ is self-dual. Therefore, there are $(2^a + 1)^t$ self-dual cyclic codes, which is consistent with the enumeration given in Chapter 3.

Moreover, the proof of Corollary 4.1.6 gives a construction of isodual cyclic codes by determining the values of m_i's. The following example explains Lemma 4.1.5 and Corollary 4.1.6: when n, q and μ_e are fixed, we find all the $[n, \frac{n}{2}]_q$ μ_e-isodual cyclic codes.

Example 4.1.7. Let $q = 4$, $n = 30$ and $\omega \in \mathbb{F}_q$ where $\omega^2 + \omega + 1 = 0$. Then $\bar{n} = 15$ and $p^a = 2$. The following table lists all the 4-cyclotomic cosets modulo 15 and their corresponding irreducible factors of $x^{15} - 1$.

$g_1(x) = x + 1$	$C_{z_1} = C_0 = \{0\}$
$g_2(x) = x^2 + x + \omega$	$C_{z_2} = C_1 = \{1, 4\}$
$g_3(x) = x^2 + x + \omega^2$	$C_{z_3} = C_2 = \{2, 8\}$
$g_4(x) = x^2 + \omega^2 x + 1$	$C_{z_4} = C_3 = \{3, 12\}$
$g_5(x) = x + \omega$	$C_{z_5} = C_5 = \{5\}$
$g_6(x) = x^2 + \omega x + 1$	$C_{z_6} = C_6 = \{6, 9\}$
$g_7(x) = x^2 + \omega x + \omega$	$C_{z_7} = C_7 = \{7, 13\}$
$g_8(x) = x + \omega^2$	$C_{z_8} = C_{10} = \{10\}$
$g_9(x) = x^2 + \omega^2 x + \omega^2$	$C_{z_9} = C_{11} = \{11, 14\}$

If $e = 13$, then

$$C_{-ez_1} = C_0 = C_{z_1},$$

$$C_{-ez_2} = C_2 = C_{z_3},$$

$$C_{-ez_3} = C_1 = C_{z_2},$$

$$C_{-ez_4} = C_6 = C_{z_6},$$

$$C_{-ez_5} = C_{10} = C_{z_8},$$

$$C_{-ez_6} = C_3 = C_{z_4},$$

$$C_{-ez_7} = C_{11} = C_{z_9},$$

$$C_{-ez_8} = C_5 = C_{z_5},$$

$$C_{-ez_9} = C_7 = C_{z_7},$$

Then the permutation π_{-e} of indices $\{1, 2, 3, \ldots, 8, 9\}$ of the coset representatives is

decomposed into the following cycle decomposition

$$(1)(2\ 3)(4\ 6)(5\ 8)(7\ 9).$$

Let $\mathscr{C}$ be a $[30, 15]_4$ μ_{13}-isodual cyclic code. Suppose that the defining set T of $\mathscr{C}$ is

$$T = m_1 C_{z_1} \cup m_2 C_{z_2} \cdots \cup m_9 C_{z_9},$$

where $m_1, m_2, \ldots, m_9$ are nonnegative integers not larger than 2. By Lemma 4.1.5, we have

$$\begin{cases} m_1 + m_1 & = 2, \\ m_2 + m_3 & = 2, \\ m_4 + m_6 & = 2, \\ m_5 + m_8 & = 2, \\ m_7 + m_9 & = 2. \end{cases}$$

Therefore, we have 81 solutions:

$$\begin{cases} m_1 = 1, \\ m_2 = i_1, \\ m_3 = 2 - i_1, \\ m_4 = i_2, \\ m_5 = i_3, \\ m_6 = 2 - i_2, \\ m_7 = i_4, \\ m_8 = 2 - i_3, \\ m_9 = 2 - i_4, \end{cases}$$

where i_1, i_2, i_3, i_4 are integers 0, 1 or 2, and they are independent. Therefore, there are 81 $[30, 15]_4$ μ_{13}-isodual cyclic codes. Their corresponding generator polynomials are

$$g_1(x)g_2(x)^{i_1}g_3(x)^{2-i_1}g_4(x)^{i_2}g_5(x)^{i_3}g_6(x)^{2-i_2}g_7(x)^{i_4}g_8(x)^{2-i_3}g_9(x)^{2-i_4}.$$

In particular, when $i_2 = 1$ and $i_1 = i_4$, the corresponding codes are self-dual cyclic codes.

In order to exclude self-dual cyclic codes from μ_e-isodual cyclic codes, we focus on the lengths of the cycles in the decompositions of π_{-e} first. The following two propositions discuss about the properties of the cycles in the decompositions of π_{-e}.

Proposition 4.1.8. *Let e and n be integers and $\gcd(e, n) = 1$ and let π_{-e} be a*

permutation of the q-cyclotomic cosets modulo $\bar{n}$. Then in the same cycle in the decomposition of π_{-e}, the zeros corresponding to all the cosets are of the same order.

Proof. Let O be any cycle in the decomposition of π_{-e} whose first coset is C_{z_i}. Assume that the zeros corresponding to C_{z_i} are of order j. Then j is the order of z_i in the additive group $\mathbb{Z}/\bar{n}\mathbb{Z}$, i.e., $jz_i \equiv 0 \pmod{\bar{n}}$. By the definition of π_{-e}, any coset in the cycle O can be written as $C_{(-e)^k z_i}$, for some integer $k \geq 0$. Since $\gcd(e, n) = 1$ implies $\gcd(-e, \bar{n}) = 1$, the order of $(-e)^k z_i$ in the additive group $\mathbb{Z}/\bar{n}\mathbb{Z}$ is j, too. Then the zeros corresponding to the coset $C_{(-e)^k z_i}$ are of order j. Therefore, the statement is true. □

By the above lemma, it makes sense if we define the *order of the zeros corresponding to the cycle* as the order of the zeros corresponding to any coset in the cycle.

Proposition 4.1.9. *Let e and n be integers and $\gcd(e, n) = 1$ and let π_{-e} be a permutation of the q-cyclotomic cosets modulo $\bar{n}$. If the zeros corresponding to two cycles in the decomposition of π_{-e} are of the same order, then the lengths of the two cycles are same. Therefore, for an integer $j|\bar{n}$, all cyclotomic cosets corresponding to the j-th cyclotomic polynomial $Q_j(x)$ is union of cycles of the same length.*

Proof. Let O_1 and O_2 be two cycles of the same order j, whose first cyclotomic cosets are C_{z_1} and C_{z_2}, respectively. Then z_i can be written as

$$z_i = \frac{\bar{n}}{j} N_i,$$

where $i = 1, 2$ and integers $N_i < j$ are coprime to j. Then N_i has inverse in the

multiplicative group $(\mathbb{Z}/j\mathbb{Z})^*$, say N_i^{-1}, for $i = 1, 2$. Then we have

$$\begin{aligned} N_i N_i^{-1} &\equiv 1 \pmod{j}, \\ \frac{\bar{n}}{j} N_i N_i^{-1} &\equiv \frac{\bar{n}}{j} \pmod{\bar{n}}, \\ z_i N_i^{-1} &\equiv \frac{\bar{n}}{j} \pmod{\bar{n}}, \end{aligned}$$

where $i = 1, 2$. Letting $i = 2$ and multiplying N_1 on both sides of the above equation, we have

$$z_1 \equiv z_2 N_2^{-1} N_1 \pmod{\bar{n}}. \tag{4.5}$$

Similarly, we have

$$z_2 \equiv z_1 N_1^{-1} N_2 \pmod{\bar{n}}. \tag{4.6}$$

Let the length of O_1 be L_1 and let the length of O_2 be L_2. Then L_i is the smallest positive integer such that $C_{(-e)^{L_i} z_i} = C_{z_i}$, for $i = 1, 2$. By (4.5), we have

$$C_{(-e)^{L_1} z_2 N_2^{-1} N_1} = C_{z_2 N_2^{-1} N_1},$$

which implies that

$$C_{(-e)^{L_1} z_2} = C_{z_2}.$$

Therefore, $L_1 \geq L_2$. Similarly, by (4.6), we have $L_2 \geq L_1$. Therefore, $L_1 = L_2$. □

The following is another proposition regarding the lengths of the cycles.

Proposition 4.1.10. *Let e and n be integers and $\gcd(e, n) = 1$ and let π_{-e} be a permutation of the q-cyclotomic cosets modulo $\bar{n}$. Let C_z and C_{-z} be two different cyclotomic cosets, i.e., C_z and C_{-z} are two cyclotomic cosets corresponding to a*

reciprocal pair polynomials. If C_z and C_{-z} are contained in the same cycle O in the decomposition of π_{-e} and L is the smallest positive integer such that $C_{-z} = C_{(-e)^L z}$, then the length of O is $2L$.

Proof. Let L' be the length of O. Then L' is the smallest positive integer such that

$$C_z = C_{(-e)^{L'} z}.$$

Obviously, we have $L' > L$. Furthermore, we have $L|L'$. Otherwise, we can write $L' = b_1 L + b_2$ with $b_1 \geq 1$ and $0 < b_2 < L$. Then we have

$$\begin{aligned} C_z &= C_{(-e)^{L'} z} \\ &= C_{(-e)^{b_1 L + b_2} z} \\ &= C_{(-e)^{b_1 L} z (-e)^{b_2}} \\ &= C_{(-1)^{b_1} z (-e)^{b_2}}. \end{aligned}$$

If b_1 is even, then b_2 is an integer such that

$$C_z = C_{(-e)^{b_2} z},$$

which contradicts the minimality of L'. If b_1 is odd, then

$$\begin{aligned} C_z &= C_{-(-e)^{b_2} z} \\ C_{-z} &= C_{(-e)^{b_2} z}, \end{aligned}$$

which contradicts the minimality of L. Therefore, we have $L|L'$. Since

$$C_z = C_{-(-z)} = C_{-(-e)^L z} = C_{(-e)^{2L} z},$$

we have $L' \leq 2L$. Then $L' = 2L$. □

The following proposition says for any two cyclotomic cosets corresponding to $Q_j(x)$, there exists a multiplier permutation which maps one to the other.

Proposition 4.1.11. *Let $q = p^m$ and let n be an integer with $n = p^a\bar{n}$, where p is a prime. Let C_{z_1} and C_{z_2} be any two q-cyclotomic cosets modulo $\bar{n}$ corresponding to the j-th cyclotomic polynomial $Q_j(x)$. Then there exists a multiplier e such that $C_{-ez_1} = C_{z_2}$.*

Proof. Since the elements in z_i's, $i = 1, 2$, are all of order j in the additive group $\mathbb{Z}/j\mathbb{Z}$, there exist positive integers $N_i < j$ with $\gcd(N_i, j) = 1$ such that

$$z_i = \frac{\bar{n}}{j} N_i,$$

where $i = 1, 2$. Then $-N_1^{-1}N_2$ is in the multiplicative group $(\mathbb{Z}/j\mathbb{Z})^*$, denoted by N_3 and $0 < N_3 < j$. Obviously, $\gcd(N_3, j) = 1$. Let N_4 be the product of all the primes which divide $\frac{n}{j}$ but do not divide N_3, i.e.,

$$N_4 = \prod_{\substack{p' \text{ is a prime} \\ p'|\frac{n}{j} \\ p' \nmid N_3}} p'.$$

Let $e = N_4 j + N_3$. Then $\gcd(e, j) = \gcd(N_3, j) = 1$. Next we need to show that $\gcd(e, \frac{n}{j}) = 1$ and then we shall have $\gcd(e, n) = 1$. Let p'' be any prime with $p''|\frac{n}{j}$. If $p''|N_4$, then by the definition of N_4, we have $p'' \nmid N_3$. Then p'' does not divide $N_4 j + N_3 = e$. If $p'' \nmid N_4$, then by the definition of N_4, we have $p''|N_3$. Since $\gcd(N_3, j) = 1$, we have $p'' \nmid j$ and hence we have p'' does not divide $N_4 j + N_3 = e$. Therefore, for any $p''|\frac{\bar{n}}{j}$, we have p'' does not divide e. Therefore, we have $\gcd(e, \frac{n}{j}) = 1$

and hence $\gcd(e, n) = 1$. Then e is a multiplier. Furthermore, we have

$$\begin{aligned} -ez_1 &= -(N_4 j + N_3)\frac{\bar{n}}{j} N_1 \\ &= -N_4 N_1 \bar{n} + z_2 \\ &\equiv z_2 \pmod{\bar{n}}. \end{aligned}$$

Therefore, we have $C_{-ez_1} = C_{z_2}$. □

By the above proposition, once we fix two cyclotomic cosets corresponding to the same cyclotomic polynomial, then we can find a multiplier permutation which maps one coset to the other. Notice that the choice of such a multiplier e is not unique. We shall prove in the following proposition that although there are several such multipliers, their corresponding multiplier permutations restrict on the cosets corresponding to the same cyclotomic polynomial are the same.

Proposition 4.1.12. *Let $q = p^m$ and let n be an integer with $n = p^a \bar{n}$, where p is a prime. Let C_{z_1} and C_{z_2} be two q-cyclotomic cosets modulo $\bar{n}$ corresponding to the j-th cyclotomic polynomial $Q_j(x)$. Then any two different multipliers e_1 and e_2 such that $C_{z_1} = C_{-e_i z_2}$, for $i = 1, 2$, the permutations π_{-e_i}, for $i = 1, 2$, of the cyclotomic cosets corresponding to $Q_j(x)$ have the same cycle decompositions.*

Proof. Let C_{z_3} be any cyclotomic coset corresponding to $Q_j(x)$ and let e_1 and e_2 be any two multiplier such that $C_{z_1} = C_{-e_i z_2}$, for $i = 1, 2$. Then it remains to show that $C_{-e_1 z_3} = C_{-e_2 z_3}$. Mimicking the proof of Proposition 4.1.9, for $i = 1, 2, 3$, we have

$$z_i = \frac{\bar{n}}{j} N_i,$$

where $\gcd(N_i, j) = 1$. Furthermore, we have

$$z_3 \equiv z_2 N_2^{-1} N_3 \pmod{\bar{n}}.$$

Then, for $i = 1, 2$, we have

$$\begin{aligned} C_{-e_i z_3} &= C_{-e_i z_2 N_2^{-1} N_3} \\ &= C_{z_1 N_2^{-1} N_3}. \end{aligned}$$

Therefore, we have $C_{-e_1 z_3} = C_{-e_2 z_3}$. □

The above proposition says if the image of one coset is determined, then the images of the other cosets corresponding to the same cyclotomic polynomial are determined. Note that only the permutations restrict on the cosets corresponding to the same cyclotomic polynomial are the same. The permutations on all the cosets are not necessarily the same. For example, in Example 4.1.7, $e_1 = 13$ and $e_2 = 1$ are two different multipliers such that $C_{-e_i z_5} = C_{z_8}$. Furthermore, C_{z_5} and C_{z_8} are exactly the cyclotomic cosets corresponding to the cyclotomic polynomial $Q_3(x)$. However, the cycle decomposition of π_{-13} is (1)(2 3)(4 6)(5 8)(7 9) while the cycle decomposition of π_{-1} is (1)(2 9)(3 7)(4)(5 8)(6).

In order to study the existence of the E1-isodual cyclic codes which are not self-dual, we need to recall the following definitions and some facts regarding self-dual cyclic codes over finite fields.

Let j be an odd positive integer and let m be a positive integer. We say the pair (j, m) is *good* if j divides $(2^m)^k + 1$ for some integer $k \geq 0$ and *bad* otherwise (see Definition 3.3.2).

Proposition 4.1.13 (Theorem 3.2.2). *Let $n = 2^a\bar{n}$ and let $x^{\bar{n}} - 1$ be factorized over $\mathbb{F}_{2^m}$ as*

$$x^{\bar{n}} - 1 = f_1(x)f_2(x)\cdots f_r(x)h_1(x)h_1^*(x)\cdots h_t(x)h_t^*(x), \tag{4.7}$$

where $f_i(x)$'s are self-reciprocal irreducible polynomials, and $h_j(x)$'s are reciprocal polynomials of $h_j^*(x)$'s, respectively. A cyclic code $\mathscr{C}$ of length n over $\mathbb{F}_q$ is self-dual if and only if its generator polynomial is of the form

$$f_1(x)^{2^{a-1}}\cdots f_s(x)^{2^{a-1}}h_1(x)^{\beta_1}h_1^*(x)^{2^a-\beta_1}\cdots h_t(x)^{\beta_t}h_t^*(x)^{2^a-\beta_t},$$

where $0 \le \beta_i \le 2^a$ for each $1 \le i \le t$.

Proposition 4.1.14 (Lemma 3.3.4). *Let j be an odd positive integer. The j-th cyclotomic polynomial $Q_j(x)$ factors into $\frac{\phi(j)}{\mathrm{ord}_j(2^m)}$ distinct monic irreducible polynomials over $\mathbb{F}_{2^m}$ of the same degree $\mathrm{ord}_j(2^m)$, where ϕ is the Euler function. Moreover, if (j, m) is good, then all the irreducible polynomials in the factorization of $Q_j(x)$ are self-reciprocal. Otherwise, all of them form reciprocal polynomial pairs.*

Using the above results, we give the following theorem about the existence of the E1-isodual cyclic codes which are not self-dual.

Theorem 4.1.15. *There exists an E1-isodual cyclic code of length n over $\mathbb{F}_q$ which is not self-dual if and only if $q = 2^m$, n is even and at least one of the following two conditions satisfied:*

C1: *there exists a good pair (j, m) with $j|\bar{n}$ such that $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ is even,*

C2: *there exists a bad pair (j, m) with $j|\bar{n}$ such that $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ is doubly even,*

where ϕ is the Euler function.

Proof. Assume that $\mathscr{C}$ is a μ_e-isodual cyclic code of length n over $\mathbb{F}_q$ for some multiplier permutation μ_e, which is not self-dual. Obviously, n is even and q is even by Theorem 4.1.3. Then we write $n = 2^a\bar{n}$ with $\bar{n}$ odd and write $q = 2^m$.

Suppose that $x^{\bar{n}} - 1$ is factorized as (4.7). Then the generator polynomial $G(x)$ of $\mathscr{C}$ can be written as

$$G(x) = f_1(x)^{\alpha_1} \cdots f_s(x)^{\alpha_s} h_1(x)^{\beta_1} h_1^*(x)^{\gamma_1} \cdots h_t(x)^{\beta_t} h_t^*(x)^{\gamma_t},$$

where $\alpha_1, \alpha_2, \ldots, \alpha_s$, $\beta_1, \beta_2, \ldots, \beta_t$ and $\gamma_1, \gamma_2, \ldots, \gamma_t$ are all nonnegative integers not greater than 2^a.

By Proposition 4.1.13, at least one of the following condition satisfied:

D1: there exists some self-reciprocal irreducible polynomial, say $f_i(x)$ with $\alpha_i \neq 2^{a-1}$,

D2: there exists some reciprocal polynomial pair, say $h_k(x)$ and $h_k^*(x)$ with $\beta_k + \gamma_k \neq 2^a$.

Next, we need to show that D1 implies C1 and D2 implies C2, respectively.

Assume that the polynomial $f_i(x)$ is a self-reciprocal irreducible polynomial with $\alpha_i \neq 2^{a-1}$. Let the q-cyclotomic coset modulo $\bar{n}$ corresponding to $f_i(x)$ be C_{z_i}. Then the multiplicity m_i of C_{z_i} in defining set T of $\mathscr{C}$ is equal to α_i and hence $m_i \neq 2^{a-1}$. By Lemma 4.1.5, the cycle in the decomposition of π_{-e} containing C_{z_i} is of even length. Let $f_i(x)$ divide the j-th cyclotomoic polynomial $Q_j(x)$. Since $f_i(x)$ is self-reciprocal, by Proposition 4.1.14, we know that (j, m) is good and $j|\bar{n}$. By Proposition 4.1.9, the $\frac{\phi(j)}{\mathrm{ord}_j(2^m)}$ cyclotomic cosets corresponding to $Q_j(x)$ are divided into cycles of even length since the cycle containing C_{z_i} is of even length. Then we have $\frac{\phi(j)}{\mathrm{ord}_j(2^m)}$ is even. Therefore, D1 implies C1.

Assume that the reciprocal polynomial pair $h_k(x)$ and $h_k^*(x)$ is a reciprocal pair with $\beta_k + \gamma_k \neq 2^a$. Obviously, both of them are factors of the same cyclotomic polynomial, say j'-th cyclotomic polynomial $Q_{j'}(x)$. Then by Proposition 4.1.14, we have (j', m) is bad and $j'|\bar{n}$. Let the q-cyclotomic coset modulo $\bar{n}$ corresponding to $h_k(x)$ be $C_{z_{i'}}$. Then the q-cyclotomic coset modulo $\bar{n}$ corresponding to $h_k^*(x)$ is $C_{-z_{i'}}$. Then the multiplicity $m_{i'}$ of $C_{z_{i'}}$ in defining set T of $\mathscr{C}$ is β_k and the multiplicity $m_{i''}$ of $C_{-z_{i'}}$ in defining set T of $\mathscr{C}$ is γ_k. Therefore, $m_{i'} + m_{i''} \neq 2^a$. Next we discuss in the following two cases.

Case 1. Let $C_{z_{i'}}$ and $C_{-z_{i'}}$ be in different cycles, say O_1 and O_2, in the decomposition of π_{-e}. Then by Lemma 4.1.5, the length L_1 of O_1 and the length L_2 of O_2 are both even. By Proposition 4.1.9, we have $L_1 = L_2 := L$ with L even. We define the following map on all the cosets corresponding to the j'-th cyclotomic polynomial $Q_{j'}(x)$:

$$C_z \mapsto C_{-z}. \tag{4.8}$$

Since (j', m) is bad, we have $C_z \neq C_{-z}$. Moreover, it is easy to observe that if two cosets are in the same cycle, then their image under the map in (4.8) are also in the same cycle. Therefore the map in (4.8) can also be regarded as a map defined on the cycles corresponding to $Q_{j'}(x)$. In particular, it maps O_1 to O_2. If there exists some cycle such that it equals to its image under the map in (4.8), then by Proposition 4.1.10, the length of the cycle must be $2L$ that is doubly even. Then $\frac{\phi(j')}{\mathrm{ord}_{j'}(q)}$ is doubly even. If cycle is different from its image under the map in (4.8), then the map in (4.8) actually matches the cycle containing C_z with the cycle containing its image C_{-z}. Therefore, there are

even number of cycles corresponding to $Q_{j'}(x)$ and each cycle is of even length. Then we also have $\frac{\phi(j')}{\mathrm{ord}_{j'}(q)}$ is doubly even.

Case 2. Let $C_{z_{i'}}$ and $C_{-z_{i'}}$ be in the same cycle, say O, in the decomposition of π_{-e}. Then by Lemma 4.1.5, O is of even length and the smallest positive integer L such that $C_{-z_{i'}} = C_{(-e)^L z_{i'}}$ is even. By Proposition 4.1.10, the length of O is $2L$ which is doubly even. Therefore, we have $\frac{\phi(j')}{\mathrm{ord}_{j'}(q)}$ is doubly even.

Based on the above discussion, we conclude that D2 implies C2.

Conversely, assume that $q = 2^m$, n is even and at lease one of Conditions C1 and C2 is satisfied. We need to show that there exists an E1-isodual cyclic code of length n over $\mathbb{F}_q$ which is not self-dual.

First, assume that $q = 2^m$, n is even and Condition C1 is satisfied. Suppose that C_{z_i} is any cyclotomic coset corresponding to the cyclotomic polynomial $Q_j(x)$. By Proposition 4.1.11 and Proposition 4.1.12, there are $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ distinct multiplier permutations restrict on the cosets corresponding to $Q_j(x)$ totally and all such permutations restrict on the cosets corresponding to $Q_j(x)$ form a finite group of order $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ with the multiplication in the group defined as the composition of the permutations. Since $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ is even, there must exist a permutation $\pi_{e'}$ whose order is 2. By Proposition 4.1.9, any cycle corresponding to $Q_j(x)$ in the decomposition of $\pi_{e'}$ is of length 2. In particular, the cycle containing C_{z_i} is of length 2. By Lemma 4.1.5, there is a $\mu_{e'}$-isodual cyclic code and the multiplicity m_i of C_{z_i} in its defining set is not 2^{a-1}. Since (j, m) is good, the polynomial $f_i(x)$ corresponding to C_{z_i} is self-reciprocal and its power in the generator polynomial is $m_i \neq 2^{a-1}$. By Proposition 4.1.13, this $\mu_{e'}$-isodual cyclic code is not self-dual.

