EQUIVALENT DUALS OF CYCLIC CODES OVER FINITE FIELDS

By

Jareena Tharnnukhroh

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree
Master of Science Program in Mathematics
Department of Mathematics
Graduate School, Silpakorn University
Academic Year 2015

EQUIVALENT DUALS OF CYCLIC CODES OVER FINITE FIELDS

By
Jareena Tharnnukhroh

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree
Master of Science Program in Mathematics
Department of Mathematics
Graduate School, Silpakorn University
Academic Year 2015

คู่กันแบบสมมูลของรหัสวัฏจักรบนฟีลด์จำกัด

โดย

นางสาวจารีนา ธารนุเคราะห์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์
ภาควิชาคณิตศาสตร์
บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร
ปีการศึกษา 2558

The Graduate School, Silpakorn University has approved and accredited the Thesis title of "Equivalent Duals of Cyclic Codes over Finite Fields" submitted by Miss Jareena Tharnnukhroh as a partial fulfillment of the requirements for the degree of Master of Science in Mathematics

…..

(Associate Professor Panjai Tantatsanawong, Ph.D.)

Dean of Graduate School

........../..................../..........

The Thesis Advisor

Somphong Jitman, Ph.D.

The Thesis Examination Committee

.... Chairman

(Associate Professor Nawarat Ananchuen, Ph.D.)

............/......................../.............

.... Member

(Associate Professor Patanee Udomkavanich, Ph.D.)

............/......................../.............

.... Member

(Somphong Jitman, Ph.D.)

............/......................../.............

56305202 : MAJOR : MATHEMATICS
KEY WORDS : DUAL CODES / EQUIVALENT CODES / CYCLIC CODES

JAREENA THARNNUKHROH : EQUIVALENT DUALS OF CYCLIC CODES OVER FINITE FIELDS. THESIS ADVISOR : SOMPHONG JITMAN, Ph.D. 37 pp.

The ℓ-equivalent dual of a linear code C over a finite field is introduced as a generalization of the Euclidean and Hermitian duals of C. The ℓ-equivalent dual of a cyclic code C is studied and its generator polynomial is determined. Necessary and sufficient conditions for a cyclic code over a finite field to be ℓ-isodual and to be ℓ-complementary dual are given in terms of its generator polynomial. The characterization of the existence of an ℓ-isodual cyclic code of length n over $\mathbb{F}_{p^m}$ is also determined. The enumeration of ℓ-isodual cyclic codes of length n over $\mathbb{F}_{p^m}$ is given. In some cases, the enumerations of ℓ-complementary dual cyclic codes of length n is provided as well.

Department of Mathematics Graduate School, Silpakorn University

Student's signature .... Academic Year 2015

Thesis Advisor's signature ....

56305202 : สาขาวิชาคณิตศาสตร์

คำสำคัญ : รหัสคู่กัน / รหัสสมมูล / รหัสวัฏจักร

จารีนา ธารนุเคราะห์ : คู่กันแบบสมมูลของรหัสวัฏจักรบนฟีลด์จำกัด. อาจารย์ที่ปรึกษาวิทยานิพนธ์ : ดร. สมพงค์ จิตต์มั่น. 37 หน้า.

เราให้บทนิยามของรหัสคู่กันแบบสมมูลอันดับ ℓ ของรหัสเชิงเส้น C บนฟีลด์จำกัด ซึ่งเป็นนัยทั่วไปของคู่กันแบบยุคลิดและคู่กันแบบแอร์มีตของ C ศึกษาคู่กันแบบสมมูลอันดับ ℓ ของรหัสวัฏจักร C และแสดงพหุนามก่อกำเนิดของรหัสนี้ด้วย พร้อมทั้งให้เงื่อนไขที่จำเป็นและเพียงพอของการเกิดรหัสวัฏจักรคู่กันแบบสมมูลในตัวอันดับ ℓ และรหัสคู่กันแบบสมมูลเติมเต็มอันดับ ℓ ในเทอมของพหุนามก่อกำเนิดของรหัส เราจำแนกการมีจริงของรหัสวัฏจักรคู่กันแบบสมมูลในตัวอันดับ ℓ ที่มีความยาว n บนฟีลด์ $\mathbb{F}_{p^m}$ และนับจำนวนของรหัสวัฏจักรคู่กันแบบสมมูลในตัวอันดับ ℓ ที่มีความยาว n บนฟีลด์ $\mathbb{F}_{p^m}$ นอกจากนี้ สำหรับบางกรณีเรานับจำนวนของรหัสวัฏจักรคู่กันสมมูลแบบเติมเต็มอันดับ ℓ ที่มีความยาว n

ภาควิชาคณิตศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร

ลายมือชื่อนักศึกษา.. ปีการศึกษา 2558

ลายมือชื่ออาจารย์ที่ปรึกษาวิทยานิพนธ์ ....

Acknowledgements

This thesis has been completed by the involvement of people about whom I would like to mention here.

I would like to thank Dr. Somphong Jitman, my advisor, for his helpful suggestions, valuable comments and precious supports throughout the study with great attention.

I would like to thank Assoc. Prof. Dr. Nawarat Ananchuen and Assoc. Prof. Dr. Patanee Udomkavanich, chairman and member of the thesis committee, for their valuable comments and suggestions.

I would like to thank the Development and Promotion of Science and Technology Talents Project (DPST) for the financial support throughout my undergraduate and graduate studies.

Finally, I would like to express my gratitude to my family and my friends for their understanding, encouragement and moral support during the study.

Table of Contents

Page

Chapter 1

Introduction

Due to their rich algebraic structures and various applications, cyclic codes over finite fields have been extensively studied for more than a half century (see [1], [2], [4], [8] and references therein). The study of Euclidean and Hermitian duals of codes is another interesting problem since the duals play an important role in applications and links to other objects in Mathematics. Especially, Euclidean (resp., Hermitian) self-dual codes and Euclidean (resp., Hermitian) complementary dual codes have been applied in constructions of secret sharing schemes and quantum codes (see [1], [5], [8], [9] and [10]). As in the discussion above, cyclic codes, self-dual codes and complementary dual codes are important classes of linear codes. These have motivated the study of self-dual cyclic codes and complementary dual cyclic codes in [2], [4] and [12].

For a given finite field $\mathbb{F}_{p^m}$, denote by $\mathrm{Aut}(\mathbb{F}_{p^m})$ the automorphism group of $\mathbb{F}_{p^m}$. It is well known (see [6, Theorem 2.21]) that $\mathrm{Aut}(\mathbb{F}_{p^m})$ is a cyclic group of order m generated by the Frobenius automorphism θ, where $\theta(a) = a^p$ for all $a \in \mathbb{F}_{p^m}$. We introduce a generalized notion of the Euclidean and Hermitian duals of a linear code C of length n over $\mathbb{F}_{p^m}$ as follows. For each integer $0 \leq \ell < m$, the *ℓ-equivalent dual* $\theta^\ell(C^\perp)$ of C is defined to be the set

$$\theta^\ell(C^\perp) := \{(\theta^\ell(c_0), \theta^\ell(c_1), \ldots, \theta^\ell(c_{n-1})) \mid (c_0, c_1, \ldots, c_{n-1}) \in C^\perp\},$$

where $C^{\perp}$ denotes the Euclidean dual of C. It is not difficult to see that if $\ell = 0$ (resp., m is even and $\ell = \frac{m}{2}$), then the ℓ-equivalent dual of a code is just its Euclidean (resp., Hermitian) dual.