Next, we assume that $q = 2^m$, n is even and Condition C2 is satisfied. Suppose that C_{z_i} is a cyclotomic coset corresponding to the cyclotomic polynomial $Q_j(x)$. Since (j, m) is bad, we can regard the two cosets corresponding to the reciprocal polynomial pairs in the factorization of $Q_j(x)$ as one pair of cosets. For example, C_{z_i} and C_{-z_i} form one pair. Then there are $\frac{\phi(j)}{2\mathrm{ord}_j(q)}$ pairs of cosets. Let C_{z_i} and $C_{z_{i'}}$ be any two cosets corresponding to $Q_j(x)$. By Proposition 4.1.11, there is a multiplier e such that $C_{-ez_i} = C_{z_{i'}}$. It is easy to observe that $C_{(-e)(-z_i)} = C_{-z_{i'}}$. Therefore, the multiplier permutation μ_{-e} maps one pair of cosets to another pair of cosets and hence it can be regarded as a permutation of the pairs of cosets. By Proposition 4.1.12, there are $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ multiplier permutations restrict all the cosets corresponding to $Q_j(x)$ which maps a coset to another coset. Without distinguishing the cosets in the same pair, we deduce permutations on the pairs of cosets and there are $\frac{\phi(j)}{2\mathrm{ord}_j(q)}$ such deduced permutations. Since $\frac{\phi(j)}{2\mathrm{ord}_j(q)}$ is even, there exists a deduced permutation of order 2 on the pairs of cosets. Therefore, the cycles in the decomposition of the deduced permutation is of length 1 or 2. Therefore, the cycles in the decomposition of the corresponding multiplier permutation can only contain cosets from the same pair or cosets from 2 pairs. In particular, the cycle containing C_{z_i} is either

$$(C_{z_i}, C_{-z_i}),$$

or

$$(C_{z_i}, C_{z_{i'}}, C_{-z_i}, C_{-z_{i'}}),$$

where C_{z_i} and $C_{z_{i'}}$ are in different pairs. If the cycle is (C_{z_i}, C_{-z_i}), then by Proposition 4.1.12, all the cycles is of length 2 and contain one pair. Then the deduced permutation on pairs is of order 1, contradicting to the order of the deduced permutation

which should be 2. Therefore, the cycle containing C_{z_i} is

$$(C_{z_i}, C_{z_{i'}}, C_{-z_i}, C_{-z_{i'}}),$$

where C_{z_i} and $C_{z_{i'}}$ are in different pairs. By Lemma 4.1.5, we can choose the multiplicity m_i of C_{z_i}, which is equal to the multiplicity of C_{z_i} to be any integer from 0 to 2^a such that the corresponding code is E1-isodual. When we choose $m_i \neq 2^{a-1}$, the sum of the powers of the reciprocal pairs corresponding to C_{z_i} and C_{-z_i} is not 2^a. Therefore, by Theorem 4.1.13, the corresponding E1-isodual cyclic code is not self-dual. □

The following two examples show the way to construct E1-isodual cyclic codes which are not self-dual, for the two cases C1 and C2 in Theorem 4.1.15, respectively.

Example 4.1.16. Let $n = 130$ and $q = 2$. Then $\bar{n} = 65$ and the pairs $(j, 1)$ for any $j|65$ are good pairs since $(65, 1)$ is good. Notice that

$$\begin{aligned}
Q_1(x) =& x + 1,\\
Q_5(x) =& x^4 + x^3 + x^2 + x + 1,\\
Q_{15}(x) =& x^{12} + x^8 + x^7 + x^6 + x^5 + x^4 + 1,\\
Q_{65}(x) =& (x^{12} + x^{10} + x^7 + x^6 + x^5 + x^2 + 1)\\
&\times (x^{12} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + 1)\\
&\times (x^{12} + x^{11} + x^9 + x^7 + x^6 + x^5 + x^3 + x + 1)\\
&\times (x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)
\end{aligned}$$

Observe that only $Q_{65}(x)$ has even number of irreducible factors, which means $\frac{\phi(65)}{\text{ord}_{65}(2)}$ is even. The following table lists the cyclotomic cosets corresponding to $Q_{65}(x)$.

cosets	corresponding irreducible polynomials
$C_1 = \{1, 2, 4, 8, 16, 32, 33, 49, 57, 61, 63, 64\}$	$x^{12} + x^{10} + x^7 + x^6 + x^5 + x^2 + 1$
$C_3 = \{3, 6, 12, 17, 24, 31, 34, 41, 48, 53, 59, 62\}$	$x^{12} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + 1$
$C_7 = \{7, 9, 14, 18, 28, 29, 36, 37, 47, 51, 56, 58\}$	$x^{12} + x^{11} + x^9 + x^7 + x^6 + x^5 + x^3 + x + 1$
$C_{11} = \{11, 19, 21, 22, 23, 27, 38, 42, 43, 44, 46, 54\}$	$x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

By Proposition 4.1.11, there are 4 choices for the image of the coset C_1. By Proposition 4.1.12, there are 4 different permutations of the above 4 cosets:

$$(C_1)(C_3)(C_7)(C_{11}),$$

$$(C_1, C_3, C_7, C_{11}),$$

$$(C_1, C_7)(C_3, C_{11}),$$

$$(C_1, C_{11}, C_7, C_3).$$

It easily verify that the permutations form a finite group of order 4. Among them, $(C_1, C_7)(C_3, C_{11})$ is of order 2. We can choose $e = 123$. Then μ_{123} permutes the cosets as

$$(C_0)(C_{13})(C_5)(C_1,\ C_7)(C_3,\ C_{11}).$$

In this case, the defining sets of the μ_{123}-isodual cyclic codes which are not self-dual can be chosen as

$$T = C_0 \bigcup C_{13} \bigcup C_5 \bigcup m_1 C_1 \bigcup (2 - m_1) C_7 \bigcup m_2 C_3 \bigcup (2 - m_2 C_{11}),$$

where $0 \leq m_1, m_2 \leq 2$ and $m_1 \neq 1$ or $m_2 \neq 1$.

Example 4.1.17. Let $n = 146$ and $q = 2$. Then $\bar{n} = 73$ and there are only two pairs $(j, 1)$ with $j|73$, namely $(1, 1)$ that is good and $(73, 1)$ that is bad because

$\text{ord}_{73}(2) = 9$. Note that $\frac{\phi(1)}{\text{ord}_1(2)} = 1$ that is odd and $\frac{\phi(73)}{\text{ord}_{73}(2)} = 8$ that is doubly even. All the cyclotomic cosets corresponding to $Q_{73}(x)$ are listed as the following 4 pairs (the two cosets corresponding to a reciprocal pair of polynomials) in the table.

1	$C_1 = \{1, 2, 4, 8, 16, 32, 37, 55, 64\}$	$C_9 = \{9, 18, 36, 41, 57, 65, 69, 71, 72\}$
2	$C_3 = \{3, 6, 12, 19, 23, 24, 38, 46, 48\}$	$C_{25} = \{25, 27, 35, 49, 50, 54, 61, 67, 70\}$
3	$C_5 = \{5, 7, 10, 14, 20, 28, 39, 40, 56\}$	$C_{17} = \{17, 33, 34, 45, 53, 59, 63, 66, 68\}$
4	$C_{11} = \{11, 15, 21, 22, 30, 42, 44, 47, 60\}$	$C_{13} = \{13, 26, 29, 31, 43, 51, 52, 58, 62\}$

Then there are four choices for the image of the first pair in the deduce permutations as in the proof of Theorem 4.1.15:

$$(1)(2)(3)(4),$$

$$(1, 2)(3, 4),$$

$$(1, 3, 2, 4),$$

$$(1, 4, 2, 3),$$

where the numbers are the indices of the pairs. Among them, $(1, 2)(3, 4)$ is of order 2 and whose corresponding multiplier permutation is

$$(C_1,\ C_3,\ C_9,\ C_{25})(C_5,\ C_{11},\ C_{17},\ C_{13}),$$

or

$$(C_1,\ C_{25},\ C_9,\ C_3)(C_5,\ C_{13},\ C_{17},\ C_{11}).$$

We can choose $e = 143$. Then μ_{143} permutes the cosets as

$$(C_0)(C_1,\ C_3,\ C_9,\ C_{25})(C_5,\ C_{11},\ C_{17},\ C_{13}).$$

In this case, the defining sets of the $[146, 73]_2$ μ_{143}-isodual cyclic codes which are not self-dual can be chosen as

$$\begin{aligned} T =& C_0 \bigcup m_1 C_1 \bigcup (2 - m_1) C_3 \\ & \bigcup m_1 C_9 \bigcup (2 - m_1) C_{25} \bigcup m_2 C_5 \\ & \bigcup (2 - m_2 C_{11}) \bigcup m_2 C_{17} \bigcup (2 - m_2) C_{13}, \end{aligned}$$

where $0 \leq m_1, m_2 \leq 2$ and $m_1 \neq 1$ or $m_2 \neq 1$. Similarly, we can choose $e = 121$. Then μ_{121} permutes the cosets as

$$(C_0)(C_1,\ C_{25},\ C_9,\ C_3)(C_5,\ C_{13},\ C_{17},\ C_{11}).$$

In this case, the defining sets of the $[146, 73]_2$ μ_{143}-isodual cyclic codes which are not self-dual can be chosen as

$$\begin{aligned} T =& C_0 \bigcup m_1 C_1 \bigcup (2 - m_1) C_{25} \\ & \bigcup m_1 C_9 \bigcup (2 - m_1) C_3 \bigcup m_2 C_5 \\ & \bigcup (2 - m_2 C_{13}) \bigcup m_2 C_{17} \bigcup (2 - m_2) C_{11}, \end{aligned}$$

where $0 \leq m_1, m_2 \leq 2$ and $m_1 \neq 1$ or $m_2 \neq 1$.

Using the results about classification of good and bad pairs in Chapter 3, we further simplify the condition in Theorem 4.1.15 in some cases. For convenience, we need the following lemma.

Lemma 4.1.18. *Let $j = \prod_{i=1}^{k} p_i^{\alpha_i}$, where p_i's are distinct primes and α_i's are positive integers. Let $q = 2^m$. Then $\mathrm{ord}_j(q) = \mathrm{lcm}_i\{\mathrm{ord}_{p_i^{\alpha_i}}(q)\}$. Furthermore, $\mathrm{ord}_{p_i^{\alpha_i}}(q) = p^{\epsilon_i}\mathrm{ord}_{p_i}(q)$ for some $\epsilon_i \geq 0$.*

Proof. For each $1 \leq i \leq k$, we have $\mathrm{ord}_{p_i^{\alpha_i}}(q)$ divides $\mathrm{ord}_j(q)$ because $p_i^{\alpha_i} | j$. Therefore, $\mathrm{lcm}_i\{\mathrm{ord}_{p_i^{\alpha_i}}(q)\}$ divides $\mathrm{ord}_j(q)$. Since $q^{\mathrm{lcm}_i\{\mathrm{ord}_{p_i^{\alpha_i}}(q)\}} \equiv 1 \pmod{p_i^{\alpha_i}}$ and $j = \prod_{i=1}^{k} p_i^{\alpha_i}$, for each $1 \leq i \leq k$, by the Chinese remainder theorem, we have $q^{\mathrm{lcm}_i\{\mathrm{ord}_{p_i^{\alpha_i}}(q)\}} \equiv 1 \pmod{j}$. Then $\mathrm{ord}_j(q)$ divides $\mathrm{lcm}_i\{\mathrm{ord}_{p_i^{\alpha_i}}(q)\}$. The last statement is quoted from [18, Proposition 4]. □

Let $j = \prod_{i=1}^{k} p_i^{\alpha_i}$, where p_i's are distinct odd primes and α_i's are positive integers and let $q = 2^m$. Then $\phi(j) = \prod_{i=1}^{k}(p_i - 1)p_i^{\alpha_i - 1}$. Let $2^{e_i} || (p_i - 1)$ and let $p_i \in S_{r_i}^m$, where notation $||$ is defined in Definition 3.3.6 and the set is defined in Definition 3.3.7. By Lemma 4.1.18, the parity of $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ depends on the term $\sum_{i=1}^{k} e_i - \max_i\{r_i\}$. More precisely, if $\sum_{i=1}^{k} e_i - \max_i\{r_i\} = 0$, then $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ is odd. If $\sum_{i=1}^{k} e_i - \max_i\{r_i\} = 1$, then $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ is oddly even. If $\sum_{i=1}^{k} e_i - \max_i\{r_i\} \geq 2$, then $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ is doubly even. Furthermore, it is shown in [18, Theorem 1] that the pair (j, m) is good if and only if there exists $r \geq 1$ such that $\mathrm{ord}_{p_i}(q) \in S_r^m$ for each $1 \leq i \leq k$. Then by Proposition 3.3.9 and Theorem 3.3.11, we give a corollary.

For convenience, we quote Proposition 3.3.9 and Theorem 3.3.11 in the following proposition before the corollary.

Proposition 4.1.19. *Let p be an odd prime.*

1. *Let $p \equiv 3 \pmod 8$.*
   (a) *If m is odd, then $p \in S_1^m$ and (p, m) is good.*
   (b) *If m is even, then $p \in S_0^m$ and (p, m) is bad.*
2. *Let $p \equiv 5 \pmod 8$.*
   (a) *If m is odd, then $p \in S_2^m$ and (p, m) is good.*

(b) If $m \equiv 2 \pmod 4$*, then* $p \in S_1^m$ *and* (p, m) *is good.*

(c) If $m \equiv 0 \pmod 4$*, then* $p \in S_0^m$ *and* (p, m) *is bad.*

3. *Let* $p \equiv 7 \pmod 8$*. Then* $p \in S_0^m$ *and* (p, m) *is bad.*

Let j *be an odd positive integer with no prime factor congruent to* 1 *modulo* 8*.*

1. *Let* m *be odd. Then* (j, m) *is good if and only if all the prime factors of* j *are congruent to* 3 *modulo* 8 *or all of them are congruent to* 5 *modulo* 8*.*

2. *Let* $m \equiv 2 \pmod 4$*. Then* (j, m) *is good if and only if all the prime factors of* j *are congruent to* 5 *modulo* 8*.*

3. *Let* $m \equiv 0 \pmod 4$*. Then* (j, m) *is always bad.*

Corollary 4.1.20. *Let* $n = 2^a\bar{n}$ *where* $a \geq 1$ *and* $\bar{n}$ *is an odd positive integer with no prime factor congruent to* 1 *modulo* 8*. Let* $q = 2^m$*.*

1. *If* m *is odd, then there is an* $[n, \frac{n}{2}]_q$ *E1-isodual cyclic code which is not self-dual if and only if* $\bar{n}$ *has at least two distinct prime factors and it is not one of the following two types:* $\bar{n} = p_1^{\alpha_1}p_2^{\alpha_2}$*, where* α_1, α_2 *are positive integers,* p_1*,* p_2 *are primes such that*

$$\begin{aligned} p_1 \equiv 3 \pmod 8, \quad p_2 \equiv 5 \pmod 8, \\ \text{or } p_1 \equiv 3 \pmod 8, \quad p_2 \equiv 7 \pmod 8, \\ \text{or } p_1 \equiv 5 \pmod 8, \quad p_2 \equiv 7 \pmod 8. \end{aligned}$$

Table 4.1: The prime factors of $\bar{n}$

	1	3	5	7
Case 1	×	✓	×	×
Case 2	×	×	✓	×
Case 3	×	×	×	✓
Case 4	×	✓	✓	×
Case 5	×	✓	×	✓
Case 6	×	×	✓	✓
Case 7	×	✓	✓	✓

2. *If m is even, then there is an $[n, \frac{n}{2}]_q$ E1-isodual cyclic code which is not self-dual if and only if $\bar{n}$ has at least two distinct prime factors or $\bar{n}$ is a power of a prime congruent to 5 modulo 8.*

Proof. We prove the statement case by case. Table 4.1 lists all the possible cases according to the prime factors of $\bar{n}$. The symbol ✓ means $\bar{n}$ has a prime factor which is congruent to the number given in the corresponding column, while the symbol × means $\bar{n}$ has no prime factor which is congruent to the number given in the corresponding column. For example, in Case 1, $\bar{n}$ has only prime factors which are congruent to 3 modulo 8. Since $\bar{n}$ is odd, the prime factors of $\bar{n}$ can only be congruent to 1, 3, 5 or 7 modulo 8. Furthermore, we assume that $\bar{n}$ has no prime factor congruent to 1 modulo 8, so the entries corresponding the column "1" are all ×.

Let $j|\bar{n}$ and let $j = \prod_{i=1}^{k} p_i^{\alpha_i}$, where p_i's are distinct primes not congruent to 1 modulo 8 and α_i's are positive integers. Let $2^{e_i}||(p_i - 1)$ and let $p_i \in S_{r_i}^m$.

Firstly, we assume that m is odd.

Case 1: It is obvious that $e_i = 1$ for each $1 \leq i \leq k$. By Proposition 4.1.19, we have $r_i = 1$ for each $1 \leq i \leq k$ and the pair (j, m) is good. The parity of $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ is determined by $\sum_{i=1}^{k} e_i - \max_{i\in\{1..k\}}\{r_i\} = k - 1$. Therefore, if and only if $k \geq 2$, we have $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ is even. By Theorem 4.1.15, in this case, there is an $[n, \frac{n}{2}]_q$ E1-isodual cyclic code which is not self-dual if and only if $\bar{n}$ has at least two distinct prime factors.

Case 2: Obviously, we have $e_i = 2$ for each $1 \leq i \leq k$. By Proposition 4.1.19, we have $r_i = 2$ for each $1 \leq i \leq k$ and the pair (j, m) is good. The parity of $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ is determined by $\sum_{i=1}^{k} e_i - \max_{i\in\{1..k\}}\{r_i\} = 2k - 2$. Therefore, if and only if $k \geq 2$, we have $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ is even. By Theorem 4.1.15, in this case, there is an $[n, \frac{n}{2}]_q$ E1-isodual cyclic code which is not self-dual if and only if $\bar{n}$ has at least two distinct prime factors.

Case 3: Obviously, we have $e_i = 1$ for each $1 \leq i \leq k$. By Proposition 4.1.19, we have $r_i = 0$ for each $1 \leq i \leq k$ and the pair (j, m) is bad. The parity of $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ is determined by $\sum_{i=1}^{k} e_i - \max_{i\in\{1..k\}}\{r_i\} = k$. Therefore, if and only if $k \geq 2$, we have $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ is doubly even. By Theorem 4.1.15, in this case, there is an $[n, \frac{n}{2}]_q$ E1-isodual cyclic code which is not self-dual if and only if $\bar{n}$ has at least two distinct prime factors.

Case 4: By the above discussion, if $\bar{n}$ has at least two distinct prime factors which are both congruent to 3 (or 5), then based on the discussion in Case 1 and 2, there exists an $[n, \frac{n}{2}]_q$ E1-isodual cyclic code. Therefore, it suffices to discuss the case when $\bar{n} = p_1^{\alpha_1} p_2^{\alpha_2}$, where $p_1 \equiv 3 \pmod 8$, $p_2 \equiv 5 \pmod 8$ and α_1, α_2 are positive integers. Then $e_1 = 1$, $e_2 = 2$, $r_1 = 1$ and $r_2 = 2$. If $j = p_1^{\beta_1}$ with $\beta_1 \leq \alpha_1$, then

(j, m) is good and $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ is odd. Similarly, if $j = p_2^{\beta_2}$ with $\beta_2 \leq \alpha_2$, then (j, m) is good and $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ is odd. If $j = p_1^{\beta_1} p_2^{\beta_2}$ with $1 \leq \beta_i \leq \alpha_i$ for $i = 1, 2$, then (j, m) is bad and the parity of $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ is determined by $\sum_{i=1}^{2} e_i - \max_{i\in\{1,2\}}\{r_i\} = 3-2 = 1$. Then $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ is oddly even. Then by Theorem 4.1.15, in this case, there is an E1-isodual cyclic code which is not self-dual except when $\bar{n} = p_1^{\alpha_1} p_2^{\alpha_2}$, where $p_1 \equiv 3 \pmod 8$, $p_2 \equiv 5 \pmod 8$ and α_1, α_2 are positive integers.

Case 5: Similarly to Case 4, it is sufficient to discuss the case when $\bar{n} = p_1^{\alpha_1} p_2^{\alpha_2}$, where $p_1 \equiv 3 \pmod 8$, $p_2 \equiv 7 \pmod 8$ and α_1, α_2 are positive integers. Then $e_1 = 1$, $e_2 = 1$, $r_1 = 1$ and $r_2 = 0$. Then if $p_1 \nmid j$ (or $p_2 \nmid j$), then it is shown in Case 3 (or Case 1) that there is no E1-isodual cyclic code which is not self-dual. If $p_1 | j$ and $p_2 | j$, then (j, m) is bad and we have $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ is oddly even. Therefore, by Theorem 4.1.15, in this case there is an E1-isodual cyclic code which is not self-dual except when $\bar{n} = p_1^{\alpha_1} p_2^{\alpha_2}$, where $p_1 \equiv 3 \pmod 8$, $p_2 \equiv 7 \pmod 8$ and α_1, α_2 are positive integers.

Case 6: Similarly to Case 5, it is sufficient to discuss the case when $\bar{n} = p_1^{\alpha_1} p_2^{\alpha_2}$, where $p_1 \equiv 5 \pmod 8$, $p_2 \equiv 7 \pmod 8$ and α_1, α_2 are positive integers. Then $e_1 = 2$, $e_2 = 1$, $r_1 = 2$ and $r_2 = 0$. Then for any $j | \bar{n}$, if $p_1 \nmid j$ or $p_2 \nmid j$, then it is shown in Case 3 or Case 2 that there is no E1-isodual cyclic code which is not self-dual. If $p_1 | j$ and $p_2 | j$, then (j, m) is bad and we have $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ is oddly even. Therefore, by Theorem 4.1.15, in this case there is an E1-isodual cyclic code which is not self-dual except when $\bar{n} = p_1^{\alpha_1} p_2^{\alpha_2}$, where $p_1 \equiv 5 \pmod 8$, $p_2 \equiv 7 \pmod 8$ and α_1, α_2 are positive integers.

Case 7: Based on the above discussion, it is sufficient to discuss the case when $\bar{n} =$

$p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}$, where $p_1 \equiv 3 \pmod 8$, $p_2 \equiv 5 \pmod 8$, $p_3 \equiv 7 \pmod 8$ and $\alpha_1, \alpha_2, \alpha_3$ are all positive integers. Then $e_1 = 1$, $e_2 = 2$, $e_3 = 1$, $r_1 = 1$, $r_2 = 2$ and $r_3 = 0$. When $j = \bar{n}$, the parity of $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ is determined by $1 + 2 + 1 - 2 = 2$, which means $\frac{\phi(j)}{\mathrm{ord}_j(q)}$ is doubly even. Therefore, by Theorem 4.1.15, in this case there always exists an E1-isodual cyclic code.

The conclusion for odd m follows from the summary of all the cases discussed.

For the case when m is even, mimicking the proof for odd m, we obtain the conclusion. □

4.2 E2-isodual cyclic codes

In this section, we discuss the E2-isodual cyclic codes or say Λ-isodual cyclic codes where Λ is a scalar transformation defined as in Definition 1.0.2. In general, for a cyclic code $\mathscr{C}$ of length n over $\mathbb{F}_q$, the equivalent code $\Lambda(\mathscr{C})$ is not always cyclic again. Next, we discuss a necessary and sufficient condition on Λ such that $\Lambda(\mathscr{C})$ is cyclic again when $\mathscr{C}$ is cyclic. For our purpose, we need the following definition.

Definition 4.2.1. *Let N be a positive integer and let $\mathbf{V} = (V_0, V_1, \ldots, V_{N-1})$ be a vector of length N over $\mathbb{F}_q$. The* support of the vector $\mathbf{V}$*, denoted by* Supp$\mathbf{V}$*, is defined to be as follows:*

$$\mathrm{Supp}\mathbf{V} = \{i : V_i \neq 0\}.$$

For example, if $\mathbf{V} = (1, 0, 0, 2, 1, 0, 0, 1, 0, 2)$ over $\mathbb{F}_3$, then the support of the vector is $\mathrm{Supp}\mathbf{V} = \{0, 3, 4, 7, 9\}$. In order to describe a necessary and sufficient condition on Λ such that $\Lambda(\mathscr{C})$ is cyclic, we give the following lemma first.