In this thesis, we focus on the ℓ-equivalent dual of cyclic codes. The algebraic structure of the ℓ-equivalent dual of cyclic codes is investigated as well as the characterization of the following two families of cyclic codes: 1) the family of cyclic codes with the property that a code and its ℓ-equivalent dual are exactly the same, and, 2) the family of cyclic codes with the property that a code and its dual are complement of each other. The two families are generalizations of self-dual cyclic codes and complementary dual cyclic codes called *ℓ-isodual cyclic codes* and *ℓ-complementary dual cyclic codes*, respectively.

The thesis is organized as follows. Some definitions and basic properties of polynomials and codes over finite fields are recalled in Chapter 2. In Chapter 3, the generator polynomial of ℓ-equivalent dual of a cyclic code C of length n over $\mathbb{F}_{p^m}$ is studied. Cyclic codes with ℓ-isodual are studied in Chapter 4. Necessary and sufficient conditions for a cyclic code of length n over a finite field to be ℓ-isodual are given as well as the characterization and enumeration of ℓ-isodual cyclic codes of length n over $\mathbb{F}_{p^m}$. In Chapter 5, the characterization of ℓ-complementary dual cyclic codes is given in terms of their generator polynomials. In some cases, the enumeration of ℓ-complementary dual cyclic codes is provided as well.

Chapter 2

Preliminaries

In this chapter, we recall some basic properties of polynomials and codes over finite fields and introduce the ℓ-equivalent dual of a code.

2.1 Polynomials and Codes

Let $\mathbb{F}_{p^m}$ denote the finite field of order p^m, where p is a prime and m is a positive integer. A *linear code* C of length n over $\mathbb{F}_{p^m}$ is defined a subspace of the $\mathbb{F}_{p^m}$-vector space $\mathbb{F}_{p^m}^n$. A linear code of length n over $\mathbb{F}_{p^m}$ is called an $[n,k]_{p^m}$ *code* if its $\mathbb{F}_{p^m}$-dimension is k. An element $\boldsymbol{c} := (c_0, c_1, \ldots, c_{n-1})$ in C is called a *codeword*.

For $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ and $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$ in $\mathbb{F}_{p^m}^n$, the *Euclidean inner product* of $\boldsymbol{u}$ and $\boldsymbol{v}$ is defined to be

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle := \sum_{i=1}^{n} u_i v_i.$$

For a code C of length n over $\mathbb{F}_{p^m}$, denote by $C^\perp$ the Euclidean dual of C, *i.e.*,

$$C^\perp = \{\boldsymbol{v} \in \mathbb{F}_{p^m}^n \mid \langle \boldsymbol{c}, \boldsymbol{v} \rangle = 0 \text{ for all } \boldsymbol{c} \in C\}.$$

A code C is said to be *Euclidean self-dual* if $C = C^\perp$ and it is said to be *Euclidean complementary dual* if $C \cap C^\perp = \{0\}$.

If, in addition, m is even, then the *Hermitian inner product* of $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ and $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$ in $\mathbb{F}_{p^m}^n$ is defined to be

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle_H := \sum_{i=1}^{n} u_i v_i^{p^{\frac{m}{2}}}.$$

The *Hermitian dual* $C^{\perp_H}$ of C is defined to be the set

$$C^{\perp_H} = \{\boldsymbol{v} \in \mathbb{F}_{p^m}^n \mid \langle \boldsymbol{c}, \boldsymbol{v} \rangle_H = 0 \text{ for all } \boldsymbol{c} \in C\}.$$

A code C is said to be *Hermitian self-dual* if $C = C^{\perp_H}$ and it is said to be *Hermitian complementary dual* if $C \cap C^{\perp_H} = \{0\}$.

An $[n, k]_{p^m}$ code C is called *cyclic* if, for each codeword $\boldsymbol{c} = (c_0, c_1, \ldots, c_{n-1})$ in C, the vector $(c_{n-1}, c_0, \ldots, c_{n-2})$ is also a codeword in C. It is well known [7, Chapter 7] that every cyclic code of length n over $\mathbb{F}_{p^m}$ can be identified with an ideal in the principal ideal ring $\mathbb{F}_{p^m}[x]/\langle x^n - 1 \rangle$. Moreover, a (non-zero) cyclic code is generated by a unique monic divisor $g(x)$ of $x^n - 1$. Such the polynomial is called the *generator polynomial* of C. A codeword $\boldsymbol{c} = (c_0, c_1, \ldots, c_{n-1})$ will be represented by its *representation polynomial* $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$.

A relation between the dimension of a cyclic code C and the degree of its generator polynomial is given as follows.

Proposition 2.1 ([7, Theorem 7.2.14])**.** *Let C be a cyclic code of length n over $\mathbb{F}_{p^m}$ and $g(x)$ be the generator polynomial of C. If $g(x)$ has degree $n - k$, then* $\dim(C) = k$.

For each $f(x) = a_b x^b + \cdots + a_1 x + a_0 \in \mathbb{F}_{p^m}[x]$ of degree b with $a_0 \neq 0$, let

$$\begin{aligned}\widetilde{f(x)} &= x^{\deg f(x)} f\left(\frac{1}{x}\right)\\ &= x^b \left(a_b x^{-b} + \cdots + a_1 x^{-1} + a_0\right)\\ &= a_0 x^b + a_1 x^{b-1} + \cdots + a_{b-1} x + a_b.\end{aligned}$$

The *reciprocal polynomial of* $f(x)$ is defined to be $f^*(x) = a_0^{-1}\widetilde{f(x)}$. In the case where m is even, the *conjugate-reciprocal polynomial of* $f(x)$ is defined to be

$$f^\dagger(x) = a_0^{-p^{\frac{m}{2}}} \left(a_0^{p^{\frac{m}{2}}} x^b + a_1^{p^{\frac{m}{2}}} x^{b-1} + \cdots + a_{b-1}^{p^{\frac{m}{2}}} x + a_b^{p^{\frac{m}{2}}}\right).$$

The generator polynomial of the Euclidean dual of a cyclic code can be determined as follows.

Proposition 2.2 ([7, Theorem 7.3.7])**.** *Let C be an $[n,k]_{p^m}$ cyclic code generated by $g(x)$ and let $h(x) = \frac{x^n-1}{g(x)}$. Then $C^{\perp}$ is generated by $h^*(x)$.*

Corollary 2.3. *Let C be an $[n,k]_{p^m}$ cyclic code generated by $g(x)$ and let $h(x) = \frac{x^n-1}{g(x)}$. Then C is Euclidean self-dual if and only if $g(x) = h^*(x)$.*

In the same fashion, the generator polynomial of the Hermitian dual of a cyclic code can be obtained.

Proposition 2.4. *Let m be an even positive integer and let C be an $[n,k]_{p^m}$ cyclic code generated by $g(x)$. Let $h(x) = \frac{x^n-1}{g(x)}$. Then $C^{\perp_H}$ is generated by $h^{\dagger}(x)$.*

Corollary 2.5. *Let m be an even positive integer and let C be an $[n,k]_{p^m}$ cyclic code generated by $g(x)$. Let $h(x) = \frac{x^n-1}{g(x)}$. Then C is Hermitian self-dual if and only if $g(x) = h^{\dagger}(x)$.*

For each pair of nonzero polynomials $f(x)$ and $g(x)$ in $\mathbb{F}_{p^m}[x]$, the *greatest common divisor* of $f(x)$ and $g(x)$, denoted by $\gcd(f(x), g(x))$, is defined to be a monic polynomial $d(x)$ that divides $f(x)$ and $g(x)$ such that every common divisor of $f(x)$ and $g(x)$ also divides $d(x)$. Similarly, the *least common multiple* $\operatorname{lcm}(f(x), g(x))$ of $f(x)$ and $g(x)$ is defined to be a monic polynomial $m(x)$ that is a multiple of $f(x)$ and $g(x)$ such that every common multiple of $f(x)$ and $g(x)$ is a multiple of $m(x)$. The greatest common divisor and least common multiple of polynomials play an important role in determining the generator polynomial of cyclic codes in Chapter 5.

2.2 The ℓ-Equivalent Duals of Codes

Denote by $\mathrm{Aut}(\mathbb{F}_{p^m})$ the automorphism group of $\mathbb{F}_{p^m}$. It is well known (see [6, Theorem 2.21]) that $\mathrm{A}ut(\mathbb{F}_{p^m}) = \{\theta^l \mid 0 \leq l<m\}$, where θ is the Frobenius automorphism defined by $\theta(a) = a^p$ for all $a \in \mathbb{F}_{p^m}$.

For each $0 \leq \ell < m$, let $\theta^\ell : \mathbb{F}_{p^m}^n \to \mathbb{F}_{p^m}^n$ be a linear isomorphism on $\mathbb{F}_{p^m}^n$ extended form $\theta^\ell \in \mathrm{Aut}(\mathbb{F}_{p^m})$ by

$$\theta^\ell((c_0, c_1, \ldots, c_{n-1})) = (\theta^\ell(c_0), \theta^\ell(c_1), \ldots, \theta^\ell(c_{n-1})).$$

Remark 2.6. For a linear code C, the map $\theta^\ell|_C : C \to \theta^\ell(C)$ is a linear isomorphism. Hence, $\dim(C) = \dim(\theta^\ell(C))$.

For $0 \leq \ell < m$, we call $\theta^\ell(C^\perp)$ the *ℓ-equivalent dual* of C. A code C is said to be *ℓ-isodual* if $C = \theta^\ell(C^\perp)$, and it is said to be *ℓ-complementary dual* if $C \cap \theta^\ell(C^\perp) = \{0\}$.

Example 2.7. Consider $n = 2$, $p = 2$ and $m = 3$. Let $\mathbb{F}_{2^3}$ be the finite field of order 8 with primitive element α.
Let $C = \{00, 1\alpha, \alpha\alpha^2, \alpha^2\alpha^3, \alpha^3\alpha^4, \alpha^4\alpha^5, \alpha^5\alpha^6, \alpha^6 1\} \subseteq \mathbb{F}_{2^3}^2$ be a linear code of length 2 over $\mathbb{F}_{2^3}$. Then

$$\begin{aligned} C^\perp = \theta^0(C^\perp) &= \{00, \alpha 1, \alpha^2\alpha, \alpha^3\alpha^2, \alpha^4\alpha^3, \alpha^5\alpha^4, \alpha^6\alpha^5, 1\alpha^6\}, \\ \theta^1(C^\perp) &= \{00, \alpha^2 1, \alpha^4\alpha^2, \alpha^6\alpha^4, \alpha\alpha^6, \alpha^3\alpha, \alpha^5\alpha^3, 1\alpha^5\} \\ \text{and} \quad \theta^2(C^\perp) &= \{00, \alpha^4 1, \alpha\alpha^4, \alpha^5\alpha, \alpha^2\alpha^5, \alpha^6\alpha^2, \alpha^3\alpha^6, 1\alpha^3\}. \end{aligned}$$

Remark 2.8. The concept of ℓ-equivalent duals generalizes the concepts of Euclidean and Hermitian duals of codes as follows.

1. If $\ell = 0$, then $\theta^\ell(C^\perp) = C^\perp$. Hence, an ℓ-isodual (resp., ℓ-complementary dual) code is just a Euclidean self-dual (resp., Euclidean complementary dual) code.

2. If m is even and $\ell = \frac{m}{2}$, then $\theta^\ell(C^\perp) = C^{\perp_H}$. Hence, an ℓ-isodual (resp., ℓ-complementary dual) code is just a Hermitian self-dual (resp., Hermitian complementary dual) code.

We have the following property of ℓ-equivalent dual of codes.

Proposition 2.9. *Let C be a linear code of length n over $\mathbb{F}_{p^m}$. Then $(\theta^\ell(C))^\perp = \theta^\ell(C^\perp)$ for all $0 \leq \ell < m$.*

Proof. Let $\boldsymbol{a} \in \theta^\ell(C^\perp)$ and let $\boldsymbol{c} \in \theta^\ell(C)$. We have $\boldsymbol{a} = (a_0^{p^\ell}, a_1^{p^\ell}, \dots, a_{n-1}^{p^\ell})$ and $\boldsymbol{c} = (c_0^{p^\ell}, c_1^{p^\ell}, \dots, c_{n-1}^{p^\ell})$ for some $(a_0, a_1, \dots, a_{n-1}) \in C^\perp$ and $(c_0, c_1, \dots, c_{n-1}) \in C$. Then

$$\begin{aligned}\langle \boldsymbol{a}, \boldsymbol{c} \rangle &= a_0^{p^\ell} c_0^{p^\ell} + a_1^{p^\ell} c_1^{p^\ell} + \cdots + a_{n-1}^{p^\ell} c_{n-1}^{p^\ell} \\ &= (a_0c_0 + a_1c_1 + \cdots + a_{n-1}c_{n-1})^{p^\ell} \\ &= 0.\end{aligned}$$

This implies that $\boldsymbol{a} \in (\theta^\ell(C))^\perp$, and hence, $\theta^\ell(C^\perp) \subseteq (\theta^\ell(C))^\perp$. By Remark 2.6, we have

$$\dim(\theta^\ell(C^\perp)) = \dim(C^\perp),$$

and hence,

$$\dim((\theta^\ell(C))^\perp) = n - \dim(\theta^\ell(C)) = n - \dim(C) = \dim(C^\perp) = \dim(\theta^\ell(C^\perp)).$$

Therefore, $(\theta^\ell(C))^\perp = \theta^\ell(C^\perp)$ as desired. □

Corollary 2.10. *Let C be a linear code over $\mathbb{F}_{p^m}$. Then C is ℓ-isodual if and only if $C^\perp$ is ℓ-isodual.*

Proof. Assume that C is ℓ-isodual. Then we have $C = \theta^\ell(C^\perp)$. By Proposition 2.9, we have $C^\perp = (\theta^\ell(C^\perp))^\perp = \theta^\ell((C^\perp)^\perp) = \theta^\ell(C)$. Thus, $C^\perp$ is ℓ-isodual.

Conversely, suppose that $C^\perp$ is ℓ-isodual. We obtain $C^\perp = \theta^\ell((C^\perp)^\perp) = \theta^\ell(C)$. Then $C = (C^\perp)^\perp = (\theta^\ell(C))^\perp = \theta^\ell(C^\perp)$ by Proposition 2.9. Hence, C is ℓ-isodual. □

Corollary 2.11. *Let C be a linear code over $\mathbb{F}_{p^m}$. Then C is ℓ-complementary dual if and only if $C^\perp$ is ℓ-complementary dual.*

Proof. Assume that C is ℓ-complementary dual. Then we have $C \cap \theta^\ell(C^\perp) = \{0\}$. Since $\mathbb{F}_{p^m}^n = \{0\}^\perp = (C \cap \theta^\ell(C^\perp))^\perp = C^\perp \oplus (\theta^\ell(C^\perp))^\perp = C^\perp \oplus \theta^\ell(C)$, we have $C^\perp \cap \theta^\ell(C) = \{0\}$. Hence, $C^\perp$ is ℓ-complementary dual.

Conversely, suppose that $C^\perp$ is ℓ-complementary dual . We obtain $C^\perp \cap \theta^\ell(C) = \{0\}$. Since $\mathbb{F}_{p^m}^n = \{0\}^\perp = (C^\perp \cap \theta^\ell(C))^\perp = C \oplus \theta^\ell(C^\perp)$, we have $C \cap \theta^\ell(C^\perp) = \{0\}$. Therefore, C is ℓ-complementary dual. □

Chapter 3

The ℓ-Equivalent Duals of Cyclic Codes

In this chapter, we focus on the ℓ-equivalent dual of cyclic codes. The generator polynomial of such codes is determined.