Lemma 4.2.2. *If*

$$M = \begin{bmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,k-1} & \cdots & g_{0,n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_{1,1} & \cdots & g_{1,k-1} & \cdots & g_{1,n-k} & g_{1,n-k+1} & 0 & \cdots & 0 \\ \vdots & & & & \vdots & \vdots & & & & \\ 0 & \cdots & 0 & g_{k-1,k-1} & \cdots & g_{k-1,n-k} & \cdots & \cdots & \cdots & g_{k-1,n-1} \end{bmatrix}_{k\times n},$$

with $g_{0,0}, g_{1,1}, \ldots, g_{k-1,k-1}$ all nonzero, is the generator matrix of an $[n,k]_q$ linear code $\mathscr{C}$, then $\mathscr{C}$ is cyclic if and only if for $0 \le i \le k-1$, the vector

$$(g_{i,i}, g_{i,i+1}, \ldots, g_{i,i+n-k}, 0, \ldots, 0)$$

is a nonzero scalar multiple of the first row, and the polynomial

$$g_{0,n-k}^{-1}(g_{0,0} + g_{0,1}x + \cdots + g_{0,n-k}x^{n-k})$$

divides $x^n - 1$.

Proof. Assume that $\mathscr{C}$ is cyclic. Since the first row of the generator matrix M is a codeword of $\mathscr{C}$, it is corresponding to the polynomial

$$g_{0,0} + g_{0,1}x + \cdots + g_{0,n-k}x^{n-k}.$$

Let $G(x)$ be the generator polynomial of $\mathscr{C}$. Then $G(x)$ is the unique polynomial which is monic and has least degree among all the polynomials in $\mathscr{C}$. Since $\mathscr{C}$ is of length n and dimension k, we have $\deg(G(x)) = n - k$. By the uniqueness of the generator polynomial, we have

$$G(x) = g_{0,n-k}^{-1}(g_{0,0} + g_{0,1}x + \cdots + g_{0,n-k}x^{n-k}),$$

and hence $g_{0,n-k}^{-1}(g_{0,0} + g_{0,1}x + \cdots + g_{0,n-k}x^{n-k})$ divides $x^n - 1$. Since $\mathscr{C}$ is cyclic, the $(n-i)$-cyclic shift of the $(i+1)$-th row of M

$$(g_{i,i}, g_{i,i+1}, \ldots, g_{i,i+n-k}, 0, \ldots, 0)$$

is also a codeword of $\mathscr{C}$, for $0 \leq i \leq k-1$. Therefore, for $0 \leq i \leq k-1$, we have

$$G(x) = g_{i,i+n-k}^{-1}(g_{i,0} + g_{i,i+1}x + \cdots + g_{i,i+n-k}x^{n-k}),$$

and the vector

$$(g_{i,i}, g_{i,i+1}, \ldots, g_{i,i+n-k}, 0, \ldots, 0)$$

is a nonzero scalar multiple of the first row.

Conversely, since for $0 \leq i \leq k-1$, the vector

$$(g_{i,i}, g_{i,i+1}, \ldots, g_{i,i+n-k}, 0, \ldots, 0)$$

is a nonzero scalar multiple of the first row, the cyclic shift of the j-th row of M is still in $\mathscr{C}$, for any $1 \leq j \leq k-1$. The cyclic shift of the k-th row of M is

$$\begin{aligned} v &= (g_{k-1,n-1}, 0, \ldots, 0, g_{k-1,k-1}, \ldots, g_{k-1,n-k}, \ldots, g_{k-1,n-2}) \\ &= g_{k-1,n-1}g_{0,n-k}^{-1}(g_{0,n-k}, 0, \ldots, 0, g_{0,0}, \ldots, g_{0,n-k-1}). \end{aligned}$$

Let the polynomial $G'(x)$ be

$$G'(x) = g_{0,n-k}^{-1}(g_{0,0} + g_{0,1}x + \cdots + g_{0,n-k}x^{n-k}).$$

Then the polynomial $v(x)$ corresponding to the vector $\mathbf{v}$ is $g_{k-1,n-1}(x^k G'(x) - x^n + 1)$. Since $G'(x)$ divides $x^n - 1$, we write $x^n - 1 = G'(x)h(x)$ and $h(x)$ is a monic polynomial

of degree k. Therefore, we have

$$x^k G'(x) - x^n + 1 = (x^k - h(x))G'(x),$$

where $x^k - h(x)$ is a polynomial of degree smaller than k. Therefore, the vector $\mathbf{v}$ is a linear combination of the row vectors of the matrix M. Therefore, we have the cyclic shift of the k-th row of M is also in $\mathscr{C}$. Then the code $\mathscr{C}$ is cyclic. □

The following theorem is a necessary and sufficient condition on Λ for $\Lambda(\mathscr{C})$ to be cyclic again.

Theorem 4.2.3. *Let $\mathscr{C}$ be an $[n, \frac{n}{2}]_q$ cyclic code with generator polynomial*

$$G(x) = G_0 + G_1 x + \cdots + G_{\frac{n}{2}} x^{\frac{n}{2}}.$$

Let $\Delta = \gcd\{i : i \in \mathrm{Supp}((G_0, G_1 \ldots, G_{\frac{n}{2}}))\}$. Let $\Lambda = (\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$ be a scalar transformation, where $\lambda_i \in \mathbb{F}_q^*$ for $0 \leq i \leq n-1$. Then $\Lambda(\mathscr{C})$ is cyclic if and only if there exists a constant $\rho \in \mathbb{F}_q^*$ such that $(\lambda_i, \lambda_{i+\Delta}, \lambda_{i+2\Delta}, \ldots, \lambda_{i+(\frac{n}{\Delta}-1)\Delta})$ forms a geometric sequence with ratio ρ for each $0 \leq i \leq \Delta - 1$ and $\lambda_0 G_0 + \lambda_1 G_1 x + \cdots + \lambda_{\frac{n}{2}} G_{\frac{n}{2}} x^{\frac{n}{2}}$ divides $x^n - 1$.

Proof. Since the generator polynomial of $\mathscr{C}$ is

$$G(x) = G_0 + G_1 x + \cdots + G_{\frac{n}{2}} x^{\frac{n}{2}},$$

then the generator matrix of $\mathscr{C}$ can be written as

$$M = \begin{bmatrix} G_0 & G_1 & G_2 & \cdots & G_{\frac{n}{2}} & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & G_0 & G_1 & G_2 & \cdots & G_{\frac{n}{2}} & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & G_0 & G_1 & G_2 & \cdots & G_{\frac{n}{2}} & 0 & \cdots & \cdots & 0 \\ 0 & \cdots & 0 & \ddots & \ddots & \ddots & \cdots & \ddots & 0 & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & G_0 & G_1 & G_2 & \cdots & G_{\frac{n}{2}} & 0 & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & G_0 & G_1 & G_2 & \cdots & G_{\frac{n}{2}} & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & G_0 & G_1 & G_2 & \cdots & G_{\frac{n}{2}} \end{bmatrix}_{\frac{n}{2} \times n}.$$

Then the generator matrix of $\Lambda(\mathscr{C})$ is

$$M' = M \cdot \begin{bmatrix} \lambda_0 & 0 & \cdots & 0 \\ 0 & \lambda_1 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_{n-1} \end{bmatrix}_{n \times n}.$$

Assume that $\Lambda(\mathscr{C})$ is cyclic. Then by Lemma 4.2.2, the polynomial

$$G'(x) = \lambda_{\frac{n}{2}}^{-1} G_{\frac{n}{2}}^{-1} (\lambda_0 G_0 + \lambda_1 G_1 x + \cdots + \lambda_{\frac{n}{2}} G_{\frac{n}{2}} x^{\frac{n}{2}})$$

is the generator polynomial of $\Lambda(\mathscr{C})$ and $\lambda_0 G_0 + \lambda_1 G_1 x + \cdots + \lambda_{\frac{n}{2}} G_{\frac{n}{2}} x^{\frac{n}{2}}$ divides $x^n - 1$. Furthermore, for $0 \leq k \leq \frac{n}{2} - 2$, we have

$$(\lambda_k G_0, \lambda_{k+1} G_1, \ldots, \lambda_{k+\frac{n}{2}} G_{\frac{n}{2}})$$

and

$$(\lambda_{k+1} G_0, \lambda_{k+2} G_1, \ldots, \lambda_{k+\frac{n}{2}+1} G_{\frac{n}{2}})$$

are linearly dependent, which holds if and only if for $0 \leq k \leq \frac{n}{2} - 2$ and $0 \leq i \leq \frac{n}{2}$

$$\lambda_{k+\frac{n}{2}}^{-1} \lambda_{k+i} G_i = \lambda_{k+\frac{n}{2}+1}^{-1} \lambda_{k+i+1} G_i,$$

if and only if for $0 \leq k \leq \frac{n}{2} - 2$ and $i \in \mathrm{Supp}((G_0, G_1 \ldots, G_{\frac{n}{2}}))$,

$$\lambda_{k+\frac{n}{2}}^{-1} \lambda_{k+i} = \lambda_{k+\frac{n}{2}+1}^{-1} \lambda_{k+i+1}. \tag{4.9}$$

Let $\frac{\lambda_j}{\lambda_{j-1}} = Q_j$ for $1 \leq j \leq n-1$. Then by the above equation, for $i \in \mathrm{Supp}((G_0, G_1, \ldots, G_{\frac{n}{2}}))$, we have

$$Q_{i+k+1} = Q_{\frac{n}{2}+k+1}, \text{ for any } 0 \leq k \leq \frac{n}{2} - 2. \tag{4.10}$$

In particular, since $G_0 \neq 0$, we have

$$Q_{k+1} = Q_{\frac{n}{2}+k+1}, \text{ for any } 0 \leq k \leq \frac{n}{2} - 2. \tag{4.11}$$

Define $Q_0 := Q_{\frac{n}{2}}$ and the sequence $Q = (Q_0, Q_1, Q_2, \ldots, Q_{\frac{n}{2}-1})$. Then by Equations (4.10) and (4.11), it is easy to check that for each $i \in \mathrm{Supp}((G_0, G_1, \ldots, G_{\frac{n}{2}}))$, the sequence Q is invariant under i cyclic shifts. Therefore, the sequence Q is invariant under $\gcd\{i : i \in \mathrm{Supp}((G_0, G_1, \ldots, G_{\frac{n}{2}}))\} = \Delta$ cyclic shifts. Let $\rho = Q_1 Q_2 \cdots Q_\Delta$. Then we conclude that for each $0 \leq i \leq \Delta - 1$, the sequence $(\lambda_i, \lambda_{i+\Delta}, \lambda_{i+2\Delta}, \ldots, \lambda_{i+(\frac{n}{\Delta}-1)\Delta})$ is a geometric sequence with ratio ρ.

Conversely, we assume that there exists a constant $\rho \in \mathbb{F}_q^*$ such that

$$(\lambda_i, \lambda_{i+\Delta}, \lambda_{i+2\Delta}, \ldots, \lambda_{i+(\frac{n}{\Delta}-1)\Delta})$$

forms a geometric sequence with ratio ρ for each $0 \leq i \leq \Delta - 1$. and $\lambda_0 G_0 + \lambda_1 G_1 x + \cdots + \lambda_{\frac{n}{2}} G_{\frac{n}{2}} x^{\frac{n}{2}}$ divides $x^n - 1$.

Then for $0 \leq i \leq \frac{n}{2} - 1$, the $(i+1)$-th row of M' is

$$[\underbrace{0, \cdots, 0}_{i}, \lambda_{i-1}G_0, \lambda_i G_1, \cdots, \lambda_{i+\frac{n}{2}-1}G_{\frac{n}{2}}, \underbrace{0, \cdots, 0}_{\frac{n}{2}-i-1}].$$

and its $(n-i)$-cyclic shift is the vector $\mathbf{v_i} = (\lambda_{i-1}G_0, \lambda_i G_1, \cdots, \lambda_{i+\frac{n}{2}-1}G_{\frac{n}{2}}, \underbrace{0, \cdots, 0}_{\frac{n}{2}-1})$.

For $0 \leq j \leq \frac{n}{2}$, if $G_j = 0$, then

$$\begin{aligned}\lambda_{i+j-1}G_j &= 0 \\ &= \lambda_j G_j \\ &= \lambda_{i-1}{\lambda_0}^{-1}(\lambda_j G_j).\end{aligned}$$

If $G_j \neq 0$, then j is a multiple of Δ by the definition of Δ, say $j = k\Delta$. Then by the assumption, we have $\lambda_j = \rho^k \lambda_0$ and $\lambda_{i+j-1} = \rho^k \lambda_{i-1}$. Therefore,

$$\begin{aligned}\lambda_{i+j-1}G_j &= \rho^k \lambda_{i-1}G_j \\ &= \lambda_j {\lambda_0}^{-1}\lambda_{i-1}G_j \\ &= \lambda_{i-1}{\lambda_0}^{-1}(\lambda_j G_j).\end{aligned}$$

Therefore, we have

$$\begin{aligned}\mathbf{v_i} &= (\lambda_{i-1}G_0, \lambda_i G_1, \cdots, \lambda_{i+\frac{n}{2}-1}G_{\frac{n}{2}}, \underbrace{0, \cdots, 0}_{\frac{n}{2}-1}) \\ &= \lambda_{i-1}\lambda_0^{-1}(\lambda_0 G_0, \lambda_1 G_1, \cdots, \lambda_{\frac{n}{2}}G_{\frac{n}{2}}, 0, \cdots, 0).\end{aligned}$$

By Lemma 4.2.2, the code $\Lambda(\mathscr{C})$ is cyclic. □

Theorem 4.2.3 gives a necessary and sufficient condition for the code $\Lambda(\mathscr{C})$ to be cyclic if $\mathscr{C}$ is an $[n, \frac{n}{2}]_q$ cyclic code.

We now assume that $\Lambda(\mathscr{C})$ is cyclic, i.e., the condition in Theorem 4.2.3 is met. We show that more restrictions on Λ are needed to make $\mathscr{C}$ Λ-isodual. In the following theorem, Conditions 1 and 2 are just from Theorem 4.2.3, and Condition 3 is obtained by identifying the generator polynomial of $\Lambda(\mathscr{C})$ with the generator polynomial of $\mathscr{C}^{\perp}$.

Theorem 4.2.4. *Let $\mathscr{C}$ be an $[n, \frac{n}{2}]_q$ cyclic code with the generator polynomial $G(x) = G_0 + G_1x + \cdots + G_{\frac{n}{2}}x^{\frac{n}{2}}$ and the check polynomial $H(x) = H_0 + H_1x + \cdots + H_{\frac{n}{2}}x^{\frac{n}{2}}$. Let the scalar transformation be $\Lambda = (\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$, where $\lambda_i \in \mathbb{F}_q^*$ for $0 \leq i \leq n-1$. Then $\mathscr{C}$ is Λ-isodual if and only if Λ satisfies all of the following conditions:*

1. *There exists a constant $\rho \in \mathbb{F}_q^*$ such that $(\lambda_i, \lambda_{i+\Delta}, \lambda_{i+2\Delta}, \ldots, \lambda_{i+(\frac{n}{\Delta}-1)\Delta})$ forms a geometric sequence with quotient ρ for each $0 \leq i \leq \Delta - 1$, where $\Delta = \gcd\{i : i \in \mathrm{Supp}((G_0, G_1, \ldots, G_{\frac{n}{2}}))\}$.*

2. *The polynomial $\lambda_0G_0 + \lambda_1G_1x + \cdots + \lambda_{\frac{n}{2}}G_{\frac{n}{2}}x^{\frac{n}{2}}$ divides $x^n - 1$.*

3. *$G_{\frac{n}{2}}\lambda_{\frac{n}{2}}H_{\frac{n}{2}-i} = H_0G_i\lambda_i$ for all $0 \leq i \leq \frac{n}{2}$.*

Proof. By Theorem 4.2.3, Conditions 1 and 2 are necessary and sufficient for $\Lambda(\mathscr{C})$ to be cyclic. Therefore, it remains to show that when $\Lambda(\mathscr{C})$ is cyclic, Condition 3 is necessary and sufficient for $\Lambda(\mathscr{C})$ to be the dual code of $\mathscr{C}$. Since the generator polynomial of $\Lambda(\mathscr{C})$ is $G'(x) = \lambda_{\frac{n}{2}}^{-1}G_{\frac{n}{2}}^{-1}(\lambda_0G_0 + \lambda_1G_1x + \cdots + \lambda_{\frac{n}{2}}G_{\frac{n}{2}}x^{\frac{n}{2}})$, $\Lambda(\mathscr{C}) = \mathscr{C}^{\perp}$ if and only if $G'(x) = H^*(x)$. By comparing the coefficients, we get Condition 3. $\square$

The above theorem gives a necessary and sufficient condition for a cyclic code $\mathscr{C}$ to be Λ-isodual.

The following example shows how to find a scalar transformation Λ such that a cyclic code $\mathscr{C}$ is Λ-isodual if there exists such a Λ.

Example 4.2.5. Assume $n = 8$ and $q = 5$. Then over $\mathbb{F}_5$, we have

$$x^8 - 1 = (x + 1)(x + 2)(x + 3)(x + 4)(x^2 + 2)(x^2 + 3).$$

Let $\mathscr{C}$ be an $[8, 4]_5$ cyclic code with generator polynomial

$$\begin{aligned} G(x) &= (x + 1)(x + 4)(x^2 + 2) \\ &= x^4 + x^2 + 3. \end{aligned}$$

Then

$$\begin{aligned} &\mathrm{Supp}((G_0, G_1, G_2, G_3, G_4)) \\ =&\mathrm{Supp}((3, 0, 1, 0, 1)) \\ =&\{0, 2, 4\}. \end{aligned}$$

Therefore, the parameter Δ in Theorem 4.2.3 is

$$\Delta = \gcd\{0, 2, 4\} = 2.$$

In order to find a $\Lambda = (\lambda_0, \lambda_1, \ldots, \lambda_7)$ such that $\mathscr{C}$ is Λ-isodual cyclic, by Theorem 4.2.4, the following sequences must be geometric with the same ratio ρ:

$$(\lambda_0, \lambda_2, \lambda_4, \lambda_6),$$

$$(\lambda_1, \lambda_3, \lambda_5, \lambda_7).$$

Since

$$H(x) = (x+2)(x+3)(x^2+3)$$

$$= x^4 + 4x^2 + 3.$$

Therefore, the generator polynomial $H^*(x)$ of its dual code is

$$H^*(x) = x^4 + 3x^2 + 2.$$

Since Condition 3 in Theorem 4.2.4 implies that $H^*(x)$ is a nonzero scalar multiple of the polynomial

$$G'(x) := \lambda_4 G_4 x^4 + \lambda_3 G_3 x^3 + \lambda_2 G_2 x^2 + \lambda_1 G_1 x + \lambda_0 G_0$$

$$= \lambda_4 x^4 + \lambda_2 x^2 + 3\lambda_0.$$

Without loss of generality, we assume $\lambda_4 = 1$. Then we have

$$\lambda_2 = 3,$$

$$\lambda_0 = 4.$$

Then the ratio $\rho = 2$ and we have

$$(\lambda_0, \lambda_2, \lambda_4, \lambda_6) = (4, 3, 1, 2).$$

Therefore, for any $\lambda_1 \in \mathbb{F}_q^*$, , the code $\mathscr{C}$ is Λ-isodual cyclic, where

$$\Lambda = (4, \lambda_1, 3, 2\lambda_1, 1, 4\lambda_1, 2, 3\lambda_1).$$

Actually, we can check that the generator matrix of $\mathscr{C}$ is

$$M = \begin{bmatrix} 3 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 3 & 0 & 1 & 0 & 1 \end{bmatrix},$$

and therefore the generator matrix of $\Lambda(\mathscr{C})$ is

$$M' = M \begin{bmatrix} 2 & 0 & 3 & 0 & 1 & 0 & 0 & 0 \\ 0 & 3\lambda_1 & 0 & 2\lambda_1 & 0 & 4\lambda_1 & 0 & 0 \\ 0 & 0 & 4 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & \lambda_1 & 0 & 4\lambda_1 & 0 & 3\lambda_1 \end{bmatrix}$$

$$= \begin{bmatrix} 2 & 0 & 3 & 0 & 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 2 & 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 & 4 & 0 & 3 \end{bmatrix}.$$

It is easy to check that the product of two matrices $M'M^T = 0$, where M^T is the transpose of M. Therefore, M' is also a generator matrix of $\mathscr{C}^\perp$ and hence $\mathscr{C}^\perp = \Lambda(\mathscr{C})$.

Next we study some properties for Λ-isodual cyclic codes.

Proposition 4.2.6. *If $\mathscr{C}$ is Λ-isodual cyclic code, where Λ is a scalar transformation and $\Lambda = (\lambda_0, \ldots, \lambda_{n-1})$, then*

$$(c_0(\sum_{i=0}^{n-1}\lambda_i), c_1(\sum_{i=0}^{n-1}\lambda_i), \ldots, c_{n-1}(\sum_{i=0}^{n-1}\lambda_i)) \in \mathscr{C}^\perp,$$

and

$$(\lambda_0(\sum_{i=0}^{n-1}c_i), \lambda_1(\sum_{i=0}^{n-1}c_i), \ldots, \lambda_{n-1}(\sum_{i=0}^{n-1}c_i)) \in \mathscr{C}^\perp,$$

for any $(c_0, c_1, \ldots, c_{n-1}) \in \mathscr{C}$.

Proof. For any $(c_0, c_1, \ldots, c_{n-1}) \in \mathscr{C}$, then for each $0 \leq i \leq n-1$,

$$(c_i, c_{i+1}, \ldots, c_{n-1}, c_0 \ldots, c_{i-1}) \in \mathscr{C}.$$

Since $\mathscr{C}$ is Λ-isodual, we have

$$(\lambda_0 c_i, \lambda_1 c_{i+1}, \ldots, \lambda_{n-i-1} c_{n-1}, \lambda_{n-i} c_0 \ldots, \lambda_{n-1} c_{i-1}) \in \mathscr{C}^{\perp}, \text{ for any } 0 \leq i \leq n-1. \tag{4.12}$$

Since $\mathscr{C}^{\perp}$ is linear, summing up all the above codewords, we get

$$(\lambda_0(\sum_{i=0}^{n-1} c_i), \lambda_1(\sum_{i=0}^{n-1} c_i), \ldots, \lambda_{n-1}(\sum_{i=0}^{n-1} c_i)) \in \mathscr{C}^{\perp}.$$

Since $\mathscr{C}^{\perp}$ is cyclic, by Equation (4.12), we have

$$(\lambda_{n-i} c_0, \ldots, \lambda_{n-1} c_{i-1}, \ldots, \lambda_0 c_i, \ldots, \lambda_{n-i-1} c_{n-1}) \in \mathscr{C}^{\perp}, \text{ for any } 0 \leq i \leq n-1.$$

Then summing up all the codewords above, we have

$$(c_0(\sum_{i=0}^{n-1} \lambda_i), c_1(\sum_{i=0}^{n-1} \lambda_i), \ldots, c_{n-1}(\sum_{i=0}^{n-1} \lambda_i)) \in \mathscr{C}^{\perp}.$$

□

The two conclusions in this proposition are important in the following theorem.

Theorem 4.2.7. *Let $\Lambda = (\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$ be a scalar transformation. If $\sum_{i=0}^{n-1} \lambda_i \neq 0$, then Λ-isodual cyclic codes are self-dual cyclic codes. Furthermore, if $\sum_{i=0}^{n-1} \lambda_i \neq 0$, no Λ-isodual cyclic code exists over $\mathbb{F}_q$ with q odd.*

Proof. If $\sum_{i=0}^{n-1} \lambda_i \neq 0$, then by Proposition 4.2.6, $\mathscr{C}$ is isodual cyclic only if $\mathscr{C}$ is self-dual cyclic. Therefore, the second statement follows since no self-dual cyclic codes exist over $\mathbb{F}_q$ with q odd. □

As a consequence of the above theorem, we may as well assume that $\sum_{i=0}^{n-1} \lambda_i = 0$.

Therefore, it is natural to consider a special scalar transformation. Let $\lambda \neq 1$ be an element in $\mathbb{F}_q^*$ and let its order be r with $r|n$. Let the scalar transformation $\Lambda = (1, \lambda, \lambda^2, \ldots, \lambda^{n-1})$. Since $r|n$, we have $\lambda^n = 1$ and hence

$$\begin{aligned}\sum_{i=0}^{n-1} \lambda^i &= \frac{1-\lambda^n}{1-\lambda} \\ &= 0.\end{aligned}$$

Furthermore, by Theorem 4.2.3, for any cyclic code $\mathscr{C}$ with generator polynomial $G(x)$, the code $\Lambda(\mathscr{C})$ is always cyclic with generator polynomial $\lambda^{-\frac{n}{2}} G(\lambda x)$. Therefore, $\mathscr{C}$ is $(1, \lambda, \lambda^2, \ldots, \lambda^{n-1})$-isodual if and only if $H^*(x) = \lambda^{-\frac{n}{2}} G(\lambda x)$.