Given a polynomial $f(x) = a_b x^b + \cdots + a_1 x + a_0 \in \mathbb{F}_{p^m}[x]$ and an integer $0 \leq \ell < m$, denote by $\theta^\ell(f(x))$ the image of $f(x)$ by applying θ^ℓ on the coefficients of $f(x)$, *i.e.*,

$$\theta^\ell(f(x)) = \theta^\ell(a_b)x^b + \cdots + \theta^\ell(a_1)x + \theta^\ell(a_0).$$

Lemma 3.1. *Let $f(x) = \sum_{i=0}^{r} a_i x^i$ and $g(x) = \sum_{i=0}^{s} b_i x^i$ be polynomials in $\mathbb{F}_{p^m}[x]$. Then the following statements hold.*

i) *$\theta^\ell(f(x)g(x)) = \theta^\ell(f(x))\theta^\ell(g(x))$ for all $0 \leq \ell < m$.*

ii) *If $a_0 \neq 0$ and $b_0 \neq 0$, then $(f(x)g(x))^* = f^*(x)g^*(x)$.*

iii) *If $a_0 \neq 0$ and $b_0 \neq 0$, then $\theta^\ell\left((f(x)g(x))^*\right) = \theta^\ell\left(f^*(x)\right)\theta^\ell\left(g^*(x)\right)$ for all $0 \leq \ell < m$.*

Proof. Since $f(x)g(x) = \sum_{k=0}^{r+s}\left(\sum_{k=i+j} a_i b_j\right)x^k$ and θ^ℓ is an automorphism, we have

$$\begin{aligned}\theta^{\ell}(f(x)g(x)) &= \sum_{k=0}^{r+s} \theta^{\ell}\left(\sum_{k=i+j} a_i b_j\right) x^k \\ &= \sum_{k=0}^{r+s} \left(\sum_{k=i+j} \theta^{\ell}(a_i)\theta^{\ell}(b_j)\right) x^k \\ &= \left(\sum_{i=0}^{r} \theta^{\ell}(a_i)x^i\right)\left(\sum_{i=0}^{s} \theta^{\ell}(b_i)x^i\right) \\ &= \theta^{\ell}(f(x))\theta^{\ell}(g(x)).\end{aligned}$$

Therefore, *i)* is proved.

To prove *ii)*, assume that $a_0 \neq 0$ and $b_0 \neq 0$. Without loss of generality, we assume that $f(x)$ and $g(x)$ have degree r and s, respectively. Then

$$\begin{aligned}(f(x)g(x))^* &= x^{r+s}(a_0b_0)^{-1}\left(\sum_{k=0}^{r+s}\left(\sum_{k=i+j} a_i b_j\right) x^{-k}\right) \\ &= \left(x^r a_0^{-1}\sum_{i=0}^{r} a_i x^{-i}\right)\left(x^s b_0^{-1}\sum_{i=0}^{s} b_i x^{-i}\right) \\ &= f^*(x)g^*(x).\end{aligned}$$

The statement *iii)* follows immediately from *i)* and *ii)*. □

The generator polynomial of the ℓ-equivalent dual of a cyclic code is determined in the following proposition.

Proposition 3.2. *Assume that $x^n - 1 = g(x)h(x)$ in $\mathbb{F}_{p^m}[x]$, where $g(x)$ and $h(x)$ are monic polynomials. If C is a cyclic code of length n with the generator polynomial $g(x)$, then $\theta^{\ell}(C^{\perp})$ is generated by $\theta^{\ell}(h^*(x))$.*

Proof. Assume that $\dim(C) = k$. Let $g(x) = \sum_{i=0}^{n-1} g_i x^i$ and $h(x) = \sum_{i=0}^{n-1} h_i x^i$, where $g_i = 0$ for all $i>n-k$ and $h_i = 0$ for all $i>k$. In the quotient ring

$\mathbb{F}_{p^m}[x]/\langle x^n-1\rangle$, we have

$$\begin{aligned} 0 &= x^n-1\\ &= g(x)h(x)\\ &= (g_0+g_1x+g_2x^2+\cdots+g_{n-k}x^{n-k}+\cdots+g_{n-1}x^{n-1})\\ &\quad\times(h_0+h_1x+h_2x^2+\cdots+h_{n-k}x^{n-k}+\cdots+h_{n-1}x^{n-1})\\ &= (g_0h_0+g_1h_{n-1}+\cdots+g_{n-1}h_1)+(g_0h_1+g_1h_0+g_2h_{n-1}+\cdots+g_{n-1}h_2)x\\ &\quad+\cdots+(g_0h_{n-1}+g_1h_{n-2}+\cdots+g_{n-1}h_0)x^{n-1}. \end{aligned}$$

Then $g_0h_i+g_1h_{i-1}+\cdots+g_{n-1}h_{n-1+i}=0$ for all $i=0,1,\ldots,n$. It follows that the polynomial representation of $(h_i,h_{i-1},\ldots,h_{n-1+i})$ is in $C^\perp$. Since $C^\perp$ is also cyclic, we have that the polynomial representation of $(h_{n-1},h_{n-2},\ldots,h_k,\ldots,h_2,h_1,h_0)$ is $\widetilde{h(x)}$ and it is in $C^\perp$. Hence, $\theta^\ell(\widetilde{h(x)})\in\theta^\ell(C^\perp)$. Therefore, $\langle\theta^\ell(h^*(x))\rangle=\langle\theta^\ell(\widetilde{h(x)})\rangle\subseteq\theta^\ell(C^\perp)$. Since

$$\dim(\langle\theta^\ell(h^*(x))\rangle)=n-\deg(\theta^\ell(h^*(x)))=n-k=\dim(\theta^\ell(C^\perp)),$$

the generator polynomial of $\theta^\ell(C^\perp)$ is $\theta^\ell(h^*(x))$. □

From the definition of $\theta^\ell(f(x))$, the 0-equivalent dual of a cyclic code is just its Euclidean dual generated by $h^*(x)$. In addition, if m is even, then the $\frac{m}{2}$-equivalent dual of a cyclic code is its Hermitian dual generated by $h^\dagger(x)$.

Example 3.3. Let $n=7$, $p=3$ and $m=4$. Let α be a primitive element of $\mathbb{F}_{81}=\mathbb{F}_{3^4}$. The polynomial x^7-1 can be factorized into a product of monic irreducible polynomials over $\mathbb{F}_{81}$ of the form

$$x^7-1=(x+2)(x^3+\alpha^{10}x^2+\alpha^{70}x+2)(x^3+\alpha^{30}x^2+\alpha^{50}x+2).$$

Let C be the cyclic code of length 7 over $\mathbb{F}_{81}$ generated by

$$g(x)=x^3+\alpha^{10}x^2+\alpha^{70}x+2.$$

Since $h(x) = \frac{x^7-1}{x^3+\alpha^{10}x^2+\alpha^{70}x+2} = (x+2)(x^3+\alpha^{30}x^2+\alpha^{50}x+2)$, we have

$$\begin{aligned}
\theta^0(C^\perp) &= C^\perp = \langle \theta^0(h^*(x))\rangle = \langle h^*(x)\rangle = \langle (x+2)(x^3+\alpha^{10}x^2+\alpha^{70}x+2)\rangle,\\
\theta^1(C^\perp) &= \langle \theta^1(h^*(x))\rangle = \langle (x+2)(x^3+\alpha^{30}x^2+\alpha^{50}x+2)\rangle,\\
\theta^2(C^\perp) &= \langle \theta^2(h^*(x))\rangle = \langle (x+2)(x^3+\alpha^{10}x^2+\alpha^{70}x+2)\rangle,
\end{aligned}$$

and

$$\theta^3(C^\perp) = \langle \theta^3(h^*(x))\rangle = \langle (x+2)(x^3+\alpha^{30}x^2+\alpha^{50}x+2)\rangle.$$

Chapter 4

ℓ-Isodual Cyclic Codes

In this chapter, the characterization of ℓ-isodual cyclic codes over finite fields is given as well as necessary and sufficient conditions for cyclic codes to be ℓ-isodual. The enumeration of such codes is also completely determined.

4.1 Characterization of ℓ-Isodual Cyclic Codes

The characterization of ℓ-isodual cyclic codes is given as follows.

Proposition 4.1. *Assume that $x^n - 1 = g(x)h(x)$ in $\mathbb{F}_{p^m}[x]$. Let C be a cyclic code of length n generated by $g(x)$. Then C is ℓ-isodual if and only if $g(x) = \theta^\ell(h^*(x))$.*

Proof. Assume that C is ℓ-isodual. Then $C = \theta^\ell(C^\perp)$. Since $C = \langle g(x)\rangle$ and $\theta^\ell(C^\perp) = \langle \theta^\ell(h^*(x))\rangle$, we have $\langle g(x)\rangle = \langle \theta^\ell(h^*(x))\rangle$. Thus there exist $p(x), q(x) \in \mathbb{F}_{p^m}[x]$ such that $g(x) = \theta^\ell(h^*(x))p(x)$ and $\theta^\ell(h^*(x)) = g(x)q(x)$. Hence, $g(x) = g(x)p(x)q(x)$, *i.e.*, $p(x)q(x) = 1$. Since $g(x)$ and $\theta^\ell(h^*(x))$ are monic polynomials, it follows that $p(x) = 1$ and $q(x) = 1$. Therefore, $g(x) = \theta^\ell(h^*(x))$.

Conversely, assume that $g(x) = \theta^\ell(h^*(x))$. Then we have $\langle g(x)\rangle = \langle \theta^\ell(h^*(x))\rangle$ which implies that $C = \theta^\ell(C^\perp)$. Therefore, C is ℓ-isodual. □

Example 4.2. Let $n = 14$, $p = 2$ and $m = 3$. Let α be a primitive element of $\mathbb{F}_8$. Then $x^{14} - 1$ can be factorized into a product of irreducible polynomials over $\mathbb{F}_8$ as

$$x^{14} - 1 = (x+1)^2(x+\alpha)^2(x+\alpha^2)^2(x+\alpha^3)^2(x+\alpha^4)^2(x+\alpha^5)^2(x+\alpha^6)^2.$$

Let $g(x) = (x+1)(x+\alpha)^2(x+\alpha^2)^2(x+\alpha^4)^2$. Then we have

$$h(x) = \frac{x^n - 1}{g(x)} = (x+1)(x+\alpha^3)^2(x+\alpha^5)^2(x+\alpha^6)^2.$$

For $0 \leq \ell < 3$, by direct computation, we conclude that

$$\theta^\ell(h^*(x)) = g(x).$$

Hence, $\langle g(x) \rangle$ is an ℓ-isodual cyclic code for all $0 \leq \ell < 3$.

Theorem 4.3. *Let m and n be positive integers and let $0 \leq \ell < m$ be an integer. Then there exists an ℓ-isodual cyclic code of length n over $\mathbb{F}_{p^m}$ if and only if $p = 2$ and n is even.*

Proof. Assume that $x^n - 1 = g(x)h(x)$, where $g(x)$ and $h(x)$ are monic polynomials. Let C be a cyclic code of length n over $\mathbb{F}_{p^m}$ generated by $g(x)$.

Assume that C is ℓ-isodual. Then $C = \langle g(x) \rangle$ and $\theta^\ell(C^\perp) = \langle \theta^\ell(h^*(x)) \rangle$. Since $C = \theta^\ell(C^\perp)$, we have $\dim(C) = \dim(\theta^\ell(C^\perp))$. Therefore,

$$\begin{aligned} n - \deg(g(x)) &= \dim(C) = \dim(\theta^\ell(C^\perp)) = \dim(C^\perp) \\ &= n - \deg(h^*(x)) = n - \deg(h(x)). \end{aligned}$$

Hence, $\deg(g(x)) = \deg(h(x))$. Since $\deg(h(x)) = n - \deg(g(x))$, we have

$$n = 2\deg(g(x))$$

which implies that $2|n$. Hence, n is even and $\deg(g(x)) = \deg(h(x)) = \frac{n}{2}$.

Write $n = \bar{n}p^\nu$, where $p \nmid \bar{n}$ and $0 \leq \nu$. Since

$$g(x)h(x) = x^n - 1 = (x-1)^{p^\nu}(f(x))^{p^\nu}$$

for some $f(x) \in \mathbb{F}_{p^m}[x]$, we have $(x-1)|g(x)$ or $(x-1)|h(x)$.

Case 1 $(x-1)|g(x)$. Since $g(x) = \theta^\ell(h^*(x))$, we have $(x-1)|\theta^\ell(h^*(x))$. Note that $x-1 = \theta^\ell((x-1)^*)$. Hence, $\theta^\ell((x-1)^*)|\theta^\ell(h^*(x))$. It follows that $(x-1)|h(x)$. From the discussion, for each $1 \leq r \leq p^\nu$, we note that $(x-1)^r|g(x)$ if and only if $(x-1)^r|h(x)$. Therefore, the exponents of $(x-1)$ in $h(x)$ and $g(x)$ are exactly the same, denoted by λ. Then $2\lambda = p^\nu$, and hence, p is even.

Case 2 $(x-1)|h(x)$. Since $g(x) = \theta^\ell(h^*(x))$ and

$$g(x)h(x) = x^n - 1 = \theta^\ell((x^n-1)^*) = \theta^\ell(g^*(x))\theta^\ell(h^*(x)),$$

we have $h(x) = \theta^\ell(g^*(x))$. Hence, $(x-1)|\theta^\ell(g^*(x))$. Similar to Case 1, we have $(x-1)|g(x)$, and hence, the exponents of $(x-1)$ in $h(x)$ and $g(x)$ are exactly the same, denoted by λ. Therefore, $2\lambda = p^\nu$, and hence, p is even.

Conversely, assume $p = 2$ and n is even. Then the polynomial $x^n - 1$ can be written as

$$x^n - 1 = x^n + 1 = \left(x^{\frac{n}{2}} + 1\right)^2 \in \mathbb{F}_{2^m}[x].$$

Choose $g(x) = x^{\frac{n}{2}} + 1$. Then $h(x) = x^{\frac{n}{2}} + 1$. Since

$$\begin{aligned}\theta^\ell(h^*(x)) = \theta^\ell(h_0^{-1}\widetilde{h(x)}) &= \theta^\ell\left(x^{\frac{n}{2}}\left(\frac{1}{x^{\frac{n}{2}}} + 1\right)\right)\\ &= \theta^\ell(1 + x^{\frac{n}{2}}) = 1 + x^{\frac{n}{2}} = g(x),\end{aligned}$$

by Proposition 4.1, we have that $C = \langle g(x)\rangle$ is an ℓ-isodual cyclic code of length n over $\mathbb{F}_{2^m}$. □

4.2 Enumeration of ℓ-Isodual Cyclic Codes

In this section, we focus on the enumeration of ℓ-isodual cyclic codes of length n over $\mathbb{F}_{p^m}$. Some necessary tools are introduced and proved.