4.3 $(1, \lambda, \lambda^2, \ldots, \lambda^{n-1})$-isodual cyclic codes

Throughout this section, the scalar transformation Λ *is fixed as* $(1, \lambda, \lambda^2, \ldots, \lambda^{n-1})$ *and order* r *of* λ *divides* n*, where the nonzero element* $\lambda \neq 1$. In order to describe the generator polynomial of a Λ-isodual cyclic code, we focus on the factorization of $x^{\bar{n}} - 1$ first.

4.3.1 Factorization of $x^{\bar{n}} - 1$

It is easy to observe that, for any irreducible polynomial $f(x)$ dividing $x^{\bar{n}} - 1$, the polynomial $f(\lambda x)$ is also irreducible and divides

$$(\lambda x)^{\bar{n}} - 1 = \lambda^{\bar{n}} x^{\bar{n}} - 1.$$

Since for any $\lambda \in \mathbb{F}_q^*$, its order r divides $q - 1 = p^m - 1$, we have $\gcd(r, p) = 1$. Moreover, because $r|n$ and $n = p^a \bar{n}$, we have $r|\bar{n}$ and hence $\lambda^{\bar{n}} = 1$. Therefore, the

polynomial $f(\lambda x)$ divides $x^{\bar{n}} - 1$. Next we define the following equivalence relation $\bowtie$ on all the distinct irreducible factors of $x^{\bar{n}} - 1$.

Definition 4.3.1. *Let $f_{i_1}(x)$ and $f_{i_2}(x)$ be two irreducible factors of $x^{\bar{n}} - 1$. Define $f_{i_1}(x) \bowtie f_{i_2}(x)$ if and only if there exists an integer j such that $f_{i_2}(x) = \delta f_{i_1}(\lambda^j x)$ for some $\delta \in \mathbb{F}_q^*$.*

Then the equivalence relation $\bowtie$ partitions all the irreducible factors of $x^{\bar{n}} - 1$ into equivalence classes. We call each equivalence class (or simply class) an orbit *of $\bowtie$ (because each class can be generated by one polynomial when replacing x by λx repeatedly).*

Suppose there are k equivalence classes and we arrange the polynomials in each class in the following order: $f(x), f(\lambda x), \ldots, f(\lambda^i x), \ldots$ (in the rest of the chapter, we will simply refer to the way of arrangement as λ-*ascending order*).

$$\begin{aligned} x^{\bar{n}} - 1 =& \delta[f_{1,0}(x)f_{1,1}(x)f_{1,2}(x)\cdots f_{1,N_1-1}(x)] \\ & \times [f_{2,0}(x)f_{2,1}(x)f_{2,2}(x)\cdots f_{2,N_2-1}(x)]\cdots \\ & \times [f_{k,0}(x)f_{k,1}(x)f_{k,2}(x)\cdots f_{k,N_k-1}(x)], \end{aligned} \tag{4.13}$$

where $\delta \in \mathbb{F}_q^*$ and for each $1 \le i \le k$ and $0 \le j \le N_i - 2$, $f_{i,j+1}(x) = f_{i,j}(\lambda x)$ and $f_{i,0}(x) = \delta_i f_{i,N_i-1}(\lambda x)$ for some $\delta_i \in \mathbb{F}_q^*$.

Throughout the rest of this chapter, we shall denote by $f_{i,j}(x)$ the j-th irreducible polynomial in Class i, and denote by N_i the number of irreducible polynomials in Class i.

Next we study the reciprocal polynomials of the polynomials in the equivalence classes.

By [10], for any $f_{i_1,j_1}(x)$, its reciprocal polynomial is also a factor of $x^{\bar{n}}-1$. Assume the reciprocal polynomial of $f_{i_1,j_1}(x)$ is a nonzero scalar multiple of $f_{i_2,j_2}(x)$. Then we have the following proposition.

Proposition 4.3.2. *Let $f_{i_1,j_1}(x)$ and $f_{i_2,j_2}(x)$ be factors of $x^{\bar{n}}-1$, as in (4.13). If $f_{i_1,j_1}(x) = \delta f^*_{i_2,j_2}(x)$ for some $\delta \in \mathbb{F}_q^*$, then $N_{i_1} = N_{i_2}$ and for any $0 \leq l \leq N_{i_1}$, there exists a unit $\delta_l \in \mathbb{F}_q^*$ depending on l such that $f_{i_1,j_1+l}(x) = \delta_l f^*_{i_2,j_2-l}(x)$, where the subscripts $j_1 + l$ and $j_2 - l$ are taken modulo N_{i_1}.*

Proof. Since we arrange the polynomials in the equivalence classes in λ-ascending order, we have

$$f_{i_1,j_1+l}(x) = \delta'_l f_{i_1,j_1}(\lambda^l x), \tag{4.14}$$

where, $\delta'_l \in \mathbb{F}_q^*$ and the subscript j_1+l is taken modulo N_{i_1}. Since $f_{i_1,j_1}(x) = \delta f^*_{i_2,j_2}(x)$ for some $\delta \in \mathbb{F}_q^*$, we have

$$f_{i_1,j_1}(x) = \delta''_1 x^{d_2} f_{i_2,j_2}(x^{-1}), \tag{4.15}$$

for some $\delta''_1 \in \mathbb{F}_q^*$ and $d_2 = \deg(f_{i_2,j_2}(x))$. Replacing x by $\lambda^l x$ in (4.15), we have

$$\begin{aligned} f_{i_1,j_1}(\lambda^l x) &= \delta''_1 (\lambda^l x)^{d_2} f_{i_2,j_2}((\lambda^l x)^{-1}) \\ &= \delta''_1 \lambda^{ld_2} x^{d_2} f_{i_2,j_2}(\lambda^{-l} x^{-1}) \\ &= \delta''_2 \lambda^{ld_2} x^{d_2} f_{i_2,j_2-l}(x^{-1}) \\ &= \delta''_3 f^*_{i_2,j_2-l}(x), \end{aligned} \tag{4.16}$$

where $\delta''_i \in \mathbb{F}_q^*$ for $i = 1, 2$ and 3 and the subscript $j_2 - l$ is taken modulo N_{i_2}.

By Equations (4.14) and (4.16), we have

$$f_{i_1,j_1+l}(x) = \delta_l f^*_{i_2,j_2-l}(x), \tag{4.17}$$

where, $\delta_l = \delta_l'\delta_3''$. Next we show that $N_{i_1} = N_{i_2}$. Since each equivalence class is cyclic in λ-ascending order, without loss of generality, we can assume that $f_{i_1,0}(x) = \delta'' f^*_{i_2,N_{i_2}-1}(x)$ for some $\delta'' \in \mathbb{F}_q^*$. Then by (4.17), for any $0 \leq l \leq N_{i_1}$

$$f_{i_1,l}(x) = \delta_l f_{i_2,N_{i_2}-1-l}(x).$$

Then

$$f_{i_1,0}(x) = \delta_0 f_{i_2,N_{i_2}-1}(x),$$

and

$$f_{i_1,0}(x) = f_{i_1,N_{i_1}}(x) = \delta_{N_{i_1}} f_{i_2,N_{i_2}-N_{i_1}-1}(x),$$

where the subscript $N_{i_2} - N_{i_1} - 1$ is taken modulo N_{i_2}. Then $f_{i_2,N_{i_2}-1}(x)$ is a nonzero scalar multiple of $f_{i_2,N_{i_2}-N_{i_1}-1}(x)$. Since $\gcd(\bar{n}, q) = 1$, all the irreducible factors in Equation (4.13) are distinct. Therefore, we have

$$N_{i_2} - 1 \equiv N_{i_2} - N_{i_1} - 1 \pmod{N_{i_2}}.$$

Then we have

$$N_{i_1} \equiv 0 \pmod{N_{i_2}}.$$

Similarly, we have

$$N_{i_2} \equiv 0 \pmod{N_{i_1}}.$$

Therefore, we have $N_{i_1} = N_{i_2}$. □

With the above proposition, we can classify all the equivalence classes. To simplify the description, we need the following definitions before we give the lemma.

Definition 4.3.3. *Let $f(x)$ be a polynomial over $\mathbb{F}_q$. Then $f(x)$ is said to be* quasi-self-reciprocal *if $f(x)$ is a nonzero scalar multiple of its reciprocal polynomial, i.e., $f(x) = \delta f^*(x)$ for some $\delta \in \mathbb{F}_q^*$.*

Definition 4.3.4. *Let $f(x)$ and $g(x)$ be two polynomials over $\mathbb{F}_q$. Then $f(x)$ and $g(x)$ are said to be a* quasi-reciprocal pair *if $f^*(x)$ is a nonzero scalar multiple $g(x)$, i.e., $g(x) = \delta f^*(x)$ for some $\delta \in \mathbb{F}_q^*$, and $g(x)$ is said to be a* quasi-reciprocal *polynomial of $f(x)$.*

Lemma 4.3.5. *Let $x^{\bar{n}} - 1$ factorize as in* (4.13)*. There are four types of equivalence classes:*

Type I class: If Class i contains a quasi-self-reciprocal polynomial and N_i is odd, then there is only one quasi-self-reciprocal polynomial in this class and after suitable cyclic shifts on the class, we have $f_{i,0}(x)$ is the quasi-self-reciprocal polynomial and

$$f_{i,j}(x) = \delta_j f^*_{i,N_i-j}(x), \text{ for all } 1 \leq j \leq N_i - 1,$$

where, $\delta_j \in \mathbb{F}_q^*$.

Type II class: If Class i contains a quasi-self-reciprocal polynomial and N_i is even, then there are only two quasi-self-reciprocal polynomials in this class and after suitable cyclic shifts on the class, we have $f_{i,0}(x)$ and $f_{i,\frac{N_i}{2}}(x)$ are the two quasi-self-reciprocal polynomials and

$$f_{i,j}(x) = \delta_j f^*_{i,N_i-j}(x), \text{ for all } 1 \leq j \leq N_i - 1,$$

where, $\delta_j \in \mathbb{F}_q^*$.

Type III class: *If Class i contains no quasi-self-reciprocal polynomial and Class i contains a quasi-reciprocal pair. Then N_i is even and after suitable cyclic shifts on the class, we have*

$$f_{i,j}(x) = \delta_j f^*_{i,N_i-1-j}(x), \text{ for all } 0 \le j \le N_i - 1,$$

where, $\delta_j \in \mathbb{F}_q^*$.

Type IV class: *If Class i_1 contains a polynomial whose quasi-reciprocal polynomial is in Class i_2 with $i_1 \neq i_2$, Then we have $N_{i_1} = N_{i_2} := N$ and after suitable cyclic shifts on both classes, we have $f_{i_1,0}(x)$ and $f_{i_2,N-1}(x)$ form a quasi-reciprocal pair and*

$$f_{i_1,j}(x) = \delta_j f^*_{i_2,N-1-j}(x), \text{ for all } 0 \le j \le N - 1,$$

where, $\delta_j \in \mathbb{F}_q^*$.

Proof. The statements about Type I, II and IV classes are straight forward by Proposition 4.3.2. We need to show the statement about Type III class is true. Without loss of generality, we can assume that Class i contains $f_{i,0}(x)$ and $f_{i,b}(x)$ for some $1 \le b \le N_i - 1$ as a quasi-reciprocal pair. Then by Proposition 4.3.2, we have

$$f_{i,j}(x) = \delta'_j f_{i,b-j}(x),$$

where, $0 \le j \le N_i - 1$ and the subscript $(b-j)$'s are taken modulo N_i. Since there is no quasi-self-reciprocal polynomial in Class i, we have b is odd and $b + N_i$ is odd (otherwise, $f_{i,\frac{b}{2}}(x)$ or $f_{i,\frac{N_i+b}{2}}(x)$ is quasi-self-reciprocal). Then we have N_i is even. Furthermore, cyclic shifting Class i such that the polynomial $f_{i,\frac{b+1}{2}}(x)$ is in the first position of the class and hence its quasi-reciprocal polynomial $f_{i,\frac{b-1}{2}}(x)$ is in the last position of the class. By Proposition 4.3.2 again, we obtain the conclusion. □

Note that in the above theorem, the Type IV Classes i_1 and i_2 form a quasi-reciprocal pair as class. Then Type IV classes always appear as pairs. Also note that cyclic shifts on the class do not change its type. Therefore, there are 4 types of equivalence classes called Type I class, Type II class, Type III class and Type IV class, respectively. For convenience, we call the form of the arrangement of the polynomials in the classes given in the above lemma the *standard form*. When we mention the types of classes, without specifying, we shall refer to the types of classes in standard form.

Then we can rearrange the classes in (4.13) by their types in standard form as follows:

$$\begin{aligned} x^{\bar{n}} - 1 =& \delta[f_{1,0}(x)\cdots f_{1,N_1-1}(x)]\cdots[f_{s_1,0}(x)\cdots f_{s_1,N_{s_1}-1}(x)] \\ & \times [f'_{1,0}(x)\cdots f'_{1,N'_1-1}(x)]\cdots[f'_{s_2,0}(x)\cdots f'_{s_2,N'_{s_2}-1}(x)] \\ & \times [g_{1,0}(x)\cdots g_{1,L_1-1}(x)]\cdots[g_{s_3,0}(x)\cdots g_{s_3,L_{s_3}-1}(x)] \\ & \times [h_{1,0}(x)\cdots h_{1,M_1-1}(x)][h^*_{1,M_1-1}(x)\cdots h^*_{1,0}(x)]\cdots \\ & \times [h_{t,0}(x)\cdots h_{t,M_t-1}(x)][h^*_{t,M_t-1}(x)\cdots h^*_{t,0}(x)], \end{aligned} \tag{4.18}$$

where $\delta \in \mathbb{F}_q^*$, the polynomials in the same bracket form a class in λ-ascending order. Furthermore, in the above equation $f_{i,j}(x)$ for $1 \le i \le s_1$ and $0 \le j \le N_i - 1$ form Type I classes, $f'_{i,j}(x)$ for $1 \le i \le s_2$ and $0 \le j \le N'_i - 1$ form Type II classes, $g_{i,j}(x)$ for $1 \le i \le s_3$ and $0 \le j \le L_i - 1$ form Type III classes, and the rest polynomials form Type IV classes. Using this rearragement, we can describe the generator polynomial of a $(1, \lambda, \lambda^2, \ldots)$-isodual cyclic code in the following subsection.

4.3.2 Generator polynomials of $(1, \lambda, \lambda^2, \ldots)$-isodual cyclic codes

Theorem 4.3.6. *Let $\mathscr{C}$ be an $[n, \frac{n}{2}]$ cyclic code over $\mathbb{F}_q$ and let nonzero element $\lambda \neq 1$ be of order r with $r|n$. Let $x^{\bar{n}} - 1$ factorize as in (4.18) and let the generator polynomial of $\mathscr{C}$ be*

$$\begin{aligned} G(x) =& \delta[f_{1,0}(x)^{\alpha_{1,0}} \cdots f_{1,N_1-1}(x)^{\alpha_{1,N_1-1}}] \cdots [f_{s_1,0}(x)^{\alpha_{s_1,0}} \cdots f_{s_1,N_{s_1}-1}(x)^{\alpha_{s_1,N_{s_1}-1}}] \\ & \times [f'_{1,0}(x)^{\alpha'_{1,0}} \cdots f'_{1,N'_1-1}(x)^{\alpha'_{1,N'_1-1}}] \cdots [f'_{s_2,0}(x)^{\alpha'_{s_2,0}} \cdots f'_{s_2,N'_{s_2}-1}(x)^{\alpha'_{s_2,N'_{s_2}-1}}] \\ & \times [g_{1,0}(x)^{\alpha''_{1,0}} \cdots g_{1,L_1-1}(x)^{\alpha''_{1,L_1-1}}] \cdots [g_{s_3,0}(x)^{\alpha''_{s_3,0}} \cdots g_{s_3,L_{s_3}-1}(x)^{\alpha''_{s_3,L_{s_3}-1}}] \\ & \times [h_{1,0}(x)^{\beta_{1,0}} \cdots h_{1,M_1-1}(x)^{\beta_{1,M_1-1}}][h^*_{1,M_1-1}(x)^{\gamma_{1,0}} \cdots h^*_{1,0}(x)^{\gamma_{1,M_1-1}}] \cdots \\ & \times [h_{t,0}(x)^{\beta_{t,0}} \cdots h_{t,M_t-1}(x)^{\beta_{t,M_t-1}}][h^*_{t,M_t-1}(x)^{\gamma_{t,0}} \cdots h^*_{t,0}(x)^{\gamma_{t,M_t-1}}], \end{aligned} \tag{4.19}$$

where $\delta \in \mathbb{F}_q^*$ such that $G(x)$ is monic, $0 \leq \alpha_{i,j} \leq p^a$ for $1 \leq i \leq s_1$ and $0 \leq j \leq N_i - 1$, $0 \leq \alpha'_{i,j} \leq p^a$ for $1 \leq i \leq s_2$ and $0 \leq j \leq N'_i - 1$, $0 \leq \alpha''_{i,j} \leq p^a$ for $1 \leq i \leq s_3$ and $0 \leq j \leq L_i - 1$, $0 \leq \beta_{i,j}, \gamma_{i,j} \leq p^a$ for $1 \leq i \leq t$ and $0 \leq j \leq M_i$. Then $\mathscr{C}$ is $(1, \lambda, \lambda^2, \ldots, \lambda^{n-1})$-isodual if and only if

$$\begin{cases} \alpha_{i,j} + \alpha_{i,N_i-1-j} = p^a, \text{ for } 1 \leq i \leq s_1 \text{ and } 0 \leq j \leq N_i - 1, \text{in particular, } \alpha_{i,\frac{N_i-1}{2}} = p^a/2, \\ \alpha'_{i,j} + \alpha'_{i,N'_i-1-j} = p^a, \text{ for } 1 \leq i \leq s_2 \text{ and } 0 \leq j \leq N'_i - 1, \\ \alpha''_{i,j} + \alpha''_{i,L_i-2-j} = p^a, \text{ for } 1 \leq i \leq s_3 \text{ and } 0 \leq j \leq L_i - 2, \\ \alpha''_{i,L_i-1} = p^a/2, \text{ for } 1 \leq i \leq s_3, \\ \beta_{i,j} + \gamma_{i,M_i-2-j} = p^a, \text{ for } 1 \leq i \leq t \text{ and } 0 \leq j \leq M_i - 2, \\ \beta_{i,M_i-1} + \gamma_{i,M_i-1} = p^a, \text{ for } 1 \leq i \leq t. \end{cases} \tag{4.20}$$

Proof. Let $G(x)$ be the generator polynomial of the form in (4.19). Then the parity-check polynomial is

$$\begin{aligned}
H(x) =&\delta'[f_{1,0}(x)^{p^a-\alpha_{1,0}}\cdots f_{1,N_1-1}(x)^{p^a-\alpha_{1,N_1-1}}]\cdots[f_{s_1,0}(x)^{p^a-\alpha_{s_1,0}}\cdots f_{s_1,N_{s_1}-1}(x)^{p^a-\alpha_{s_1,N_{s_1}-1}}]\\
&\times[f'_{1,0}(x)^{p^a-\alpha'_{1,0}}\cdots f'_{1,N'_1-1}(x)^{p^a-\alpha'_{1,N'_1-1}}]\cdots[f'_{s_2,0}(x)^{p^a-\alpha'_{s_2,0}}\cdots f'_{s_2,N'_{s_2}-1}(x)^{p^a-\alpha'_{s_2,N'_{s_2}-1}}]\\
&\times[g_{1,0}(x)^{p^a-\alpha''_{1,0}}\cdots g_{1,L_1-1}(x)^{p^a-\alpha''_{1,L_1-1}}]\cdots[g_{s_3,0}(x)^{p^a-\alpha''_{s_3,0}}\cdots g_{s_3,L_{s_3}-1}(x)^{p^a-\alpha''_{s_3,L_{s_3}-1}}]\\
&\times[h_{1,0}(x)^{p^a-\beta_{1,0}}\cdots h_{1,M_1-1}(x)^{p^a-\beta_{1,M_1-1}}][h^*_{1,M_1-1}(x)^{p^a-\gamma_{1,0}}\cdots h^*_{1,0}(x)^{p^a-\gamma_{1,M_1-1}}]\cdots\\
&\times[h_{t,0}(x)^{p^a-\beta_{t,0}}\cdots h_{t,M_t-1}(x)^{p^a-\beta_{t,M_t-1}}][h^*_{t,M_t-1}(x)^{p^a-\gamma_{t,0}}\cdots h^*_{t,0}(x)^{p^a-\gamma_{t,M_t-1}}],
\end{aligned}$$

where $\delta' \in \mathbb{F}_q^*$ such that $H(x)$ is monic. Moreover, the generator polynomial of $\Lambda(\mathscr{C})$ is

$$
\begin{aligned}
&G'(x)\\
=&\lambda^{-\frac{n}{2}}G(\lambda x)\\
=&\delta''[f_{1,0}(x)^{\alpha_{1,N_1-1}}f_{1,1}(x)^{\alpha_{1,0}}\cdots f_{1,N_1-1}(x)^{\alpha_{1,N_1-2}}]\\
&\cdots[f_{s_1,0}(x)^{\alpha_{s_1,N_{s_1}-1}}f_{s_1,1}(x)^{\alpha_{s_1,0}}\cdots f_{s_1,N_{s_1}-1}(x)^{\alpha_{s_1,N_{s_1}-2}}]\\
\times&[f'_{1,0}(x)^{\alpha'_{1,N'_1-1}}f'_{1,1}(x)^{\alpha'_{1,0}}\cdots f'_{1,N'_1-1}(x)^{\alpha'_{1,N'_1-2}}]\\
&\cdots[f'_{s_2,0}(x)^{\alpha'_{s_2,N'_{s_2}-1}}f'_{s_2,1}(x)^{\alpha'_{s_2,0}}\cdots f'_{s_2,N'_{s_2}-1}(x)^{\alpha_{s_2,N'_{s_2}-2}}]\\
\times&[g_{1,0}(x)^{\alpha''_{1,L_1-1}}g_{1,1}(x)^{\alpha''_{1,0}}\cdots g_{1,L_1-1}(x)^{\alpha''_{1,L_1-2}}]\\
&\cdots[g_{s_3,0}(x)^{\alpha''_{s_3,L_{s_3}-1}}g_{s_3,1}(x)^{\alpha''_{s_3,0}}\cdots g_{s_3,L_{s_3}-2}(x)^{\alpha''_{s_3,L_{s_3}-1}}]\\
\times&[h_{1,0}(x)^{\beta_{1,M_1-1}}h_{1,1}(x)^{\beta_{1,0}}\cdots h_{1,M_1-1}(x)^{\beta_{1,M_1-2}}]\\
&\times[h^*_{1,M_1-1}(x)^{\gamma_{1,M_1-1}}h^*_{1,0}(x)^{\gamma_{1,0}}\cdots h^*_{1,0}(x)^{\gamma_{1,M_1-2}}]\cdots\\
\times&[h_{t,0}(x)^{\beta_{t,M_t-1}}h_{t,1}(x)^{\beta_{t,0}}\cdots h_{t,M_t-1}(x)^{\beta_{t,M_t-2}}(x)]\\
&\times[h^*_{t,M_t-1}(x)^{\gamma_{t,M_t-1}}h^*_{t,M_t-2}(x)^{\gamma_{t,0}}\cdots h^*_{t,0}(x)^{\gamma_{t,M_t-2}}],
\end{aligned}
$$

where $\delta'' \in \mathbb{F}_q^*$ such that $G'(x)$ is monic.