Definition 4.4. For a given integer i>0, let $S_2(i)$ denote the largest integer 2^k such that $2^k|i$.

Lemma 4.5. *Let m be an even integer and ℓ be an integer such that $0<\ell<m$. Then*

$$\gcd(m,2\ell)=\begin{cases}\gcd(m,\ell) & \text{if } S_2(\ell)\geq S_2(m),\\ 2\gcd(m,\ell) & \text{if } S_2(\ell)<S_2(m).\end{cases}$$

Proof. We distinguish the proof into two cases.

Case 1 $S_2(\ell)\geq S_2(m)$. Let $d=\gcd(m,2\ell)$. Clearly, $\gcd(m,\ell)|d$. Since $S_2(d)=S_2(m)\leq S_2(\ell)$, $\frac{d}{S_2(d)}$ is odd and $S_2(d)|\ell$. Note that $\frac{d}{S_2(d)}|2\ell$. It follows that $\frac{d}{S_2(d)}|\ell$. Since $\ell=\frac{\ell}{S_2(d)}\cdot S_2(d)$ and $\gcd\left(\frac{d}{S_2(d)},S_2(d)\right)=1$, $\frac{d}{S_2(d)}|\frac{\ell}{S_2(d)}$. Hence, $d|\ell$. Therefore, $d|\gcd(m,\ell)$. Thus, $\gcd(m,2\ell)=\gcd(m,\ell)$

Case 2 $S_2(\ell)<S_2(m)$. Let $d=\gcd(m,\ell)$. Clearly, $\gcd(m,2\ell)|2d$. Since $S_2(d)=S_2(\ell)<S_2(m)$, we have $\frac{d}{S_2(d)}$ is odd but $\frac{m}{S_2(d)}$ is even. Since $\frac{m}{S_2(d)}=\frac{m}{2\cdot S_2(d)}\cdot 2$ and $\frac{d}{S_2(d)}|\frac{m}{S_2(d)}$, we have $\frac{d}{S_2(d)}|\frac{m}{2\cdot S_2(d)}$. It follows that $d|\frac{m}{2}$, and hence, $2d|\gcd(m,2\ell)$. Therefore, $\gcd(m,2\ell)=2\gcd(m,\ell)$. □

Remark 4.6. We note that if m is odd, then $S_2(\ell)\geq S_2(m)$ for all $0<\ell<m$. Hence, in this case, $\gcd(m,2\ell)=\gcd(m,\ell)$.

Definition 4.7. For integers ℓ and m such that $0\leq\ell<m$, let

$$\mathrm{Fix}(\theta^\ell)=\{\alpha\in\mathbb{F}_{p^m}\mid\theta^\ell(\alpha)=\alpha\}.$$

Lemma 4.8. *Let ℓ and m be integers such that $0\leq\ell<m$. Then*

$$\mathrm{Fix}(\theta^\ell)=\mathbb{F}_{p^{\gcd(m,\ell)}}.$$

Proof. Let $\alpha\in\mathrm{Fix}(\theta^\ell)$. Then $\theta^\ell(\alpha)=\alpha$. There exist $a,b\in\mathbb{Z}$ such that $\gcd(m,\ell)=am+b\ell$ and

$$\alpha^{p^{\gcd(m,\ell)}}=\alpha^{p^{am+b\ell}}=(\alpha^{p^{am}})^{p^{b\ell}}.$$

Since

$$\alpha^{p^{am}}=(\alpha^{p^m})^{p^{m(a-1)}}=\alpha^{p^{m(a-1)}}=\alpha^{p^{m(a-2)}}=\cdots=\alpha^{p^{m(0)}}=\alpha,$$

we have $\alpha^{p^{\gcd(m,\ell)}} = \alpha^{p^{b\ell}} = (\alpha^{p^{\ell}})^{p^{\ell(b-1)}} = \alpha^{p^{\ell(b-1)}} = \alpha^{p^{\ell(b-2)}} = \cdots = \alpha^{p^{\ell(0)}} = \alpha$. Hence, $\alpha^{p^{\gcd(m,\ell)}} = \alpha$. Therefore, $\alpha \in \mathbb{F}_{p^{\gcd(m,\ell)}}$.

On the other hand, assume that $\alpha \in \mathbb{F}_{p^{\gcd(m,\ell)}}$. Then $\alpha^{p^{\gcd(m,\ell)}} = \alpha$. We have

$$\begin{aligned}\theta^{\ell}(\alpha) &= \alpha^{p^{\ell}}\\ &= \alpha^{p^{\gcd(m,\ell)\cdot\frac{\ell}{\gcd(m,\ell)}}}\\ &= \left(\alpha^{p^{\gcd(m,\ell)}}\right)^{p^{\gcd(m,\ell)\left(\frac{\ell}{\gcd(m,\ell)}-1\right)}}\\ &= \alpha^{p^{\gcd(m,\ell)\left(\frac{\ell}{\gcd(m,\ell)}-1\right)}}\\ &= \alpha^{p^{(\ell-\gcd(m,\ell))}}.\end{aligned}$$

Continue this process, we have $\theta^{\ell}(\alpha) = \alpha^{p^{(\ell-2\gcd(m,\ell))}} = \cdots = \alpha^{p^0} = \alpha$. Hence, $\alpha \in \mathrm{Fix}(\theta^{\ell})$. Therefore, we have $\mathrm{Fix}(\theta^{\ell}) = \mathbb{F}_{p^{\gcd(m,\ell)}}$ as desired. □

We next give a characterization of ℓ-isodual cyclic codes of length n over $\mathbb{F}_{2^m}$ in terms of Euclidean and Hermitian self-dual cyclic codes over some subfield of $\mathbb{F}_{2^m}$.

Lemma 4.9. *Let n and m be positive integers and let ℓ be an integer such that $0 \leq \ell < m$. Let $g(x) \in \mathbb{F}_{2^m}[x]$ be a divisor of $x^n - 1$. Then the following statements hold.*

i) If $\ell = 0$ or $S_2(\ell) \geq S_2(m)$, then the cyclic code C of length n over $\mathbb{F}_{2^m}$ generated by $g(x)$ is ℓ-isodual if and only if $g(x) \in \mathbb{F}_{2^{\gcd(m,\ell)}}[x]$ and the cyclic code of length n over $\mathbb{F}_{2^{\gcd(m,\ell)}}$ generated by $g(x)$ is Euclidean self-dual.

ii) If $\ell > 0$ and $S_2(\ell) < S_2(m)$, then the cyclic code C of length n over $\mathbb{F}_{2^m}$ generated by $g(x)$ is ℓ-isodual if and only if $g(x) \in \mathbb{F}_{2^{2\gcd(m,\ell)}}[x]$ and the cyclic code of length n over $\mathbb{F}_{2^{2\gcd(m,\ell)}}$ generated by $g(x)$ is Hermitian self-dual.

Proof. To prove $i)$, assume that $S_2(\ell) \geq S_2(m)$ or $\ell = 0$.