Furthermore, by Lemma 4.3.5, the generator polynomial of $\mathscr{C}^{\perp}$ is

$$
\begin{aligned}
&H^*(x)\\
=&\delta'''[f_{1,0}(x)^{p^a-\alpha_{1,0}} f_{1,1}(x)^{p^a-\alpha_{1,N_1-1}} \cdots f_{1,N_1-1}(x)^{p^a-\alpha_{1,1}}]\\
&\cdots [f_{s_1,0}(x)^{p^a-\alpha_{s_1,0}} f_{s_1,1}(x)^{p^a-\alpha_{s_1,N_{s_1}-1}} \cdots f_{s_1,1}(x)^{p^a-\alpha_{s_1,1}}]\\
\times&[f'_{1,0}(x)^{p^a-\alpha'_{1,0}} f'_{1,1}(x)^{p^a-\alpha'_{1,N'_1-1}} \cdots f'_{1,N'_1/2}(x)^{p^a-\alpha'_{1,N'_1/2}} \cdots f'_{1,N'_1-1}(x)^{p^a-\alpha'_{1,1}}]\\
&\cdots [f'_{s_2,0}(x)^{p^a-\alpha'_{s_2,0}} f'_{s_2,1}(x)^{p^a-\alpha'_{s_2,N'_{s_2}-1}} \cdots f'_{s_2,N'_{s_2}/2}(x)^{p^a-\alpha'_{s_2,N'_{s_2}/2}} \cdots f'_{s_2,N'_{s_2}-1}(x)^{p^a-\alpha'_{s_2,1}}]\\
\times&[g_{1,0}(x)^{p^a-\alpha''_{1,L_1-1}} g_{1,1}(x)^{p^a-\alpha''_{1,L_1-2}} \cdots g_{1,L_1-1}(x)^{p^a-\alpha''_{1,0}}]\\
&\cdots [g_{s_3,0}(x)^{p^a-\alpha''_{s_3,L_{s_s}-1}} \cdots g_{s_3,L_{s_3}-1}(x)^{p^a-\alpha''_{s_3,0}}]\\
\times&[h_{1,0}(x)^{p^a-\gamma_{1,M_1-1}} \cdots h_{1,M_1-1}(x)^{p^a-\gamma_{1,0}}][h^*_{1,M_1-1}(x)^{p^a-\beta_{1,M_1-1}} \cdots h^*_{1,0}(x)^{p^a-\beta_{1,0}}] \cdots\\
\times&[h_{t,0}(x)^{p^a-\gamma_{t,M_t-1}} \cdots h_{t,M_t-1}(x)^{p^a-\gamma_{t,0}}][h^*_{t,M_t-1}(x)^{p^a-\beta_{t,M_t-1}} \cdots h^*_{t,0}(x)^{p^a-\beta_{t,0}}],
\end{aligned}
$$

where $\delta''' \in \mathbb{F}_q^*$ such that $H^*(x)$ is monic.

Therefore, $\mathscr{C}^{\perp} = \Lambda(\mathscr{C})$ if and only if $G'(x) = H^*(x)$, i.e., (4.20) holds. □

Using this result, we discuss the existence of $(1, \lambda, \lambda^2, \ldots)$-isodual cyclic code in the following subsection.

4.3.3 Existence of $(1, \lambda, \lambda^2, \ldots)$-isodual cyclic codes

Note that the condition in (4.20) can be always satisfied if $p = 2$. However, if p is odd, then the condition in (4.20) is satisfied if and only if there is no Type I class or Type III class in the factorization of $x^{\bar{n}} - 1$. Therefore, we immediately give the following corollary.

Corollary 4.3.7. *Let q be odd. Let the nonzero element $\lambda \neq 1$ be of order r with $r|n$. Let $\Lambda = (1, \lambda, \ldots, \lambda^{n-1})$ be a scalar transformation. Then there exists a Λ-isodual*

cyclic code if and only if there is no Type I class or Type III class in the factorization of $x^{\bar{n}} - 1$.

Next we give a more straight forward necessary and sufficient condition on the existence of $[n, \frac{n}{2}]_q$ $(1, \lambda, \ldots, \lambda^{n-1})$-isodual cyclic codes, where q is odd.

Theorem 4.3.8. *Let q be odd. Let the nonzero element $\lambda \neq 1$ be of order r with $r|n$. Let $\Lambda = (1, \lambda, \ldots, \lambda^{n-1})$ be a scalar transformation. Then there exists a Λ-isodual cyclic code if and only if $\frac{\bar{n}}{r}$ is odd and r is even.*

Proof. Since $x - 1$ divides $x^{\bar{n}} - 1$, there is a class in λ-ascending order:

$$(x - 1, \lambda x - 1, \ldots, \lambda^{r-1} x - 1).$$

Since $x - 1$ is a self-reciprocal polynomial over $\mathbb{F}_q$, the above class is Type I if r is odd and Type II if r is even. By Corollary 4.3.7, r must be even for the existence of the Λ-isodual codes. In the rest of the proof, we always assume that r is even and therefore $\lambda^{\frac{r}{2}} = -1$.

We assume that $\frac{\bar{n}}{r}$ is even. Then

$$\lambda^{\frac{\bar{n}}{2}} = \lambda^{\frac{r}{2}\frac{\bar{n}}{r}} = (-1)^{\frac{\bar{n}}{r}} = 1.$$

Therefore, we have $y - \lambda$ divides $y^{\frac{\bar{n}}{2}} - 1$. Replacing y by x^2, we have $x^2 - \lambda$ divides $x^{\bar{n}} - 1$.

1. If $x^2 - \lambda$ is irreducible, then we have the following class in the factorization of $x^{\bar{n}} - 1$:

$$(x^2 - \lambda, \lambda^2 x^2 - \lambda, \ldots, \lambda^{2(\frac{r}{2}-1)} x^2 - \lambda). \tag{4.21}$$

In order to determine the type of the above class, we need to determine the existence of quasi-self-reciprocal polynomial in this class. Assume that $\lambda^{2j}x^2-\lambda$ is a quasi-self-reciprocal polynomial in the class, with $0 \leq j \leq \frac{r}{2}-1$. Since its reciprocal polynomial is $x^2-\lambda^{2j-1}$, we have

$$\lambda^{1-2j} = \lambda^{2j-1},$$

$$\lambda^{2(2j-1)} = 1,$$

which implies the order r divides $2(2j-1)$. If there is a quasi-self-reciprocal polynomial in this class, then r must be oddly even. If $r \geq 6$, then $\lambda^{\frac{r}{2}+1}x^2-\lambda$ is a quasi-self-reciprocal polynomial. If $r=2$, then $\lambda=-1$ and the class only contains one polynomial x^2+1 which is quasi-self-reciprocal. Since there are $\frac{r}{2}$ polynomials in the class in (4.21) for any oddly even r, the class is a Type I class. Furthermore, if r is doubly even, there is no quasi-self-reciprocal polynomial since r never divides $2(2j-1)$. We observe that for any j, we have $(\lambda^j x)^2-\lambda$ and $(\lambda^{1-j}x)^2-\lambda$ form a quasi-reciprocal pair. Therefore, if r is doubly even, the class in (4.21) is a Type III class. Therefore, by Corollary 4.3.7, if $x^2-\lambda$ is irreducible, there is no Λ-isodual cyclic code.

2. If $x^2-\lambda$ is reducible, then we write

$$x^2-\lambda = (x+\kappa_1)(x+\kappa_2),$$

where

$$\begin{cases} \kappa_1+\kappa_2 = 0, \\ \kappa_1\kappa_2 = -\lambda. \end{cases}$$

Therefore, we have $\kappa_1^2 = \kappa_2^2 = \lambda$. Consider the following class

$$(x + \kappa_1, \lambda x + \kappa_1, \ldots, \lambda^{r-1} x + \kappa_1). \tag{4.22}$$

It is easy to check that $x+\kappa_1$ and $\lambda x+\kappa_1$ form a quasi-reciprocal pair. Furthermore, for any $0 \leq j \leq r-1$, the reciprocal polynomial of $\lambda^j x + \kappa_1$ is $x + \lambda^j \kappa_1^{-1}$. Since r never divides $2j-1$ for any j, we have

$$\lambda^{2j-1} \neq 1,$$
$$\lambda^j \neq \lambda^{1-j},$$

which means there is no quasi-self-reciprocal polynomial in the class. Therefore, in this case, the class in (4.22) is a Type III class. Therefore, if $x^2-\lambda$ is reducible, there exists no Λ-isodual cyclic code.

As a conclusion, there is no Λ-isodual cyclic code if $\frac{\bar{n}}{r}$ is even.

Next we assume $\frac{\bar{n}}{r}$ is odd. Write

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

Let $\mathscr{C}$ be an $[n, \frac{n}{2}]_q$ with generator polynomial $G(x) = x^{\frac{\bar{n}}{2}} + 1$. Then

$$\begin{aligned} G(\lambda x) &= (\lambda x)^{\frac{\bar{n}}{2}} + 1 \\ &= \lambda^{\frac{\bar{n}}{2}} x^{\frac{\bar{n}}{2}} + 1 \\ &= \lambda^{\frac{r}{2}\frac{\bar{n}}{r}} x^{\frac{\bar{n}}{2}} + 1 \\ &= (-1)^{\frac{\bar{n}}{r}} x^{\frac{\bar{n}}{2}} + 1 \\ &= -(x^{\frac{\bar{n}}{2}} - 1), \end{aligned}$$

because $\frac{\bar{n}}{r}$ is odd. Then $\Lambda(\mathscr{C})$ is a cyclic code with generator polynomial $(x^{\frac{\bar{n}}{2}}-1)$ which is exactly the dual code of $\mathscr{C}$. Therefore, $\mathscr{C}$ is a Λ-isodual cyclic code.

As a consequence, there exists a Λ-isodual cyclic code if and only if $\frac{\bar{n}}{r}$ is odd and r is even. □

The following example gives a $(1, \lambda, \ldots, \lambda^{n-1})$-isodual cyclic code with p even.

Example 4.3.9. Let $q = 4$ and let $\lambda = \omega$ where $\omega^2 + \omega + 1 = 0$ in $\mathbb{F}_4$. Then the order r of λ is 3. Let $n = 18$. Then

$$x^{18} - 1 = (x+1)^2(x+\omega)^2(x+\omega^2)^2(x^3+\omega)^2(x^3+\omega^2)^2.$$

Then we have

$$(x+1) \bowtie (\omega x+1) = \omega(x+\omega^2),$$
$$(\omega x+1) \bowtie (\omega^2 x+1) = \omega^2(x+\omega),$$

and $x+1$ is self-reciprocal polynomial. Then the class

$$(x+1, \omega x+1, \omega^2 x+1)$$

is a Type I class in standard form. Similarly, the class $(x^3+\omega)$ and the class $(x^3+\omega^2)$ are Type IV classes in standard form and they form a quasi-reciprocal pair as class. Therefore, we can write

$$x^{18} - 1 = [(x+1)(\omega x+1)(\omega^2 x+1)]^2[x^3+\omega]^2[x^3+\omega^2]^2.$$

By Theorem 4.3.6, the generator polynomial of an $[18, 9]_4$ $(1, \omega, \ldots, \omega^{n-1})$-isodual cyclic code can be chosen as

$$G(x) = \delta(x+1)^{\alpha_1}(\omega x+1)(\omega^2 x+1)^{2-\alpha_1}(x^3+\omega)^{\alpha_2}(x^3+\omega^2)^{2-\alpha_2},$$

where α_1 and α_2 are integers 0, 1 or 2 and $\delta \in \mathbb{F}_q$ depends on α_1 and α_2 such that $G(x)$ is monic.

The following example gives a $(1, \lambda, \ldots, \lambda^{n-1})$-isodual cyclic code with p odd.

Example 4.3.10. Let $q = p^m$ with p odd and let ω be a primitive element in $\mathbb{F}_q$, i.e. the order of ω is $q-1$. Then $\omega^{\frac{q-1}{2}} = -1$. Let $n = q-1$. Then we can write the factorization of $x^n - 1$ in the following ω-ascending order.

$$\begin{aligned} x^n - 1 &= \prod_{i=0}^{n-1}(x - \omega^i) \\ &= -[(x-1)(\omega x - 1)(\omega^2 x - 1)\cdots(\omega^{\frac{n}{2}-1}x - 1)(-x-1)(\omega^{\frac{n}{2}+1}x - 1)\cdots(\omega^{n-1}x - 1)]. \end{aligned}$$

Since only the polynomials $(x-1)$ and $(-x-1)$ are quasi-self-reciprocal, all the polynomials form a class of Type II in standard form. Let $\mathscr{C}$ be a $(1, \omega, \ldots, \omega^{n-1})$-isodual cyclic code. By Theorem 4.3.6, the generator polynomial of $\mathscr{C}$ can be chosen as

$$\begin{aligned} G(x) = \delta(x-1)^{\alpha_0}(\omega x - 1)^{\alpha_1}(\omega^2 x - 1)^{\alpha_2}\cdots(\omega^{\frac{n}{2}-1}x - 1)^{\alpha_{\frac{n}{2}-1}} \\ \times (-x-1)^{1-\alpha_{\frac{n}{2}-1}}(\omega^{\frac{n}{2}+1}x - 1)^{1-\alpha_{\frac{n}{2}-2}}\cdots(\omega^{n-1}x - 1)^{1-\alpha_0}, \end{aligned}$$

where for $0 \leq i \leq \frac{n}{2} - 1$, $\alpha_i = 0$ or 1 and $\delta \in \mathbb{F}_q^*$ depends on α_i such that $G(x)$ is monic.

Simplifying the above expression, we obtain

$$\begin{aligned} G(x) = (x-1)^{\alpha_0}(x - \omega^{n-1})^{\alpha_1}(x - \omega^{n-2})^{\alpha_2}\cdots(x - \omega^{\frac{n}{2}+1})^{\alpha_{\frac{n}{2}-1}} \\ \times (x+1)^{1-\alpha_{\frac{n}{2}-1}}(x - \omega^{\frac{n}{2}-1})^{1-\alpha_{\frac{n}{2}-2}}\cdots(x - \omega)^{1-\alpha_0}. \end{aligned}$$

Note that when $\alpha_i = 1$ for all $0 \leq i \leq \frac{n}{2} - 1$, the code $\mathscr{C}$ is a Reed-Solomon code with the generator polynomial

$$G(x) = \prod_{i=1}^{\frac{n}{2}} (x - \omega^{\frac{n}{2}+i}).$$

4.4 $(1, -1, \ldots, (-1)^{n-1})$-isodual cyclic codes

Throughout this section, the scalar transformation Λ *is fixed as* $\Lambda = (1, -1, \ldots, (-1)^{n-1})$ *and the finite field is of odd characteristic.* This section discusses a special case of the previous section when $\lambda = -1$. Then the order r of λ is 2. By Theorem 4.3.8, we have the following theorem immediately.

Theorem 4.4.1. *Let* $\Lambda = (1, -1, \ldots, (-1)^{n-1})$ *be a scalar transformation, where* n *is even. Let* $\mathbb{F}_q$ *be a finite field with* q *odd. Then there exists an* $[n, \frac{n}{2}]_q$ Λ*-isodual cyclic code if and only if* $\frac{n}{2}$ *is odd.*

Next we describe all the Λ-isodual cyclic codes when $\frac{n}{2}$ is odd.

Write

$$n = p^a \bar{n},$$

where $\gcd(\bar{n}, p) = 1$ and $a \geq 0$. Note that $\bar{n}$ must be even since n is even and p is odd.

Then

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

Since $\frac{n}{2}$ is odd, and the factorization of $x^{\frac{\bar{n}}{2}} + 1$ can be determined by that of $x^{\frac{\bar{n}}{2}} - 1$.

Suppose that $x^{\frac{\bar{n}}{2}} - 1$ is factorized into the product of distinct irreducible polynomials as follows ([10, p.2753])

$$x^{\frac{\bar{n}}{2}} - 1 = \delta f_1(x) \cdots f_s(x) h_1(x) h_1^*(x) \cdots h_t(x) h_t^*(x), \tag{4.23}$$

where $\delta \in \mathbb{F}_q^*$, $f_i(x)$ $(1 \leq i \leq s)$ are irreducible self-reciprocal polynomials over $\mathbb{F}_q$ while $h_j(x)$ and $h_j^*(x)$ $(1 \leq j \leq t)$ are irreducible reciprocal pairs over $\mathbb{F}_q$.

Since $x^{\frac{\bar{n}}{2}} + 1 = -[(-x)^{\frac{\bar{n}}{2}} - 1]$, we have

$$x^{\frac{\bar{n}}{2}} + 1 = -\delta f_1(-x) \cdots f_s(-x) h_1(-x) h_1^*(-x) \cdots h_t(-x) h_t^*(-x).$$

Therefore, we have

$$\begin{aligned} x^{\bar{n}} - 1 = & -\delta^2 f_1(x) \cdots f_s(x) h_1(x) h_1^*(x) \cdots h_t(x) h_t^*(x) \\ & \times f_1(-x) \cdots f_s(-x) h_1(-x) h_1^*(-x) \cdots h_t(-x) h_t^*(-x). \end{aligned}$$

Since the $f_i(x)$'s are irreducible, so are the $f_i(-x)$'s. Since $\gcd(\bar{n}, p) = 1$, the $f_i(\pm x)$'s, $h_j(\pm x)$'s and $h_j^*(\pm x)$'s are pairwise distinct. Therefore, we classify the polynomials by classes and include the polynomials in the same classes in a bracket in -1-ascending order.

$$\begin{aligned} x^{\bar{n}} - 1 = & \delta' [f_1(x) f_1(-x)] \cdots [f_s(x) f_s(-x)] \cdots \\ & [h_1(x) h_1(-x)][h_1^*(-x) h_1^*(x)] \cdots [h_t(x) h_t(-x)][h_t^*(-x) h_t^*(x)], \end{aligned} \tag{4.24}$$

where $\delta' \in \mathbb{F}_q^*$, $[f_i(x) f_i(-x)]$ for $1 \leq i \leq s$ are Type II classes, and $[h_j(x) h_j(-x)]$, $[h_1^*(-x) h_1^*(x)]$ for $1 \leq j \leq t$ are Type IV classes.

By Theorem 4.3.6, we immediately obtain the following theorem.

Theorem 4.4.2. *Assume that $x^n - 1$ is factorized as in Equation (4.24). Let $\mathscr{C}$ be a cyclic code of length n over $\mathbb{F}_q$ with generator polynomial $G(x)$. Then $\mathscr{C}$ is a*

$(1, -1, \ldots, (-1)^{n-1})$-*isodual cyclic code if and only if the generator polynomial* $G(x)$ *is of the following form*

$$\begin{aligned} G(x) =& \delta f_1(x)^{\alpha_1} \cdots f_s(x)^{\alpha_s} h_1(x)^{\beta_1} (h_1^*(x))^{\gamma_1} \cdots h_t(x)^{\beta_t} (h_t^*(x))^{\gamma_t} \\ & \times f_1(-x)^{p^a-\alpha_1} \cdots f_s(-x)^{p^a-\alpha_s} h_1(-x)^{p^a-\gamma_1} h_1^*(-x)^{p^a-\beta_1} \cdots h_t(-x)^{p^a-\gamma_t} h_t^*(-x)^{p^a-\beta_t}, \end{aligned} \tag{4.25}$$

where $\delta \in \mathbb{F}_q^*$ *such that* $G(x)$ *is monic,* $0 \leq \alpha_i \leq p^a$ *for* $1 \leq i \leq s$, $0 \leq \beta_j \leq p^a$ *and* $0 \leq \gamma_j \leq p^a$ *for* $1 \leq j \leq t$.

To simplify the notation in the above theorem, we set

$$\begin{cases} u_1(x) & = f_1(x)^{\alpha_1} \cdots f_s(x)^{\alpha_s}, \\ u_2(x) & = h_1(x)^{\beta_1} (h_1^*(x))^{\gamma_1} \cdots h_t(x)^{\beta_t} (h_t^*(x))^{\gamma_t}, \\ v_1(-x) & = f_1(-x)^{p^a-\alpha_1} \cdots f_s(-x)^{p^a-\alpha_s}, \\ v_2(-x) & = h_1(-x)^{p^a-\gamma_1} h_1^*(-x)^{p^a-\beta_1} \cdots h_t(-x)^{p^a-\gamma_t} h_t^*(-x)^{p^a-\beta_t}. \end{cases}$$

Then $G(x) = \delta u_1(x) u_2(x) v_1(-x) v_2(-x)$. When $t = 0$, i.e., no reciprocal pairs exist in the factorization of $x^{\frac{\bar{n}}{2}} - 1$, we have

$$G(x) = \delta u_1(x) v_1(-x), \tag{4.26}$$

where

$$\begin{aligned} u_1(x) v_1(x) &= x^n - 1, \\ u_1^*(x) &= u_1(x), \\ v_1^*(x) &= \pm v_1(x). \end{aligned}$$

The above construction is the same as in [17, Proposition 5]. When $t = 0$ (i.e., $\bar{n}|(q^i+1)$ for some integer $i \geq 0$), the generator polynomial of a $(1, -1, \ldots, (-1)^{n-1})$-isodual cyclic code is exactly of the form as in (4.26). Therefore, the construction in [17, Proposition 5] is complete when $t = 0$.

The following is a corollary about the enumeration of $(1, -1, \ldots, (-1)^{n-1})$-isodual cyclic codes.

Corollary 4.4.3. *There exists a $(1, -1, \ldots, (-1)^{n-1})$-isodual cyclic code which is not self-dual if and only if $\frac{n}{2}$ and q are odd. Moreover, if $\frac{n}{2}$ and q are odd, then there are $(1+p^a)^{s+2t}$ $(1, -1, \ldots, (-1)^{n-1})$-isodual cyclic codes of length n over $\mathbb{F}_q$ which are not self-dual, and all of them can be described by their generator polynomials as* (4.25). *Assume that $x^n - 1$ is factorized as in Equation* (4.24).

This corollary immediately follows from Theorem 4.4.2.

The following is an example to construct $[6, 3]_7$ $(1, -1, 1, -1, 1, -1)$-isodual cyclic codes.

Example 4.4.4. Let $n = 6$, $q = 7$ and the scalar transformation $\Lambda = (1, -1, 1, -1, 1, -1)$. Then we have

$$x^{\frac{n}{2}} - 1 = x^3 - 1 = (x+6)(x+5)(x+3),$$
$$x^{\frac{n}{2}} + 1 = x^3 + 1 = (x+1)(x+2)(x+4).$$

Notice that in the factorization of $x^3 - 1$, $x + 6$ is a self-reciprocal polynomial while

$x+5$ and $x+3$ form a reciprocal polynomial pair. Write

$$f(x) = x + 6,$$

$$h_1(x) = x + 5,$$

$$h_1^*(x) = x + 3.$$

Then we have

$$f(-x) = 6x + 6 = 6(x + 1),$$

$$h_1(-x) = 6x + 5 = 6(x + 2),$$

$$h_1^*(-x) = 6x + 3 = 6(x + 4).$$

Therefore, $x^3 + 1 = 6f(-x)h_1(-x)h_1^*(-x)$. By Theorem 4.4.2, the generator polynomial of a $[6, 3]_7$ Λ-isodual cyclic code is of the form

$$\begin{aligned} G(x) =& \delta(x+2)^{\alpha}(x+5)^{\beta}(x+3)^{\gamma} \\ & \times (6x+6)^{1-\alpha}(6x+5)^{1-\gamma}(6x+3)^{1-\beta}, \\ =& (x+2)^{\alpha}(x+5)^{\beta}(x+3)^{\gamma} \\ & \times (x+1)^{1-\alpha}(x+2)^{1-\gamma}(x+4)^{1-\beta}, \end{aligned}$$

where $0 \leq \alpha \leq 1$, $0 \leq \beta \leq 1$ and $0 \leq \gamma \leq 1$. There are $(1+1)^3 = 8$ choices of $G(x)$. Therefore, there are 8 Λ-isodual cyclic codes of length 6 over $\mathbb{F}_7$. Furthermore, when $\alpha = 0$ and $\beta = \gamma = 1$, the code with generator polynomial $(x+5)(x+3)(x+1) = x^3 + 2x^2 + 2x + 1$ is an MDS (maximum distance separable) code.

4.5 Conclusion

In this chapter, we have discussed two kinds of isodual cyclic codes, namely, isodual cyclic codes up to multiplier permutations (E1-isodual cyclic codes) and those up to scalar transformations (E2-isodual cyclic codes). When the multiplier permutation is specified as μ_e, then the E1-isodual cyclic codes up to μ_e are called μ_e-isodual cyclic codes. Similarly, when the scalar transformation is specified as $\Lambda = (\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$, then the E2-isodual cyclic codes up Λ are called Λ-isodual cyclic codes or $(\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$-isodual cyclic codes.

If q is odd, no E1-isodual cyclic codes exist over $\mathbb{F}_q$. Furthermore, if q is even, we have given a construction of all the $[n, \frac{n}{2}]_q$ μ_e-isodual cyclic codes given any multiplier permutation μ_e. Then its enumeration is given. Moreover, we have given a necessary and sufficient condition for the existence of E1-isodual cyclic codes that are not self-dual.

In order to discuss E2-isodual cyclic codes, we have given a necessary and sufficient condition on the scalar transformation that transform a cyclic code to a cyclic code again. As a consequence, a necessary and sufficient condition on the scalar transformation Λ has been given to make a cyclic code Λ-isodual.

Furthermore, it has been shown that if the scalar transformation is $\Lambda = (\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$ with $\sum_{i=0}^{n-1} \lambda_i \neq 0$ and q is odd, then there are no Λ-isodual cyclic codes of length n over $\mathbb{F}_q$. Especially, we have considered a class of Λ-isodual cyclic codes case where $\Lambda = (1, \lambda, \ldots, \lambda^{n-1})$ and the order r of λ divides n. In this class of code, there always exist Λ-isodual cyclic codes of length n over $\mathbb{F}_q$ if q is even. Furthermore, if q is odd, there exist Λ-isodual cyclic codes of length n over $\mathbb{F}_q$ if and only if $\frac{n}{r}$ is odd. As a

special case, $\Lambda = (1, -1, \ldots, (-1)^{n-1})$ has been considered. Besides a necessary and sufficient condition on the existence, we have also given a construction of the generator polynomials of all $(1, -1, \ldots, (-1)^{n-1})$-isodual cyclic codes of length n over $\mathbb{F}_q$ and the enumeration of such codes.

Chapter 5

Quasi-twisted codes over finite fields

Quasi-twisted (QT) codes over finite fields form an important class of block codes that includes cyclic codes, quasi-cyclic codes and constacyclic codes as special cases. In this chapter, we investigate issues related to the decomposition and construction of a QT code. The important tool used is the generalized discrete Fourier transform.

This chapter is organized as follows. The decomposition of a (λ, l)-QT code is given in Section 5.1. Section 5.2 deals with the decomposition of the dual code of a QT code in two cases: $\lambda = \pm 1$ and $\lambda \neq \pm 1$. In Section 5.3, the GDFT and the inverse formula are given. After the construction formula is given in Section 5.4, some examples are shown in Section 5.5. A summary concludes the chapter in Section 5.6.

Throughout the chapter, let $\mathscr{L}_{\lambda,l}$ be the cyclic shifts defined in Definition 2.2.4.

5.1 Decomposition of QT Codes

Let $\mathscr{C}$ be a (λ, l)-QT code of length n over $\mathbb{F}_q$. Recall that $\mathscr{C}$ is a module over the ring $\mathbb{F}_q[x]/(x^\theta - \lambda)$, where $\theta = \frac{n}{l}$ (see Section 2.2). Denote the ring $\mathbb{F}_q[x]/(x^\theta - \lambda)$ by $\mathbb{R}_{\theta,\lambda}$.

In order to know more about the algebraic structure of QT codes, we next focus on the ring $\mathbb{R}_{\theta,\lambda}$.

Let $\theta = p^a\bar{\theta}$, where $\gcd(\bar{\theta}, p) = 1$. Since the map $x \mapsto x^{p^a}$ is a power of the Frobenius automorphism of $\mathbb{F}_q$ defined by $x \mapsto x^p$, it is an automorphism of $\mathbb{F}_q$. Therefore, for any $\lambda \in \mathbb{F}_q^*$, there exists a unique $\bar{\lambda} \in \mathbb{F}_q^*$ such that $\bar{\lambda}^{p^a} = \lambda$. Therefore, we may write

$$x^\theta - \lambda = (x^{\bar{\theta}} - \bar{\lambda})^{p^a}.$$

Since $\gcd(\bar{\theta}, p) = 1$, the polynomial $x^{\bar{\theta}} - \bar{\lambda}$ is factorized into distinct irreducible polynomials over $\mathbb{F}_q$ as follows:

$$x^{\bar{\theta}} - \bar{\lambda} = f_1(x)f_2(x)\cdots f_k(x).$$

Therefore, we have

$$x^\theta - \lambda = (f_1(x))^{p^a}(f_2(x))^{p^a}\cdots(f_k(x))^{p^a}. \tag{5.1}$$

By the Chinese Remainder Theorem, we have the following decomposition:

$$\frac{\mathbb{F}_q[x]}{(x^\theta - \lambda)} \simeq \frac{\mathbb{F}_q[x]}{\big((f_1(x))^{p^a}\big)} \bigoplus \frac{\mathbb{F}_q[x]}{\big((f_2(x))^{p^a}\big)} \bigoplus \cdots \frac{\mathbb{F}_q[x]}{\big((f_k(x))^{p^a}\big)}$$

$$r(x) \leftrightarrow \big(r(x) + ((f_1(x))^{p^a}), \cdots, r(x) + ((f_k(x))^{p^a})\big).$$

For convenience, we denote the ring $\frac{\mathbb{F}_q[x]}{\big((f_i(x))^{p^a}\big)}$ by $\mathbb{R}_i$ for $1 \le i \le k$. It follows that

$$\mathbb{R}_{\theta,\lambda}^l \simeq \bigoplus_{i=1}^{k} \mathbb{R}_i^l. \tag{5.2}$$

Then we have the following theorem immediately.

Theorem 5.1.1. *Let $\mathscr{C}$ be a (λ, l)-QT code of length $l\theta$ over $\mathbb{F}_q$. Then $\mathscr{C}$ is a $\mathbb{R}_{\theta,\lambda}$-linear code over $\mathbb{R}_{\theta,\lambda}$ of length l and it can be decomposed as the direct sum*

$$\mathscr{C} \simeq \bigoplus_{i=1}^{k} \mathscr{C}_i, \tag{5.3}$$

where $\mathscr{C}_i$ is a $\mathbb{R}_i$-linear code over $\mathbb{R}_i$ of length l for each $1 \leq i \leq k$.

5.2 Dual Codes of QT codes

In this section, we discuss the dual codes of QT codes. Recall that the index l always divides the length n for a QT code.

The following proposition follows directly from the definition of QT codes.

Proposition 5.2.1. *Let $\mathscr{C}$ be a (λ, l)-QT code of length n over $\mathbb{F}_q$ and let $\mathscr{C}^\perp$ be the dual code of $\mathscr{C}$ with respect to the Euclidean inner product. Then $\mathscr{C}^\perp$ is a (λ^{-1}, l)-QT code of length n.*

By the above proposition, we know that $\mathscr{C}^\perp$ is a submodule of $\mathbb{R}^l_{\theta,\lambda^{-1}}$ over $\mathbb{R}_{\theta,\lambda^{-1}}$, and hence a linear code over $\mathbb{R}_{\theta,\lambda^{-1}}$.

Notice that a (λ, l)-QT code is an $\mathbb{R}_{\theta,\lambda}$-module while its dual code is an $\mathbb{R}_{\theta,\lambda^{-1}}$-module. However, the two rings $\mathbb{R}_{\theta,\lambda}$ and $\mathbb{R}_{\theta,\lambda^{-1}}$ are isomorphic:

$$\mathbb{R}_{\theta,\lambda} \simeq \mathbb{R}_{\theta,\lambda^{-1}}$$

$$x \leftrightarrow x^{-1},$$

where $x^{-1} = \lambda^{-1}x^{\theta-1}$ in the ring $\mathbb{R}_{\theta,\lambda}$ and $x^{-1} = \lambda x^{\theta-1}$ in the ring $\mathbb{R}_{\theta,\lambda^{-1}}$.

By the above isomorphism, we define the map Φ as follows.

Definition 5.2.2. *For all* $(r_0(x), r_1(x), \ldots, r_{l-1}(x)) \in \mathbb{R}^l_{\theta,\lambda^{-1}}$*, we define the map* $\Phi : \mathbb{R}^l_{\theta,\lambda^{-1}} \to \mathbb{R}^l_{\theta,\lambda}$ *with*

$$\Phi\big((r_0(x), r_1(x), \ldots, r_{l-1}(x))\big) = (r_0(x^{-1}), r_1(x^{-1}), \ldots, r_{l-1}(x^{-1})),$$

Obviously, the map Φ is bijective since it is induced from the isomorphism between $\mathbb{R}_{\theta,\lambda}$ and $\mathbb{R}_{\theta,\lambda^{-1}}$. Therefore, it immediately follows that:

Proposition 5.2.3. *The map* Φ *gives a one-to-one correspondence between the* $\mathbb{R}_{\theta,\lambda}$*-submodules of* $\mathbb{R}^l_{\theta,\lambda}$ *and the* $\mathbb{R}_{\theta,\lambda^{-1}}$*-submodules of* $\mathbb{R}^l_{\theta,\lambda^{-1}}$*.*

In order to consider the dual code of a (λ, l)-QT code, it would be nice to find the description of duality $\perp_{\mathbb{R}_{\theta,\lambda}}$ over $\mathbb{R}_{\theta,\lambda}$ such that $\Phi(\mathscr{C}^{\perp}) = \mathscr{C}^{\perp_{\mathbb{R}_{\theta,\lambda}}}$. However, the (λ, l)-QT code and its dual code are modules over different rings. By the above proposition, it is natural to consider the image of the dual code of a (λ, l)-QT code under the map Φ. Then $\Phi(\mathscr{C}^{\perp})$ and $\mathscr{C}$ are modules over the same ring $\mathbb{R}_{\theta,\lambda}$. We define the inner product on the modules over the same ring as follows.

Definition 5.2.4. *Let* $\mathbf{R}$ *be a commutative ring. Let*

$$\mathbf{u} = (u_0, \ldots, u_{l-1})$$

and

$$\mathbf{v} = (v_0, \ldots, v_{l-1})$$

be two vectors over $\mathbf{R}$*. The* dot inner product *over* $\mathbf{R}$ *is defined as the componentwise multiplication, i.e.:*

$$< \mathbf{u}, \mathbf{v} >_{\mathbf{R}} = \sum_{i=0}^{l-1} u_i v_i.$$

Notice that the subscript of $<,>$ is to specify the ring where the dot inner product is defined.

With the dot inner product over rings defined, we give the definition of the dual code over rings.

Definition 5.2.5. *Let* $\mathbf{R}$ *be a ring and let* $\mathscr{C}$ *be an* $\mathbf{R}$*-linear code of length* l*. Then the dual code of* $\mathscr{C}$ *(with respect to the dot inner product over* $\mathbf{R}$*) is defined as* $\mathscr{C}^{\perp_{\mathbf{R}}} = \{\mathbf{d} \in \mathbf{R}^l :< \mathbf{d}, \mathbf{c} >_{\mathbf{R}} = 0, \text{ for each } \mathbf{c} \in \mathscr{C}\}$.

To distinguish the dual code over rings and the dual code over finite fields, we specify the corresponding inner product. The symbol $\perp$ means the dual with respect to the Euclidean inner product over finite fields while $\perp_{\mathbf{R}}$ means the dual with respect to the dot inner product over the ring $\mathbf{R}$.

The following lemma studies the dual with respect to the dot inner product over $\mathbb{R}_{\theta,\lambda}$.

Lemma 5.2.6. *Let* $\mathbf{c}$ *and* $\mathbf{d}$ *be any two vectors in* $\mathbb{F}_q^n$*, where* $n = l\theta$*. Let the vector* $\mathbf{c}(x) \in \mathbb{R}_{\theta,\lambda}^l$ *be the polynomial representation corresponding to the vector* $\mathbf{c}$ *and let the vector* $\mathbf{d}(x) \in \mathbb{R}_{\theta,\lambda^{-1}}^l$ *be the polynomial representation corresponding to the vector* $\mathbf{d}$*. Then* $< \mathbf{c}(x), \Phi(\mathbf{d}(x)) >_{\mathbb{R}_{\theta,\lambda}} = 0$ *if and only if* $\mathscr{L}_{\lambda,l}^i(\mathbf{c}) \cdot \mathbf{d} = 0$ *for each* $0 \le i \le \theta - 1$.

Proof. Assume that $< \mathbf{c}(x), \Phi(\mathbf{d}(x)) >_{\mathbb{R}_{\theta,\lambda}} = 0$. Then we have

$$\sum_{i=0}^{l-1} \big((\sum_{j=0}^{\theta-1} c_{i+jl} x^j)(\sum_{k=0}^{\theta-1} d_{i+kl} x^{-k}) \big) = 0. \tag{5.4}$$

Since the above equation is in the ring $\mathbb{R}_{\theta,\lambda}$, the left hand side can be written as a unique polynomial over $\mathbb{F}_q$ of degree less than θ. Denote by $[x^i]$ the term in x^i in such a unique expression, where $0 \le i \le \theta - 1$.

Since $x^\theta = \lambda$ in the ring $\mathbb{R}_{\theta,\lambda}$, it immediately follows that

$$x^{-j} = \lambda^{-1}x^\theta x^{-j} = \lambda^{-1}x^{\theta-j}, \text{ for } 1 \le j \le \theta - 1.$$

Therefore, each term on the left hand side of (5.4) is as follows:

$$\begin{aligned}
[x^0] &= \sum_{i=0}^{l-1}\sum_{j=0}^{\theta-1} c_{i+jl}d_{i+jl} \\
&= \sum_{i=0}^{\theta l-1} c_i d_i \\
&= \mathbf{c}\cdot\mathbf{d}, \\
[x^k] &= \sum_{i=0}^{l-1}((c_{i+kl}d_i + \cdots + c_{i+(\theta-1)l}d_{i+(\theta-1-k)l})x^k \\
&+ (c_i d_{i+(\theta-k)l} + \cdots + c_{i+(k-1)l}d_{i+(\theta-1)l})x^{k-\theta}) \\
&= \lambda^{-1}\sum_{i=0}^{l-1}(\lambda c_{i+kl}d_i + \cdots + \lambda c_{i+(\theta-1)l}d_{i+(\theta-1-k)l} \\
&+ c_i d_{i+(\theta-k)l} + \cdots + c_{i+(k-1)l}d_{i+(\theta-1)l})x^k \\
&= \lambda^{-1}(\mathscr{L}_{\lambda,l}^{\theta-k}(\mathbf{c})\cdot\mathbf{d})x^k, \text{ for each } 1 \le k \le \theta - 1.
\end{aligned}$$

Then the uniqueness of the expression of the left hand side of (5.4) implies that each term is 0. Thus, the above equations imply that $\mathscr{L}_{\lambda,l}^i(\mathbf{c})\cdot\mathbf{d} = 0$ for $0 \le i \le \theta - 1$.

It is easy to observe that the converse is also true. □

Applying Lemma 5.2.6, we have the following theorem:

Theorem 5.2.7. *Let $\mathscr{C}$ be a (λ, l)-QT code of length n over $\mathbb{F}_q$ and $\mathscr{D}$ a (λ^{-1}, l)-QT code of length n over $\mathbb{F}_q$. Then $\mathscr{D}$ is the dual code of $\mathscr{C}$ with respect to the Euclidean inner product on $\mathbb{F}_q^n$ if and only if $\Phi(\mathscr{D})$ is the dual code of $\mathscr{C}$ with respect to the dot inner product over $\mathbb{R}_{\theta,\lambda}^l$, i.e.,*

$$\Phi(\mathscr{C}^\perp) = \mathscr{C}^{\perp_{\mathbb{R}_{\theta,\lambda}}}, \tag{5.5}$$

where $\mathscr{C}$ on the left is the code over $\mathbb{F}_q$ while $\mathscr{C}$ on the right means its corresponding module over $\mathbb{R}_{\theta,\lambda}$.

Proof. Since $\mathscr{C}$ is a (λ, l)-QT code, for any codeword $\mathbf{c} \in \mathscr{C}$, we have $\mathscr{L}^i_{\lambda,l}(\mathbf{c}) \in \mathscr{C}$. Then for any codeword $\mathbf{d} \in \mathscr{C}^\perp$, we have $\mathscr{L}^i_{\lambda,l}(\mathbf{c}) \cdot \mathbf{d} = 0$. By Lemma 5.2.6, it follows $< \mathbf{c}, \Phi(\mathbf{d}) >_{\mathbb{R}_{\theta,\lambda}} = 0$. Therefore, we have $\Phi(\mathbf{d}) \in \mathscr{C}^{\perp_{\mathbb{R}_{\theta,\lambda}}}$. Then by Definition 5.2.5, we have $\Phi(\mathscr{C}^\perp) \subseteq \mathscr{C}^{\perp_{\mathbb{R}_{\theta,\lambda}}}$.

Assume that $\mathbf{v} \in \mathscr{C}^{\perp_{\mathbb{R}_{\theta,\lambda}}}$. Then by Lemma 5.2.6, for any codeword $\mathbf{c} \in \mathscr{C}$, we have $\mathscr{L}^i_{\lambda,l}(\mathbf{c}) \cdot \Phi^{-1}(\mathbf{v}) = 0$. It follows that $\Phi^{-1}(\mathbf{v}) \in \mathscr{C}^\perp$. Then $\mathscr{C}^{\perp_{\mathbb{R}_{\theta,\lambda}}} \subseteq \Phi(\mathscr{C}^\perp)$. Therefore, $\Phi(\mathscr{C}^\perp) = \mathscr{C}^{\perp_{\mathbb{R}_{\theta,\lambda}}}$. □

By the decomposition of the ring $\mathbb{R}_{\theta,\lambda}$ in (5.2), we have the following corollary.

Corollary 5.2.8. *Let $\mathscr{C}$ be a (λ, l)-QT code over $\mathbb{F}_q$ of length $n = l\theta$. Suppose that $\mathscr{C}$ is decomposed as in* (5.2)*. Then $\mathscr{C}^{\perp_{\mathbb{R}_{\theta,\lambda}}}$ is decomposed as follows:*

$$\mathscr{C}^{\perp_{\mathbb{R}_{\theta,\lambda}}} \simeq \bigoplus_{i=1}^{k} \mathscr{D}_i, \tag{5.6}$$

where, for each $1 \leq i \leq k$, $\mathscr{D}_i$ is the dual code of $\mathscr{C}_i$ with respect to the dot inner product over $\mathbb{R}^l_i$. In particular, $\mathscr{C}$ is self-dual if and only if $\mathscr{C}_i = \mathscr{D}_i$ for all $1 \leq i \leq k$.

By Theorem 5.2.7, the above corollary gives the decomposition of $\Phi(\mathscr{C}^\perp)$. Next we discuss the relationship between the decomposition of $\mathscr{C}^\perp \subseteq \mathbb{R}^l_{\theta,\lambda^{-1}}$ and that of $\Phi(\mathscr{C}^\perp) = \mathscr{C}^{\perp_{\mathbb{R}_{\theta,\lambda}}} \subseteq \mathbb{R}^l_{\theta,\lambda}$.

Assume that $x^\theta - \lambda$ is factorized as in (5.1). Then

$$x^\theta - \lambda^{-1} = -\lambda^{-1}(f_1^*(x))^{p^a} \cdots (f_k^*(x))^{p^a}, \tag{5.7}$$

where $f_i^*(x) := x^{\deg f_i(x)} f_i(x^{-1})$ is the reciprocal polynomial of $f_i(x)$ over $\mathbb{F}_q$. It is easy to check that $f_i^*(x)$ is also irreducible over $\mathbb{F}_q$ if $f_i(x)$ is irreducible. Therefore, we have the following decomposition of the ring $\mathbb{R}_{\theta,\lambda^{-1}}$:

$$\frac{\mathbb{F}_q[x]}{(x^\theta - \lambda^{-1})} \simeq \frac{\mathbb{F}_q[x]}{\left((f_1^*(x))^{p^a}\right)} \bigoplus \frac{\mathbb{F}_q[x]}{\left((f_2^*(x))^{p^a}\right)} \bigoplus \cdots \frac{\mathbb{F}_q[x]}{\left((f_k^*(x))^{p^a}\right)}$$

$$r(x) \leftrightarrow \left(r(x) + ((f_1^*(x))^{p^a}), \cdots, r(x) + ((f_k^*(x))^{p^a})\right). \tag{5.8}$$

For simplicity, we denote the ring $\frac{\mathbb{F}_q[x]}{\left((f_i^*(x))^{p^a}\right)}$ by $\mathbb{R}_i^*$ for $1 \le i \le k$. It follows that

$$\mathbb{R}_{\theta,\lambda^{-1}}^l \simeq \bigoplus_{i=1}^{k} (\mathbb{R}_i^*)^l. \tag{5.9}$$

Note that if a (λ, l)-QT code is self-dual, then it is not $\{0\}$ and we can pick a codeword with a nonzero entry at the last coordinate, say $(c_0, c_1, \ldots, c_{n-1})$. Then

$$\begin{cases} \sum_{i=0}^{n-1} c_i^2 = 0, \\ \lambda^2 c_{n-1}^2 + \sum_{i=0}^{n-2} c_i^2 = 0. \end{cases}$$

Since $c_{n-1} \neq 0$, we have $\lambda^2 = 1$. Therefore, a (λ, l)-QT code is self-dual only if $\lambda = \pm 1$. If $\lambda \neq \pm 1$, then the polynomials $x^\theta - \lambda$ and $x^\theta - \lambda^{-1}$ are coprime over $\mathbb{F}_q$. Therefore, the irreducible polynomials $f_i(x)$, $f_j^*(x)$, $1 \le i, j \le k$, are pairwise coprime where $f_i(x)$, $f_j^*(x)$, $1 \le i, j \le k$ are as in (5.1) and (5.7). Thus, no irreducible polynomial is a nonzero scalar multiple of its reciprocal polynomial and no reciprocal pair exists in the factorization of $x^\theta - \lambda$, which is different from the case when $\lambda = \pm 1$.

5.2.1 Case when $\lambda = \pm 1$

In this subsection, we focus on the case when $\lambda = \pm 1$. If $\lambda = \pm 1$, then $x^\theta - \lambda = x^\theta - \lambda^{-1}$ and hence $\mathbb{R}_{\theta,\lambda} = \mathbb{R}_{\theta,\lambda^{-1}}$. With the proper permutation of the irreducible

polynomial factors, $x^\theta - \lambda$ is written as

$$x^\theta - \lambda = \epsilon(g_1(x))^{p^a} \cdots (g_s(x))^{p^a}(h_1(x))^{p^a}(h_1^*(x))^{p^a} \cdots (h_t(x))^{p^a}(h_t^*(x))^{p^a},$$

where $s + 2t = k$, $\epsilon \in \mathbb{F}_q^*$ and, for each $1 \leq i \leq s$, $g_i(x)$ is an associate of its reciprocal polynomial, i.e., $g_i(x) = \epsilon_i g_i^*(x)$ over $\mathbb{F}_q$ for some unit ϵ_i. Throughout this subsection, we denote $\mathbb{F}_q[x]/\big((g_i(x))^{p^a}\big)$ by $\mathbb{G}_i$ for $1 \leq i \leq s$, $\mathbb{F}_q[x]/\big((h_j(x))^{p^a}\big)$ by $\mathbb{H}_j$ and $\mathbb{F}_q[x]/\big((h_j^*(x))^{p^a}\big)$ by $\mathbb{H}_j^*$ for $1 \leq j \leq t$. Then the decomposition of $\mathbb{R}_{\theta,\lambda} = \mathbb{R}_{\theta,\lambda^{-1}}$ is

$$\mathbb{R}_{\theta,\lambda} \simeq \bigoplus_{i=1}^{s} \mathbb{G}_i \bigoplus \big(\bigoplus_{j=1}^{t} (\mathbb{H}_j \bigoplus \mathbb{H}_j^*)\big). \tag{5.10}$$

Therefore, when $\lambda = \pm 1$, the map Φ is an automorphism of $\mathbb{R}_{\theta,\lambda}^l$. We define same isomorphisms between the component rings as follows.

Definition 5.2.9. *For $1 \leq i \leq s$, define*

$$\Phi_i : (\mathbb{G}_i)^l \to (\mathbb{G}_i)^l$$

by

$$\begin{aligned}&\Phi_i((r_1(x) + ((g_i(x))^{p^a}), \ldots, r_l(x) + ((g_i(x))^{p^a})))\\ =&(r_1(x^{-1}) + ((g_i(x))^{p^a}), \ldots, r_l(x^{-1}) + ((g_i(x))^{p^a})).\end{aligned}$$

For $1 \leq j \leq t$, define

$$\Phi_j' : (\mathbb{H}_j)^l \to (\mathbb{H}_j^*)^l$$

by

$$\begin{aligned}&\Phi_j'((r_1(x) + ((h_j(x))^{p^a}), \ldots, r_l(x) + ((h_j(x))^{p^a})))\\ =&(r_1(x^{-1}) + ((h_j^*(x))^{p^a}), \ldots, r_l(x^{-1}) + ((h_j^*(x))^{p^a})).\end{aligned}$$

Actually, when $\lambda = \pm 1$, the maps Φ, Φ_i and Φ'_j are exactly the conjugate maps defined in [12].