Suppose that the cyclic code C of length n over $\mathbb{F}_{2^m}$ generated by $g(x)$ is ℓ-isodual. Then $g(x) = \theta^{\ell}(h^*(x))$, which implies that $\theta^{m-\ell}(g^*(x)) = h(x)$. Since C is ℓ-isodual, by Corollary 2.10, we have that $C^{\perp}$ is ℓ-isodual. Hence $h^*(x) = \theta^{\ell}(g(x))$. Then $h(x) = \theta^{\ell}(g^*(x))$. It follows that $\theta^{\ell}(g^*(x)) = \theta^{m-\ell}(g^*(x))$, i.e., $\theta^{2\ell}(g(x)) = g(x)$. It means that $g(x) \in \mathrm{Fix}(\theta^{2\ell})[x] = \mathbb{F}_{2^{\gcd(m,2\ell)}}[x]$ by Lemma 4.8. Since $h(x) = \frac{x^n-1}{g(x)}$, we have $h(x) \in \mathbb{F}_{2^{\gcd(m,2\ell)}}[x]$. By Lemma 4.5, we have $\gcd(m, 2\ell) = \gcd(m, \ell)$ since $S_2(\ell) \geq S_2(m)$ or $\ell = 0$. Hence, $h^*(x) \in \mathbb{F}_{2^{\gcd(m,\ell)}}[x] = \mathrm{Fix}(\theta^{\ell})[x]$ by Lemma 4.8. Therefore, $g(x) = \theta^{\ell}(h^*(x)) = h^*(x) \in \mathbb{F}_{2^{\gcd(m,\ell)}}[x]$. Thus, C is Euclidean self-dual over $\mathbb{F}_{2^{\gcd(m,\ell)}}$ by Corollary 2.3.

Conversely, suppose that $g(x) \in \mathbb{F}_{2^{\gcd(m,\ell)}}[x]$ and the cyclic code C of length n over $\mathbb{F}_{2^{\gcd(m,\ell)}}$ generated by $g(x)$ is Euclidean self-dual. Then $g(x) = h^*(x) \in \mathbb{F}_{2^{\gcd(m,\ell)}}[x]$. Since $h^*(x) \in \mathbb{F}_{2^{\gcd(m,\ell)}}[x]$, we have $\theta^{\ell}(h^*(x)) = \theta^{\gcd(m,\ell)}(h^*(x)) = h^*(x) = g(x)$. Since $\mathbb{F}_{2^{\gcd(m,\ell)}} \subseteq \mathbb{F}_{2^m}$, $g(x) = \theta^{\ell}(h^*(x)) \in \mathbb{F}_{2^m}[x]$. Hence, C is ℓ-isodual over $\mathbb{F}_{2^m}$ by Proposition 4.1.

To prove $ii)$, assume that $S_2(\ell)<S_2(m)$ and $\ell>0$.

Assume that the cyclic code C of length n over $\mathbb{F}_{2^m}$ generated by $g(x)$ is ℓ-isodual. Then $g(x) = \theta^{\ell}(h^*(x))$. Similar to the proof of $i)$, we have $g(x) = \theta^{\ell}(h^*(x)) \in \mathrm{Fix}(\theta^{2\ell}) = \mathbb{F}_{2^{\gcd(m,2\ell)}}[x]$ by Lemma 4.8. Since $S_2(\ell)<S_2(m)$, by Lemma 4.5, we obtain $\gcd(m, 2\ell) = 2\gcd(m, \ell)$. Thus, $g(x) = \theta^{\ell}(h^*(x)) \in \mathbb{F}_{2^{2\gcd(m,\ell)}}[x]$. Since $\gcd(m, \ell)|\ell$, we have $\ell = \gcd(m, \ell) \cdot k$ for some $k \in \mathbb{N}$. Note that $\theta^{2\gcd(m,\ell)} = id \in \mathrm{Aut}(\mathbb{F}_{2^{2\gcd(m,\ell)}})$. Then

$$\theta^{\ell}(h^*(x)) = \begin{cases} \theta^{\gcd(m,\ell)}(h^*(x)) \text{ if } k \text{ is odd,} \\ \\ h^*(x) \text{ if } k \text{ is even.} \end{cases}$$

If k is even, then $h^*(x) \in \mathbb{F}_{2^{\gcd(m,\ell)}}[x]$. Hence, $\theta^{\ell}(h^*(x)) = h^*(x) = \theta^{\gcd(m,\ell)}(h^*(x))$. In both cases we have $g(x) = \theta^{\ell}(h^*(x)) = \theta^{\gcd(m,\ell)}(h^*(x)) = h^{\dagger}(x)$. Thus, C is Hermitian self-dual over $\mathbb{F}_{2^{2\gcd(m,\ell)}}$ by Corollary 2.5.

Conversely, suppose that $g(x) \in \mathbb{F}_{2^{2\gcd(m,\ell)}}[x]$ and the cyclic code C of length n over $\mathbb{F}_{2^{2\gcd(m,\ell)}}$ generated by $g(x)$ is Hermitian self-dual. Then $g(x) = \theta^{\gcd(m,\ell)}(h^*(x)) \in \mathbb{F}_{2^{2\gcd(m,\ell)}}[x]$. Since $S_2(\ell){<}S_2(m)$, by Lemma 4.5, we have $\gcd(m, 2\ell) = 2\gcd(m,\ell)$. Thus, $g(x) = \theta^{\gcd(m,\ell)}(h^*(x)) \in \mathbb{F}_{2^{\gcd(m,2\ell)}}[x]$. Similarly, we have $\theta^{\ell}(h^*(x)) = \theta^{\gcd(m,\ell)}(h^*(x))$. Thus, $g(x) = \theta^{\ell}(h^*(x)) \in \mathbb{F}_{2^m}[x]$ because $\mathbb{F}_{2^{\gcd(m,2\ell)}} \subseteq \mathbb{F}_{2^m}$. Therefore, C is ℓ-isodual over $\mathbb{F}_{2^m}$ by Proposition 4.1. □

Example 4.10. Let $n = 14$, $p = 2$ and $m = 3$. Let α be a primitive element of $\mathbb{F}_8$. Then $x^{14} - 1$ can be factorized into a product of irreducible polynomials over $\mathbb{F}_8$ as

$$x^{14} - 1 = (x+1)^2(x+\alpha)^2(x+\alpha^2)^2(x+\alpha^3)^2(x+\alpha^4)^2(x+\alpha^5)^2(x+\alpha^6)^2.$$

Let $g(x) = (x+1)(x+\alpha)^2(x+\alpha^2)^2(x+\alpha^4)^2$. From Example 4.2, we have that $C = \langle g(x)\rangle$ is an ℓ-isodual cyclic code for all $0 \leq \ell{<}3$. Note that $S_2(\ell) \geq S_2(3)$ for all $0 \leq \ell{<}3$. By Lemma 4.9, we have that for each $0 \leq \ell{<}3$, $g(x) \in \mathbb{F}_{2^{\gcd(3,\ell)}}[x]$ and the cyclic code of length 14 over $\mathbb{F}_{2^{\gcd(3,\ell)}}$ generated by $g(x)$ is Euclidean self-dual.

Example 4.11. Let $n = 14$, $p = 2$ and $m = 4$. Then $x^{14} - 1$ can be factorized into a product of irreducible polynomials over $\mathbb{F}_{16}$ as

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

Let $g(x) = (x+1)(x^3+x+1)^2$. Then we have

$$h(x) = \frac{x^n - 1}{g(x)} = (x+1)(x^3+x^2+1)^2.$$

For $0 \leq \ell{<}4$, by direct computation, we conclude that

$$\theta^{\ell}(h^*(x)) = g(x).$$

Hence $C = \langle g(x)\rangle$ is an ℓ-isodual cyclic code for all $0 \leq \ell{<}4$. Note that $S_2(\ell){<}S_2(4)$ for all $0 \leq \ell{<}4$. By Lemma 4.9, we conclude the following results.

1. If $\ell = 0$, then the cyclic code C of length 14 over $\mathbb{F}_{16}$ generated by $g(x)$ is

Euclidean self-dual.

2. If $1 \leq \ell \leq 3$, then we have $g(x) \in \mathbb{F}_{2^{2\gcd(4,\ell)}}$ and the cyclic code of length 14 over $\mathbb{F}_{2^{2\gcd(4,\ell)}}$ generated by $g(x)$ is Hermitian self-dual.