Lemma 5.2.10. *Assume that $\lambda = \pm 1$ and the decomposition of the ring $\mathbb{R}_{\theta,\lambda} = \mathbb{R}_{\theta,\lambda^{-1}}$ is as in* (5.10)*. Let $r(x) \in \mathbb{R}_{\theta,\lambda}$ and let its decomposition in $\mathbb{R}_{\theta,\lambda}$ be*

$$(r_1(x), \ldots, r_s(x), r'_1(x), r''_1(x), \ldots, r'_t(x), r''_t(x))$$

where for $1 \leq i \leq s$, $r_i(x) = r(x) + \left((g_i(x))^{p^a}\right) \in \mathbb{G}_i$, and for $1 \leq j \leq t$, $r'_j(x) = r(x) + \left((h_j(x))^{p^a}\right) \in \mathbb{H}_j$ and $r''_j(x) = r(x) + \left((h^*_j(x))^{p^a}\right) \in \mathbb{H}^*_j$. Then the decomposition of $\Phi^{-1}(r(x)) \in \mathbb{R}_{\theta,\lambda^{-1}}$ is

$$(r_1(x^{-1}), \ldots, r_s(x^{-1}), r''_1(x^{-1}), r'_1(x^{-1}), \ldots, r''_t(x^{-1}), r'_t(x^{-1})).$$

Proof. For $1 \leq i \leq s$, since $r_i(x) = r(x) + ((g_i(x))^{p^a})$, then

$$r_i(x^{-1}) = r(x^{-1}) + ((g_i(x^{-1}))^{p^a}).$$

Since $g(x)$ is an associate of its reciprocal polynomial, then

$$((g_i(x))^{p^a}) = ((g_i(x^{-1}))^{p^a}).$$

Therefore, we have

$$r_i(x^{-1}) = r(x^{-1}) + ((g_i(x))^{p^a}),$$

i.e., the component of $\Phi^{-1}(r(x)) = r(x^{-1})$ in $\mathbb{G}_i$ is $r_i(x^{-1})$.

For $1 \leq j \leq t$, we have

$$r'_j(x^{-1}) = r(x^{-1}) + ((h_j(x^{-1}))^{p^a}).$$

Then

$$r'_j(x^{-1}) = r(x^{-1}) + (h^*_j(x))^{p^a},$$

i.e., the component of $\Phi^{-1}(r(x)) = r(x^{-1})$ in $\mathbb{H}_j^*$ is $r'_j(x^{-1})$.

Similarly, the component of $\Phi^{-1}(r(x)) = r(x^{-1})$ in $\mathbb{H}_j$ is $r''_j(x^{-1})$. □

The following theorem gives the algebraic structure of the dual code of a (λ, l)-QT code when $\lambda = \pm 1$.

Theorem 5.2.11. *Let $\mathscr{C}$ be a (λ, l)-QT code of length $l\theta$ over $\mathbb{F}_q$ with $\lambda = \pm 1$. Let the decomposition of the ring $\mathbb{R}_{\theta,\lambda}$ be as in* (5.10) *and let the corresponding decomposition of $\mathscr{C}$ be*

$$\mathscr{C} \simeq \bigoplus_{i=1}^{s} \mathscr{C}_i \bigoplus \big(\bigoplus_{j=1}^{t} (\mathscr{C}'_j \bigoplus \mathscr{C}''_j) \big).$$

Then the decomposition of its dual code $\mathscr{C}^\perp$ (with respect to the Euclidean inner product) is

$$\mathscr{C}^\perp \simeq \bigoplus_{i=1}^{s} \Phi_i(\mathscr{C}_i^{\perp_{\mathbb{G}_i}}) \bigoplus \big(\bigoplus_{j=1}^{t} ((\Phi'_j)^{-1}((\mathscr{C}''_j)^{\perp_{\mathbb{H}_j^*}}) \bigoplus \Phi'_j((\mathscr{C}'_j)^{\perp_{\mathbb{H}_j}})) \big),$$

where the dual on the left is the dual with respect to the Euclidean inner product over $\mathbb{F}_q$, while the duals on the right are the duals with respect to the dot inner products over the respective component rings.

In particular, $\mathscr{C}$ is self-dual if and only if

$$\begin{cases} \mathscr{C}_i = \Phi_i(\mathscr{C}_i^{\perp_{\mathbb{G}_i}}), & 1 \le i \le s, \\ \mathscr{C}''_j = \Phi'_j((\mathscr{C}'_j)^{\perp_{\mathbb{H}_j}}), & 1 \le j \le t. \end{cases} \tag{5.11}$$

Proof. This theorem follows from Corollary 5.2.8 and Lemma 5.2.10. □

When $\lambda = \pm 1$, the map Φ_i's are actually the conjugates defined in [12]. We can check that the above theorem is consistent with Theorem 4.2 in [12] which describes the dual with respect to the Hermitian inner product.

5.2.2 Case when $\lambda \neq \pm 1$

In this subsection, we assume that $\lambda \neq \pm 1$. Recall that Φ is the isomorphism between $\mathbb{R}_{\theta,\lambda}$ and $\mathbb{R}_{\theta,\lambda^{-1}}$. Let the decompositions of $\mathbb{R}_{\theta,\lambda}^l$ and $\mathbb{R}_{\theta,\lambda^{-1}}^l$ be as in (5.2) and (5.9), respectively. Then the quotient rings $\mathbb{R}_i = \mathbb{F}_q[x]/((f_i(x))^{p^a})$ and $\mathbb{R}_i^* = \mathbb{F}_q[x]/((f_i^*(x))^{p^a})$ are isomorphic as rings. The corresponding isomorphism is defined as follows.

Definition 5.2.12. *The isomorphism is*

$$\Phi_i' : (\mathbb{R}_i)^l \to (\mathbb{R}_i^*)^l$$

given by

$$\begin{aligned}&\Phi_i'((r_1(x) + ((f_i(x))^{p^a}), \ldots, r_l(x) + ((f_i(x))^{p^a})))\\ =&(r_1(x^{-1}) + ((f_i^*(x))^{p^a}), \ldots, r_l(x^{-1}) + ((f_i^*(x))^{p^a})).\end{aligned}$$

By Corollary 5.2.8, the following theorem immediately follows.

Theorem 5.2.13. *Let $\lambda \neq \pm 1$ and let the decompositions of $\mathbb{R}_{\theta,\lambda}^l$ and $\mathbb{R}_{\theta,\lambda^{-1}}^l$ be as in* (5.2) *and* (5.9)*, respectively. Let $\mathscr{C}$ be a (λ, l)-QT code of length $l\theta$ over $\mathbb{F}_q$, i.e., an $\mathbb{R}_{\theta,\lambda}$-linear code. Suppose that the decomposition of $\mathscr{C}$ is as in* (5.3)*:*

$$\mathscr{C} \simeq \bigoplus_{i=1}^{k} \mathscr{C}_i.$$

Then the decomposition of its dual code $\mathscr{C}^\perp \subseteq \mathbb{R}_{\theta,\lambda^{-1}}^l$ ($\perp$ is the dual with respect to the Euclidean inner product) is

$$\mathscr{C}^\perp \simeq \bigoplus_{i=1}^{k} \Phi_i(\mathscr{C}_i^{\perp_{\mathbb{R}_i}})$$

where $\perp_{\mathbb{R}_i}$ is the dual with respect to the dot inner product over the ring $\mathbb{R}_i$.

Given the decomposition of the code $\mathscr{C} \subseteq \mathbb{R}^l_{\theta,\lambda}$, Theorems 5.2.11 and 5.2.13 give the decomposition of the dual code $\mathscr{C}^\perp \subseteq \mathbb{R}^l_{\theta,\lambda^{-1}}$, for cases $\lambda = \pm 1$ and $\lambda \neq \pm 1$ respectively.

5.3 Discrete Fourier Transform

Mattson-Solomon (MS) polynomials (sometimes called the discrete Fourier transform) were introduced by Mattson and Solomon ([16]). It is a useful device for getting the weight distribution of a cyclic code ([14, Chapter. 8]). This notion can be generalized to quasi-cyclic codes ([11]). This chapter generalizes the notion further to quasi-twisted codes.

It is well-known in real number field that if ξ is a root of $f(x)$ with multiplicity i, then $f(\xi) = 0$ and j-th derivative of $f(x)$ at ξ is 0 for all $1 \leq j \leq i-1$. To transfer the notion to finite fields, we use the Hasse derivative which is a tool to help us to deal with the repeated-root case.

Definition 5.3.1. *(see [8]) For a polynomial $g(x) = \sum_i g_i x^i \in \mathbb{F}_q[x]$, the j-th* Hasse derivative *is defined as*

$$g^{[j]}(x) = \sum_i \binom{i}{j} g_i x^{i-j}.$$

Using the Hasse derivative, we define the generalized discrete Fourier transform (GDFT). Recall that $\theta = p^a\bar{\theta}$, where $\gcd(\bar{\theta}, p) = 1$.

Definition 5.3.2. *If $c(x) = \sum_{i \in \mathbb{Z}/\theta\mathbb{Z}} c_i x^i \in \mathbb{R}_{\theta,\lambda}$, then the* generalized discrete Fourier

transform (GDFT) *of* $c(x)$ *can be described in terms of a matrix*

$$\hat{c} = \begin{bmatrix} \hat{c}_{0,0} & \hat{c}_{0,1} & \cdots & \hat{c}_{0,\bar{\theta}-1} \\ \hat{c}_{1,0} & \hat{c}_{1,1} & \cdots & \hat{c}_{1,\bar{\theta}-1} \\ \vdots & \vdots & \vdots & \vdots \\ \hat{c}_{p^a-1,0} & \hat{c}_{p^a-1,1} & \cdots & \hat{c}_{p^a-1,\bar{\theta}-1} \end{bmatrix}, \tag{5.12}$$

where

$$\hat{c}_{g,h} = \sum_{i \in \mathbb{Z}/\theta\mathbb{Z}} \binom{i}{g} c_i (\beta \xi^h)^{i-g}, \text{ for } 0 \le g \le p^a - 1, 0 \le h \le \bar{\theta} - 1,$$

β *is a* $\bar{\theta}$*-th root of* $\bar{\lambda}$,

and ξ *is a primitive* $\bar{\theta}$*-th root of unity.*

Notice that $\hat{c}_{g,h}$ is exactly the value of the g-th Hasse derivative of $c(x)$ at $\beta\xi^h$, a $\bar{\theta}$-th root of $\bar{\lambda}$. Let $x^\theta - \lambda$ be decomposed as in (5.1). Then for each $0 \le h \le \bar{\theta} - 1$, there is an irreducible factor of $x^\theta - \lambda$, say $f_i(x)$, such that $\beta\xi^h$ is a root of $f_i(x)$. Then $\hat{c}_{g,h}$ is an element in $\mathbb{F}_q[x]/\big((f_i(x))^{p^a}\big)$. Mimicking the method in [12] and replacing the root ξ^h in [12] by $\beta\xi^h$, then the explicit description of the inverse transform is given. We give the inverse transform in the following theorem and omit the proof.

Theorem 5.3.3. *The GDFT* (5.12) *is invertible. More precisely, the inverse formula of GDFT is*

$$c_{i+jp^a} = \frac{1}{\bar{\theta}} \sum_{h=0}^{\bar{\theta}-1} (\beta\xi^h)^{-jp^a} \Big(\sum_{g=0}^{p^a-1} \binom{g}{i} (-\beta\xi^h)^{g-i} \hat{c}_{g,h} \Big), \tag{5.13}$$

for $0 \le i \le p^a - 1$ *and* $0 \le j \le \bar{\theta} - 1$*, where* β *is a* $\bar{\theta}$*-th root of* $\bar{\lambda}$ *and* ξ *is a primitive* $\bar{\theta}$*-th root of unity.*

Since $(\beta^{q-1})^{\bar{\theta}} = \bar{\lambda}^{q-1} = 1$ for $\bar{\lambda} \in \mathbb{F}_q^*$, β^{q-1} is a $\bar{\theta}$-th root of unity. Then β^{q-1} can

be expressed as a power of the primitive $\bar{\theta}$-th root of unity ξ, say

$$\beta^{q-1} = \xi^{\iota},$$

where $0 \leq \iota \leq \bar{\theta} - 1$.

By the definition of $\hat{c}_{g,h}$, it is easy to verify that, for $0 \leq g \leq p^a - 1$ and $0 \leq h \leq \bar{\theta} - 1$,

$$\begin{aligned}
\hat{c}_{g,h}^{q} &= \sum_{i \in \mathbb{Z}/\theta\mathbb{Z}} \binom{i}{g}^{q} c_i^q [(\beta \xi^h)^q]^{i-g} \\
&= \sum_{i \in \mathbb{Z}/\theta\mathbb{Z}} \binom{i}{g} c_i (\beta \xi^{qh+\iota})^{i-g} \\
&= \hat{c}_{g,qh+\iota}.
\end{aligned}$$

Given an irreducible polynomial $f_i(x)$, if $\beta\xi^{z_i}$ is a root of $f_i(x)$, so is $\beta^q \xi^{qz_i} = \beta\xi^{qz_i+\iota}$. Define a map τ:

$$\begin{aligned}
\tau : \mathbb{Z}/\bar{\theta}\mathbb{Z} &\to \mathbb{Z}/\bar{\theta}\mathbb{Z} \\
z &\mapsto qz + \iota.
\end{aligned}$$

As $\gcd(\bar{\theta}, q) = 1$, it follows that the map τ is one-to-one. Therefore, the map τ defines an equivalence relation $\sim$ on $\mathbb{Z}/\bar{\theta}\mathbb{Z}$ where $h_1 \sim h_2$ if and only if there exists an integer i such that $h_1 = \tau^i(h_2)$. Therefore, there is a one-to-one correspondence between the equivalence classes and the irreducible factors $f_i's$. For convenience, we call the equivalence classes *orbits of* τ. From each orbit O_i, we can choose a representative, say z_i. Then there is a one-to-one correspondence between the irreducible factors $f_i(x)$'s and the representatives z_i's. We say the representative z_i is corresponding to the irreducible polynomial f_i. In particular, when $\iota = 0$, the equivalence classes are known as the q-cyclotomic cosets modulo $\bar{\theta}$.

Therefore, using the same notations above, the inverse formula of the GDFT can be further simplified as follows.

Theorem 5.3.4. *The GDFT* (5.12) *is invertible as follows: for* $0 \leq i \leq p^a - 1$ *and* $0 \leq j \leq \bar{\theta} - 1$,

$$c_{i+jp^a} = \frac{1}{\bar{\theta}} \sum_{g=0}^{p^a-1} \binom{g}{i} (-1)^{g-i} \Big(\sum_{\gamma=1}^{k} Tr_\gamma(\hat{c}_{g,z_\gamma} (\beta \xi^{z_\gamma})^{g-i-jp^a}) \Big), \tag{5.14}$$

where β *is a* $\bar{\theta}$*-th root of* $\bar{\lambda}$, ξ *is a primitive* $\bar{\theta}$*-th root of unity,* z_γ *is a representative in the orbit corresponding to* $f_\gamma(x)$ *and* Tr_γ *is the trace map on the field* $\mathbb{F}_q[x]/(f_\gamma(x))$ *down to* $\mathbb{F}_q$.

Although the choices of β and ξ in (5.14) are not unique, the result of (5.14) is unique when $\hat{c}_{g,h}$'s are given. The above theorem gives the trace description of QT codes. With the trace description, different choices for β and ξ will not change the construction method in following section.

5.4 Construction Formula

Let $\mathscr{C}$ be a (λ, l)-QT code of length $l\theta$. By Theorem 5.1.1, we know that

$$\mathscr{C} \simeq \bigoplus_{i=1}^{k} \mathscr{C}_i,$$

where $\mathscr{C}_i$ is a linear code over $\mathbb{R}_i$ of length l for each $1 \leq i \leq k$.

The ring $\mathbb{R}_i = \frac{\mathbb{F}_q[x]}{\left((f_i(x))^{p^a}\right)}$ is a finite chain ring. Each element in $\mathbb{R}_i$ can be written in the following canonical form:

$$a_0(x) + a_1(x) f_i(x) + \cdots + a_{p^a-1}(x)(f_i(x))^{p^a-1},$$

where $a_j(x) \in \frac{\mathbb{F}_q[x]}{(f_i(x))}$ for $0 \leq j \leq p^a - 1$. Therefore,

$$\frac{\mathbb{F}_q[x]}{\left((f_i(x))^{p^a}\right)} \simeq \frac{\mathbb{F}_q[x]}{(f_i(x))} + f_i(x)\frac{\mathbb{F}_q[x]}{(f_i(x))} + \cdots + (f_i(x)^{p^a-1})\frac{\mathbb{F}_q[x]}{(f_i(x))}.$$

Let $d_i = \deg f_i(x)$ and let $\beta\xi^{z_i}$ be a root of $f_i(x)$. Then we have the following field isomorphism:

$$\frac{\mathbb{F}_q[x]}{(f_i(x))} \simeq \mathbb{F}_q + (\beta\xi^{z_i})\mathbb{F}_q + \cdots + (\beta\xi^{z_i})^{d_i-1}\mathbb{F}_q$$

$$r(x) \leftrightarrow r(\beta\xi^{z_i}).$$

Then we have the following proposition.

Proposition 5.4.1. *The following map is a ring isomorphism:*

$$\begin{aligned}\sigma : \mathbb{R}_i \rightarrow & (\mathbb{F}_q + (\beta\xi^{z_i})\mathbb{F}_q + \cdots + (\beta\xi^{z_i})^{d_i-1}\mathbb{F}_q) + u(\mathbb{F}_q + \cdots + (\beta\xi^{z_i})^{d_i-1}\mathbb{F}_q) \\ & + \cdots + u^{p^a-1}(\mathbb{F}_q + \cdots + (\beta\xi^{z_i})^{d_i-1}\mathbb{F}_q) \\ r(x) \mapsto & r(\beta\xi^{z_i} + u),\end{aligned}$$

where $u^{p^a} = 0$ and $\beta\xi^{z_i}$ is a root of $f_i(x)$.

Proof. For convenience, denote $f_i(x)$ by $f(x)$, $d = \deg(f(x))$ and $\beta\xi^{z_i}$ by η. Suppose that $f(x) = \sum_{i=0}^{d} a_i x^i$. Since η is a root of $f(x)$ and $u^{p^a} = 0$, we have

$$\begin{aligned}\sigma((f(x))^{p^a}) &= (f(\eta + u))^{p^a} \\ &= \sum_{i=0}^{d} a_i^{p^a}(\eta^{p^a} + u^{p^a})^i \\ &= \sum_{i=0}^{d} a_i^{p^a}\eta^{p^a i} \\ &= (f(\eta))^{p^a} \\ &= 0.\end{aligned}$$

Therefore, this map is well defined.

Since η is a root of the irreducible polynomial $f(x)$, $\eta^{\bar{\theta}\bar{r}} = \bar{\lambda}^{\bar{r}} = 1$, where $\bar{r}$ is the order of $\bar{\lambda} \in \mathbb{F}_q^*$. Since $\bar{r}$ divides $q-1$, $\bar{r}$ is coprime to p^a. Since $\bar{\theta}$ is coprime to p^a too, p^a and $\bar{\theta}\bar{r}$ are coprime. Then there exist integers N_1 and N_2 such that

$$p^a N_1 + N_2 \bar{\theta}\bar{r} = 1.$$

Then we have $\eta^{p^a N_1} = \eta$.

It follows that $x^{p^a N_1}$ is mapped to η and $x - x^{p^a N_1}$ is mapped to u. Hence, the map σ is a ring isomorphism. □

For simplicity, we denote by J_i the chain ring

$$(\mathbb{F}_q + (\beta\xi^{z_i})\mathbb{F}_q + \cdots + (\beta\xi^{z_i})^{d_i-1}\mathbb{F}_q) + u(\mathbb{F}_q + \cdots + (\beta\xi^{z_i})^{d_i-1}\mathbb{F}_q) + \cdots + u^{p^a-1}(\mathbb{F}_q + \cdots + (\beta\xi^{z_i})^{d_i-1}\mathbb{F}_q).$$

Then we have

$$\mathbb{R}_{\theta,\lambda} \simeq \bigoplus_{i=1}^{k} J_i,$$

and

$$\mathscr{C} \simeq \bigoplus_{i=1}^{k} \mathscr{C}_i,$$

where $\mathscr{C}_i$ is a code over J_i of length l.

Then a codeword $\mathbf{x}_i$ of $\mathscr{C}_i$ over J_i can be written as

$$\begin{aligned}\mathbf{x}_i =& \big(\mathbf{x}_{i,0,0} + (\beta\xi^{z_i})\mathbf{x}_{i,0,1} + \cdots + (\beta\xi^{z_i})^{d_i-1}\mathbf{x}_{i,0,d_i-1}\big) \\ &+ u\big(\mathbf{x}_{i,1,0} + (\beta\xi^{z_i})\mathbf{x}_{i,1,1} + \cdots + (\beta\xi^{z_i})^{d_i-1}\mathbf{x}_{i,1,d_i-1}\big) + \cdots \\ &+ u^{p^a-1}\big(\mathbf{x}_{i,p^a-1,0} + (\beta\xi^{z_i})\mathbf{x}_{i,p^a-1,1} + \cdots + (\beta\xi^{z_i})^{d_i-1}\mathbf{x}_{i,p^a-1,d_i-1}\big),\end{aligned}$$

where, for each $1 \leq i \leq k$, $0 \leq j \leq p^a - 1$ and $0 \leq w \leq d_i - 1$, $\mathbf{x}_{i,j,w}$ is a row vector over $\mathbb{F}_q$ of length l.

We vertically join all the above row vectors $\mathbf{x}_{i,j,w}$ as

$$\tilde{\mathbf{x}_i} = (\mathbf{x}_{i,0,0}, \ldots, \mathbf{x}_{i,0,d_i-1}, \mathbf{x}_{i,1,0}, \ldots, \mathbf{x}_{i,1,d_i-1}, \ldots, \mathbf{x}_{i,p^a-1,0}, \ldots, \mathbf{x}_{i,p^a-1,d_i-1})^T.$$

Then $\tilde{\mathbf{x}_i}$ is a matrix of size $p^a d_i \times l$. We vertically joint all the above matrices as

$$\mathbf{x} = (\tilde{\mathbf{x}_1}, \tilde{\mathbf{x}_2}, \ldots, \tilde{\mathbf{x}_k})^T. \tag{5.15}$$

Then $\mathbf{x}$ is in fact a matrix of size $\theta \times l$ since $\sum_{i=1}^{k} p^a d_i = \theta$.

By Theorem 5.3.3, a codeword in a QT code can be given if the component codewords are known. With the same notations as above, we have the following result about the construction of a QT code.

Theorem 5.4.2. *Let $\theta = p^a \bar{\theta}$ with $\gcd(p, \bar{\theta}) = 1$, where p is the characteristic of $\mathbb{F}_q$. Then, for any positive integer l and any $\lambda \in \mathbb{F}_q^*$, the (λ, l)-QT codes over $\mathbb{F}_q$ of length $l\theta$ are precisely given as follows:*

1. *Write $\lambda = \bar{\lambda}^{p^a}$ where $\bar{\lambda} \in \mathbb{F}_q^*$.*

2. *Write $x^{\bar{\theta}} - \bar{\lambda} = f_1(x) f_2(x) \cdots f_k(x)$, where for $1 \leq \gamma \leq k$, $f_\gamma(x)$ are monic irreducible polynomials over $\mathbb{F}_q$.*

3. *Write $\mathbb{F}_q[x] / \big((f_\gamma(x))^{p^a}\big) = \mathbb{R}_\gamma$ and $\deg f_\gamma(x) = d_\gamma$.*

4. *Let* $\mathbf{O}_\gamma$ *denote the orbit corresponding to* $f_\gamma(x)$ *and fix* $z_\gamma \in \mathbf{O}_\gamma$.

5. *For each* $1 \leq \gamma \leq k$, *let* $\mathscr{C}_\gamma$ *be a linear code of length* l *over* $\mathbb{R}_\gamma$. *For* $\mathbf{x}_\gamma \in \mathscr{C}_\gamma$, *write*

$$\begin{aligned}\mathbf{x}_\gamma =&\big(\mathbf{x}_{\gamma,0,0} + (\beta\xi^{z_\gamma})\mathbf{x}_{\gamma,0,1} + \cdots + (\beta\xi^{z_\gamma})^{d_\gamma-1}\mathbf{x}_{\gamma,0,d_\gamma-1}\big)\\ &+ u\big(\mathbf{x}_{\gamma,1,0} + (\beta\xi^{z_\gamma})\mathbf{x}_{\gamma,1,1} + \cdots + (\beta\xi^{z_\gamma})^{d_\gamma-1}\mathbf{x}_{\gamma,1,d_\gamma-1}\big) + \cdots\\ &+ u^{p^a-1}\big(\mathbf{x}_{\gamma,p^a-1,0} + (\beta\xi^{z_\gamma})\mathbf{x}_{\gamma,p^a-1,1} + \cdots + (\beta\xi^{z_\gamma})^{d_\gamma-1}\mathbf{x}_{\gamma,p^a-1,d_\gamma-1}\big),\end{aligned}$$

where, for each $1 \leq \gamma \leq k$, $0 \leq g \leq p^a - 1$ *and* $0 \leq w \leq d_\gamma - 1$, $\mathbf{x}_{\gamma,g,w}$ *is a row vector over* $\mathbb{F}_q$ *of length* l.

6. *For each* $0 \leq i \leq p^a - 1$ *and* $0 \leq j \leq \bar{\theta} - 1$, *let*

$$\mathbf{c}_{i+jp^a} = \frac{1}{\bar{\theta}} \sum_{g=0}^{p^a-1} \binom{g}{i} (-1)^{g-i} \Big(\sum_{\gamma=1}^{k} \Big(\sum_{w=0}^{d_\gamma-1} (\mathbf{x}_{\gamma,g,w} Tr_\gamma((\beta\xi^{z_\gamma})^{g-i-jp^a+w}))\Big)\Big), \qquad (5.16)$$

and hence the codewords $\mathbf{x}_\gamma \in \mathscr{C}_\gamma$, $1 \leq \gamma \leq k$ *give a vector* $(\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{\theta-1})$.

Then when the codeword $\mathbf{x}_\gamma$ *runs through all the codewords in* $\mathscr{C}_\gamma$ *for each* γ, *the collection of all the vectors* $(\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{\theta-1})$ *given by* (5.16)

$$\mathscr{C} = \{(\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{\theta-1})\}$$

is a (λ, l)*-QT code over* $\mathbb{F}_q$ *of length* $l\theta$. *Conversely, every QT code over* $\mathbb{F}_q$ *of length* $l\theta$ *is obtained through this construction. Moreover, the construction can be expressed as follows:*

$$(\mathbf{c_0}, \mathbf{c_1}, \ldots, \mathbf{c}_{\theta-\mathbf{1}})^T = A \cdot \mathbf{x},$$

where $\mathbf{x}$ *is defined as in* (5.15)*,* A *is a* $\theta \times \theta$ *matrix over* $\mathbb{F}_q$ *such that, for* $0 \le i \le p^a-1$*,* $0 \le j \le \bar{\theta}-1$*,* $0 \le g \le p^a-1$*,* $1 \le \gamma \le k$*,* $0 \le w \le d_\gamma - 1$*, the entry in the* $(i+jp^a+1)$*-th row and* $(p^a \sum_{h=1}^{\gamma-1} d_h + gd_\gamma + w + 1)$*-th column, i.e., the coefficient in front of* $\mathbf{x}_{\gamma,g,w}$ *is*

$$A(i + jp^a + 1, p^a \sum_{h=1}^{\gamma-1} d_h + gd_\gamma + w + 1) = \frac{1}{\bar{\theta}}(-1)^{g-i}\binom{g}{i} Tr_\gamma((\beta\xi^{z_\gamma})^{g-i-jp^a+w}).$$

Proof. By the isomorphism in Proposition 5.4.1, $\hat{c}_{g,\gamma}$ in (5.14) can be written as $\sum_{w=0}^{d_\gamma-1}(\beta\xi^{z_\gamma})^w \mathbf{x}_{\gamma,g,w}$, and the γ-th component of $c(x)$ is $\hat{c}_{0,\gamma} + u\hat{c}_{1,\gamma} + \cdots + u^{p^a-1}\hat{c}_{p^a-1,\gamma}$. Then the theorem follows from (5.13). Obviously, the matrix A is over $\mathbb{F}_q$ because the entries are obtained by the respective trace maps down to $\mathbb{F}_q$. □

5.5 Examples

The examples in this section are computed by MAGMA [2].

The following example gives a self-dual $(2,2)$-QT code of length 24 over $\mathbb{F}_3$. We can see that its decomposition satisfies Equation (5.11) given in Theorem 5.2.11.

Example 5.5.1. *Factorize* $x^{12} - 2$ *over* $\mathbb{F}_3$ *as follows*

$$\begin{aligned} x^{12} - 2 &= (x^4 + 1)^3 \\ &= (x^2 + x + 2)^3(x^2 + 2x + 2)^3 \\ &:= h(x)h^*(x). \end{aligned}$$

Denote by $\mathbb{H}$ *the ring* $\frac{\mathbb{F}_3[x]}{((x^2+x+2)^3)}$*, and denote by* $\mathbb{H}^*$ *the ring* $\frac{\mathbb{F}_3[x]}{((x^2+2x+2)^3)}$*.*

Let $\mathscr{C}$ *be a self-dual* $(2,2)$*-QT code of length* 24 *over* $\mathbb{F}_3$ *with generator* $(h(x), h^*(x))$*. Then* $\mathscr{C}$ *can be decomposed as the direct sum of the following two component codes,* $\mathscr{C}_1$ *and* $\mathscr{C}_2$*, where:*

1. $\mathscr{C}_1$ is generated by $(0, h^*(x) \mod h(x))$ over $\mathbb{H}$ and

2. $\mathscr{C}_2$ is generated by $(h(x) \mod h^*(x), 0)$ over $\mathbb{H}^*$.

Since $h(x)$ and $h^*(x)$ are coprime, the vector $(0, 1)$ is also a generator of $\mathscr{C}_1$ over $\mathbb{H}$. For the same reason, $(1, 0)$ is a generator of $\mathscr{C}_2$ over $\mathbb{H}^*$.

It is easy to observe that the dual code $\mathscr{C}_1^{\perp_{\mathbb{H}}}$ of $\mathscr{C}_1$ over $\mathbb{H}$ is with generator $(1, 0)$ over $\mathbb{H}$. Since the isomorphism between $\mathbb{H}^2$ and $(\mathbb{H}^*)^2$ is

$$\phi' : \mathbb{H}^2 \to (\mathbb{H}^*)^2$$

$$(r_1(x) + (h(x)), r_2(x) + (h^*(x))) \mapsto (r_1(x^{-1}) + (h^*(x)), r_2(x^{-1}) + (h(x))),$$

the image of $(1, 0)$ over $\mathbb{H}$ is $(1, 0)$ over $\mathbb{H}^*$. Therefore, the image of $\mathscr{C}_1^{\perp_{\mathbb{H}}}$ under ϕ' is generated by $(1, 0)$ over $\mathbb{H}^*$, which is exactly $\mathscr{C}_2$ over $\mathbb{H}^*$. Therefore, Equation (5.11) given in Theorem 5.2.11 is satisfied.

The next example gives a QT code over $\mathbb{F}_5$ as well as that of its dual code where $\lambda \neq \pm 1$. We can see that they satisfy Equation (5.5) in Theorem 5.2.7 and their decompositions satisfy Equation (5.6) in Corollary 5.2.8.

Example 5.5.2. *Factorize $x^{15} - 2$ over $\mathbb{F}_5$ as follows*

$$\begin{aligned} x^{15} - 2 &= (x^3 + 3)^5 \\ &= (x + 2)^5 (x^2 + 3x + 4)^5 \\ &:= (f_1(x))^5 (f_2(x))^5. \end{aligned}$$

Then

$$\frac{\mathbb{F}_5[x]}{(x^{15} - 2)} \simeq \frac{\mathbb{F}_5[x]}{\big((x + 2)^5\big)} \bigoplus \frac{\mathbb{F}_5[x]}{\big((x^2 + 3x + 4)^5\big)}.$$

Denote the ring $\frac{\mathbb{F}_5[x]}{(x^{15}-2)}$ *by* $\mathbb{R}_{15,2}$*, denote the ring* $\frac{\mathbb{F}_5[x]}{\left((x+2)^5\right)}$ *by* $\mathbb{R}_1$ *and denote the ring* $\frac{\mathbb{F}_5[x]}{\left((x^2+3x+4)^5\right)}$ *by* $\mathbb{R}_2$*. Since* $2^{-1}=3$ *in* $\mathbb{F}_5$*, by Equation* (5.8)*, we have*

$$\mathbb{R}_{15,3} \simeq \mathbb{R}_1^* \bigoplus \mathbb{R}_2^*,$$

where

$$\begin{aligned}
\mathbb{R}_{15,3} &:= \frac{\mathbb{F}_5[x]}{(x^{15}-3)},\\
\mathbb{R}_1^* &:= \frac{\mathbb{F}_5[x]}{\left((x+3)^5\right)},\\
\mathbb{R}_2^* &:= \frac{\mathbb{F}_5[x]}{\left((x^2+2x+4)^5\right)}.
\end{aligned}$$

Let

$$G_1(x) = x^2+4x+4 = (x+2)^2,$$

and

$$G_2(x) = x^6+4x^5+4x^4+4x^3+x^2+4x+4 = (x^2+3x+4)^3.$$

Let $\mathscr{C}$ *be a* $(2,2)$*-QT code of length* 30 *over* $\mathbb{F}_5$ *with generator* $(G_1(x), G_2(x))$*. Then we can decompose* $\mathscr{C}$ *as the direct sum of the following two component codes,* $\mathscr{C}_1$ *and* $\mathscr{C}_2$*, where*

1. $\mathscr{C}_1$ *is generated by* $(G_1(x) \mod (f_1(x))^5, G_2(x) \mod (f_1(x))^5)$ *and*

2. $\mathscr{C}_2$ *is generated by* $(G_1(x) \mod (f_2(x))^5, G_2(x) \mod (f_2(x))^5)$.

Then $\mathscr{C}^{\perp_{\mathbb{F}_5}}$ *is a* $(3,2)$*-QT code of length* 30 *over* $\mathbb{F}_5$ *with generator* $(g_1(x), g_2(x))$ *(over*

the ring $\mathbb{R}_{15,3}$*) where*

$$\begin{aligned} g_1(x) &= 3x^{12} + 3x^{11} + 2x^{10} + 4x^9 + 4x^8 + 2x^7 + 2x^6 + 2x^4 + 3x^3 + 4x^2 + 4x + 1 \\ &= (x^2 + 2x + 4)^3(x^6 + 2x^3 + 3), \\ g_2(x) &= 4x^8 + 4x^7 + 2x^4 + 2x^2 + 4 \\ &= 4(x + 3)^2(x^3 + x^2 + 4x + 1)(x^3 + 4x^2 + 3x + 4). \end{aligned}$$

The generator $(g_1(x), g_2(x))$ *of* $\mathscr{C}^{\perp_{\mathbb{F}_5}}$ *over* $\mathbb{R}_{15,3}$ *is mapped to* $(g_1'(x), g_2'(x))$ *over* $\mathbb{R}_{15,2}$ *under the isomorphism defined as in Definition 5.2.2, where*

$$\begin{aligned} g_1'(x) &= 2x^{14} + 2x^{13} + 4x^{12} + x^{11} + x^9 + x^8 + 2x^7 + 2x^6 + x^5 + 4x^4 + 4x^3 + 1, \\ g_2'(x) &= x^{13} + x^{11} + 2x^8 + 2x^7 + 4. \end{aligned}$$

Then the image of $\mathscr{C}^{\perp_{\mathbb{F}_5}}$ *can be decomposed as the direct sum of the following two component codes,* $\mathscr{D}_1$ *and* $\mathscr{D}_2$*, where*

1. $\mathscr{D}_1$ *is generated by* $(g_1'(x) \mod (f_1(x))^5, g_2'(x) \mod (f_1(x))^5)$ *and*

2. $\mathscr{D}_2$ *is generated by* $(g_1'(x) \mod (f_2(x))^5, g_2'(x) \mod (f_2(x))^5)$.

Notice that

$$\begin{aligned} g_1'(x)G_1(x) + g_2'(x)G_2(x) &\equiv x^{19} + 4x^{18} + 3x^4 + 2x^3 \mod (x^{15} - 2) \\ &\equiv 0 \mod (x^{15} - 2). \end{aligned}$$

Therefore, Equation (5.5) *in Theorem 5.2.7 is satisfied.*

Since both $(f_1(x))^5$ *and* $(f_2(x))^5$ *are divisors of* $(x^{15}-2)$ *over* $\mathbb{F}_5$*, we have*

$$
\begin{aligned}
&< (g_1'(x), g_2'(x)), (G_1(x), G_2(x)) >_{\mathbb{R}_{15,2}} \\
=&(g_1'(x)G_1(x) + g_2'(x)G_2(x)) \mod (x^{15}-2) \\
=&0, \\
&< (g_1'(x) \mod (f_1(x))^5, g_2'(x) \mod (f_1(x))^5), (G_1(x) \mod (f_1(x))^5, G_2(x) \mod (f_1(x))^5) >_{\mathbb{R}_1} \\
=&(g_1'(x)G_1(x) + g_2'(x)G_2(x)) \mod (f_1(x))^5 \\
=&0, \\
&< (g_1'(x) \mod (f_2(x))^5, g_2'(x) \mod (f_2(x))^5), (G_1(x) \mod (f_2(x))^5, G_2(x) \mod (f_2(x))^5) >_{\mathbb{R}_2} \\
=&(g_1'(x)G_1(x) + g_2'(x)G_2(x)) \mod (f_2(x))^5 \\
=&0.
\end{aligned}
$$

Therefore, the decomposition of the image of $\mathscr{C}^{\perp_{\mathbb{F}_5}}$ *satisfies Equation* (5.6) *in Corollary 5.2.8.*

The following example shows the decomposition of a $(2,2)$-QT code of length 30 over $\mathbb{F}_3$ using GDFT.

Example 5.5.3. *Factorize* $x^{15}-2$ *over* $\mathbb{F}_3$ *as follows*

$$x^{15}-2 = (x^5+1)^3 = (x+1)^3(x^4+2x^3+x^2+2x+1)^3. \tag{5.17}$$

Let

$$G_1(x) = (x+1)^2(x^4+2x^3+x^2+2x+1)$$

and

$$G_2(x) = (x+1)(x^4+2x^3+x^2+2x+1)^2.$$

Therefore,

$$
\begin{aligned}
\frac{\mathbb{F}_3[x]}{(x^{15}-2)} &\simeq \frac{\mathbb{F}_3[x]}{(x+1)^3} \bigoplus \frac{\mathbb{F}_3[x]}{(x^4+2x^3+x^2+2x+1)^3} \\
&\simeq (\mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3) \bigoplus (\mathbb{F}_{3^4} + u\mathbb{F}_{3^4} + u^2\mathbb{F}_{3^4}).
\end{aligned}
$$

For simplicity, denote $\frac{\mathbb{F}_3[x]}{(x^{15}-2)}$ *by* $\mathbb{R}$, $(\mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3)$ *by* J_1 *and* $(\mathbb{F}_{3^4} + u\mathbb{F}_{3^4} + u^2\mathbb{F}_{3^4})$ *by* J_2.

Set a root of $x^5 + 1$*:* $\beta = 2$*. Let* ξ *be a* 5*-th primitive root of unity.*

Since $\beta^{3-1} = 1 = \xi^5$*, the map*

$$\tau : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$$

$$z \mapsto 3z + 5,$$

defines two orbits: $\mathbf{O}_1 = \{0\}$ *and* $\mathbf{O}_2 = \{1, 3, 4, 2\}$*. It is easily checked that* β *is the root of* $x + 1$ *while* $\beta\xi, \beta\xi^2, \beta\xi^3, \beta\xi^4$ *are the roots of* $x^4 + 2x^3 + x^2 + 2x + 1$*. Therefore, the orbit* $\mathbf{O_1}$ *corresponds to the polynomial* $x + 1$ *while the orbit* $\mathbf{O_2}$ *corresponds to the polynomial* $x^4 + 2x^3 + x^2 + 2x + 1$ *in* (5.17).

Let $\mathscr{C}$ *be the* $(2, 2)$*-QT code of length* 30 *over* $\mathbb{F}_3$ *and let the generator of its corresponding* $\mathbb{R}$*-submodule of* $\mathbb{R}^2$ *be* $(G_1(x), G_2(x))$*. Then* $\mathscr{C}$ *can be decomposed as direct sum of a code over* J_1 *and another code over* J_2.

For the codeword $(G_1(x), G_2(x)) \in \mathscr{C}$*,* $\hat{G}_1, \hat{G}_2$ *are two matrices of size* 3×5 *as defined in* (5.12)*, where*

$$\hat{G}_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 2 + 2(2\xi) + (2\xi)^2 + 2(2\xi)^3 & 1 + (2\xi)^3 & 1 + 2(2\xi)^2 & 1 + (2\xi) \\ 2 & (2\xi)^3 & 2\xi & 1 + 2(2\xi) + (2\xi)^2 + 2(2\xi)^3 & 2(2\xi)^2 \end{bmatrix},$$

and

$$\hat{G}_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 2 & 1 + (2\xi) + (2\xi)^3 & 1 + (2\xi) + 2(2\xi)^2 & 2 + 2(2\xi) + (2\xi)^2 & 2 + 2(2\xi) + 2(2\xi)^3 \end{bmatrix}.$$

Let $\mathscr{C}_1$ be the J_1-linear code of length 2 with the generator

$$(2u^2, u + 2u^2)$$

over J_1 and let $\mathscr{C}_2$ be the J_2-linear code of length 2 with the generator

$$((2 + 2(2\xi) + (2\xi)^2 + 2(2\xi)^3)u + ((2\xi)^3)u^2, (1 + (2\xi) + (2\xi)^3)u^2)$$

over J_2. Then $\mathscr{C} \simeq \mathscr{C}_1 \bigoplus \mathscr{C}_2$.

The following example shows construction of $\mathscr{C}$ from $\mathscr{C}_1$ and $\mathscr{C}_2$ where $\mathscr{C}$, $\mathscr{C}_1$ and $\mathscr{C}_2$ are as in the above example.

Example 5.5.4. *Given the generator $(2u^2, u + 2u^2) \in \mathscr{C}_1$, its associated matrix $\tilde{\mathbf{x_1}}$ defined as in (5.15) is*

$$\tilde{\mathbf{x_1}} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 2 & 2 \end{bmatrix}.$$

The matrix $\tilde{x_2}$ associated to the generator

$$((2 + 2(2\xi) + (2\xi)^2 + 2(2\xi)^3)u + ((2\xi)^3)u^2, (1 + (2\xi) + (2\xi)^3)u^2) \in \mathscr{C}_2$$

is

$$\tilde{\mathbf{x_2}} = \begin{bmatrix} 0 & 0 & 0 & 0 & 2 & 2 & 1 & 2 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}^T.$$

Then

$$\mathbf{x} = \begin{bmatrix} 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 1 & 2 & 0 & 0 & 0 & 1 \\ 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}^T.$$

By Theorem 5.4.2, the matrix A is given as follows

$$\begin{bmatrix}
2 & 2 & 2 & 2 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 1 \\
0 & 2 & 1 & 0 & 0 & 0 & 0 & 2 & 2 & 1 & 2 & 2 & 1 & 2 & 1 \\
0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 1 & 2 \\
1 & 1 & 1 & 2 & 1 & 2 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 2 & 1 \\
0 & 1 & 2 & 0 & 0 & 0 & 0 & 2 & 1 & 2 & 2 & 1 & 2 & 2 & 2 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 2 & 2 \\
2 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 2 & 1 & 2 & 1 & 2 \\
0 & 2 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 1 & 1 & 2 & 1 \\
0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 \\
1 & 1 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 2 & 2 & 1 & 1 & 1 \\
0 & 1 & 2 & 0 & 0 & 0 & 0 & 2 & 1 & 2 & 1 & 1 & 2 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 2 & 1 \\
2 & 2 & 2 & 1 & 2 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 2 \\
0 & 2 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 1 \\
0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2
\end{bmatrix}.$$

Then

$$A\mathbf{x} = \begin{bmatrix}
1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 2 & 1 & 2 & 1 & 1 & 2 & 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}^T,$$

whose columns are exactly the coefficients of $G_1(x)$ and $G_2(x)$, respectively. $(G_1(x), G_2(x))$ is the generator of the quasi-twisted code $\mathscr{C}$ in the previous example.

5.6 Conclusion

In this chapter, we study the quasi-twisted (QT) codes both in the nonrepeated-root and repeated-root cases. Based on the factorization of the polynomial $x^\theta - \lambda$ over $\mathbb{F}_q$, the decomposition of a (λ, l)-QT code of length $l\theta$ over $\mathbb{F}_q$ is given as a direct sum of linear codes over the component rings. Furthermore, the connection between the decomposition of a QT code and that of its dual code is explicitly described. In particular, the decomposition of a self-dual QT code is given. We also study the generalized discrete Fourier transform (GDFT) and its inverse formula, which are applied to both the nonrepeated-root and repeated-root cases. Finally, by the inverse formula of GDFT, we produce a formula to construct a QT code from linear codes over rings, as shown in Example 5.5.4.

Bibliography

[1] N. Aydin, I. Siap, and D. K. Ray-Chaudhuri, "The structure of 1-generator quasi-twisted codes and new linear codes," Designs, Codes and Cryptography 24, no. 3, pp. 313–326, 2001.

[2] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system. I. The user language," J. Symbolic Comput, 24(3-4), pp. 235–265, 1997.

[3] R. N. Daskalov and T. A. Gulliver, "New ternary linear codes," IEEE Trans. Inform. Theory, vol. 45, no. 5, pp. 1687–1688, 1999.

[4] T. A. Gulliver and M. Harada, "New nonbinary self-dual codes," IEEE Trans. Inform. Theory, vol. 54, no. 1, pp. 415–417, 2008.

[5] W. C. Huffman and V. Pless, Fundamentals of error-correcting codes, Cambridge Univ. Press, 2003.

[6] J. M. Jensen, "A class of constacyclic codes," IEEE Trans. Inform. Theory, vol. 40, no. 3, pp. 951–954, 1994.

[7] X. Kai and S. Zhu, "On cyclic self-dual codes," AAECC, vol. 19, pp. 275–281, 2004.

[8] R. Lidl and H. Niederreiter, Finite Fields, Cambridge Univ. Press, Cambridge, 1997

[9] C.J. Lim, "Consta-abelian polyadic codes," IEEE Trans. Inform. Theory, vol. 51, no. 6, pp. 2198–2206, 2005.

[10] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes I: Finite Fields," IEEE Trans. Inform. Theory, vol. 47, pp. 2751–2760, 2001

[11] S. Ling, H. Niederreiter, and P. Solé, "On the algebraic structure of quasi-cyclic codes IV: repeated roots," Designs, Codes and Cryptography 38, no. 3, pp. 337–361, 2006.

[12] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes II: chain rings," Designs, Codes and Cryptography 30, pp. 113–130, 2003.

[13] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes III: generator theory," IEEE Trans. Inform. Theory, vol. 51, pp. 2692–2700, 2005.

[14] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland Mathematical Library, 2003

[15] J. L. Massey and S. Serconek, "Linear complexity of periodic sequences: a general theory," Advances in Cryptology-Crypto 96 (N. Koblitz ed.), LNCS 1109, pp. 358–371, 1996.

[16] H. F. Mattson, Jr. and G. Solomon, "A new treatment of Bose-Chaudhuri codes," J. Soc. Indust. Appl. Math., vol. 9, pp. 654–668, 1961

[17] C. Mihoubi and P. Solé, "Codes cycliques optimaux de rendement $\frac{1}{2}$ sur GF(5)," International Journal of Open Problems in Computer Science and Mathematics, Appear soon.

[18] P. Moree, "On the divisors of $a^k + b^k$," Acta Arithmetica, LXXX.3, pp. 197–212, 1997

[19] E. Petrank and R. M. Roth, "Is code equivalence easy to decide?," IEEE Trans. Inform. Theory, vol. 43, pp. 1602–1604, 1997.

[20] V. Pless, Handbook of coding theory, volume I, North-Holland, Elsevier, 1998.

[21] V. Pless, P. Solé, Z. Qian, "Cyclic self-dual Z_4-codes," IEEE International Symposium on Information Theory-Proceedings, p. 200, 1997

[22] H-G. Quebbemann, "On even codes", Discrete Mathematics, pp. 29–34, 1991

[23] M. K. Siu, "When is -1 a power of 2?," Math. Mag., vol. 48, no. 5, pp. 284–286, 1975

[24] N. J. A. Sloane, "The On-Line Encyclopedia of Integer Sequences," Notices of the American Mathematical Society, vol. 50 (8), pp. 912–915, http://www.ams.org/notices/200308/comm-sloane.pdf, 2003

[25] N. J. A. Sloane and J.G.Thompson, "Cyclic self-dual codes," IEEE Transactions on Information Theory, vol. IT-29 (3), pp. 364–366, 1983

[26] K. Wiertalak, "On the density of some sets of primes," I, II, Acta Arith., vol. 34, pp. 183–196 & pp. 197–210, 1977/78

[27] J. L. Yucas and G. L. Mullen, "Self-reciprocal irreducible polynomials over finite fields", Designs, Codes and Cryptography, vol. 33, pp. 275–281, 2004