The number of ℓ-isodual cyclic codes of length n over $\mathbb{F}_{2^m}$ can be determined in terms of the numbers of Euclidean self-dual and Hermitian self-dual cyclic codes of length n over some subfields of $\mathbb{F}_{2^m}$.

Theorem 4.12. *Let n and m be positive integers and let ℓ be an integer such that $0 \leq \ell<m$. Then the number of ℓ-isodual cyclic codes of length n over $\mathbb{F}_{2^m}$ equals*

i) the number of Euclidean self-dual cyclic codes of length n over $\mathbb{F}_{2^{\gcd(m,\ell)}}$ if $S_2(m) \leq S_2(\ell)$ or $\ell = 0$, or,

ii) the number of Hermitian self-dual cyclic codes of length n over $\mathbb{F}_{2^{2\gcd(m,\ell)}}$ if $S_2(m)>S_2(\ell)$ and $\ell>0$.

Proof. It follows immediately from Lemma 4.9. □

For completeness, we recall some results concerning the numbers of Euclidean self-dual and Hermitian self-dual cyclic codes from [2] and [3].

Definition 4.13. Let j be an odd positive integer and let k be a positive integer. The pair $(j, 2^k)$ is said to be *oddly good* if j divides $(2^k)^s + 1$ for some odd integer $s \geq 1$, and *evenly good* if j divides $(2^k)^s + 1$ for some even integer $s \geq 2$. It is said to be *good* if it is oddly good or evenly good, and *bad* otherwise.

Definition 4.14. Let $\mathbb{O}$ be a set of odd positive integer and let $\chi, \lambda : \mathbb{O} \times \mathbb{N} \to \{0, 1\}$ be defined by

$$\chi(j,k) = \begin{cases} 0 & \text{if } (j, 2^k) \text{ is good,} \\ 1 & \text{otherwise,} \end{cases}$$

and

$$\lambda(j,k) = \begin{cases} 0 & \text{if } (j, 2^k) \text{ is oddly good,} \\ 1 & \text{otherwise.} \end{cases}$$

Definition 4.15. Let j and i be positive integers such that $\gcd(j, i) = 1$ and let $\mathbb{Z}_j^\times$ be the unit group of $\mathbb{Z}_j$. The order of i in $\mathbb{Z}_j^\times$ is the smallest integer e such that $j|(i^e - 1)$, denoted by $ord_j(i)$.

Theorem 4.16 ([2, Theorem 3])**.** *Let $n = 2^{\nu(n)}\bar{n}$ be positive integer such that $\bar{n} \geq 1$ is odd and $\nu(n) \geq 1$. Then the number of self-dual cyclic codes of length n over $\mathbb{F}_{2^m}$ is*

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

Theorem 4.17 ([3, Corollary 3.7])**.** *Let $n = 2^{\nu(n)}\bar{n}$ be positive integer such that $\bar{n} \geq 1$ is odd and $\nu(n) \geq 1$. Then the number of Hermitian self-dual cyclic codes of length n over $\mathbb{F}_{2^{2m}}$ is*

$$(1 + 2^{\nu(n)})^{\frac{1}{2}\sum_{j|\bar{n}} \lambda(j,m)\frac{\phi(j)}{ord_j(2^{2m})}}.$$

Corollary 4.18. *Let $n = 2^{\nu(n)}\bar{n}$ be positive integer such that $\bar{n} \geq 1$ is odd and $\nu(n) \geq 1$. Let m be a positive integer and ℓ be an integer such that $0 \leq \ell < m$. Then the number of ℓ-isodual cyclic codes of length n over $\mathbb{F}_{2^m}$ is*

i) $(1 + 2^{\nu(n)})^{\frac{1}{2}\sum_{j|\bar{n}} \chi(j,\gcd(m,\ell))\frac{\phi(j)}{ord_j(2^{\gcd(m,\ell)})}}$ *if $S_2(m) \leq S_2(\ell)$ or $\ell = 0$,*

ii) $(1 + 2^{\nu(n)})^{\frac{1}{2}\sum_{j|\bar{n}} \lambda(j,\gcd(m,\ell))\frac{\phi(j)}{ord_j(2^{2\gcd(m,\ell)})}}$ *if $S_2(m) > S_2(\ell)$ and $\ell > 0$.*

Proof. It follows immediately from Theorems 4.12, 4.16 and 4.17. □

Example 4.19. Let $n = 14$, $p = 2$ and $m = 3$. Let ℓ be an integer such that $0 \leq \ell < m$. Note that $S_2(3) \leq S_2(\ell)$ for all $0 \leq \ell < 3$. By Corollary 4.18, we have that the number of ℓ-isodual cyclic codes of length 14 over $\mathbb{F}_8$ is

$$(1 + 2^1)^{\frac{1}{2}\sum_{j|7} \chi(j,\gcd(3,\ell))\frac{\phi(j)}{\mathrm{ord}_j(2^{\gcd(3,\ell)})}}.$$

If $\ell = 0$, then the number of 0-isodual cyclic codes of length 14 over $\mathbb{F}_8$ is

$$(1 + 2^1)^{\frac{1}{2}\sum_{j|7} \chi(j,3)\frac{\phi(j)}{\mathrm{ord}_j(2^3)}}.$$

Since

$$\begin{aligned}\frac{1}{2}\sum_{j|7}\chi(j,3)\frac{\phi(j)}{\mathrm{ord}_j(2^3)} &= \frac{1}{2}\left(\chi(1,3)\frac{\phi(1)}{\mathrm{ord}_1(8)}+\chi(7,3)\frac{\phi(7)}{\mathrm{ord}_7(8)}\right)\\ &= \frac{1}{2}\left(0+\frac{(1)(6)}{1}\right)\\ &= 3,\end{aligned}$$

the number of 0-isodual cyclic codes of length 14 over $\mathbb{F}_8$ is $(1+2^1)^3 = 27$. If $\ell = 1$, then the number of 1-isodual cyclic codes of length 14 over $\mathbb{F}_8$ is

$$(1+2^1)^{\frac{1}{2}\sum_{j|7}\chi(j,1)\frac{\phi(j)}{\mathrm{ord}_j(2^1)}}.$$

Since

$$\begin{aligned}\frac{1}{2}\sum_{j|7}\chi(j,1)\frac{\phi(j)}{\mathrm{ord}_j(2^1)} &= \frac{1}{2}\left(\chi(1,1)\frac{\phi(1)}{\mathrm{ord}_1(2)}+\chi(7,1)\frac{\phi(7)}{\mathrm{ord}_7(2)}\right)\\ &= \frac{1}{2}\left(0+\frac{(1)(6)}{3}\right)\\ &= 1,\end{aligned}$$

the number of 1-isodual cyclic codes of length 14 over $\mathbb{F}_8$ is $(1+2^1)^1 = 3$. If $\ell = 2$, then the number of 2-isodual cyclic codes of length 14 over $\mathbb{F}_8$ is

$$(1+2^1)^{\frac{1}{2}\sum_{j|7}\chi(j,1)\frac{\phi(j)}{\mathrm{ord}_j(2^1)}}.$$

Since

$$\begin{aligned}\frac{1}{2}\sum_{j|7}\chi(j,1)\frac{\phi(j)}{\mathrm{ord}_j(2^1)} &= \frac{1}{2}\left(\chi(1,1)\frac{\phi(1)}{\mathrm{ord}_1(2)}+\chi(7,1)\frac{\phi(7)}{\mathrm{ord}_7(2)}\right)\\ &= \frac{1}{2}\left(0+\frac{(1)(6)}{3}\right)\\ &= 1,\end{aligned}$$

the number of 2-isodual cyclic codes of length 14 over $\mathbb{F}_8$ is $(1+2^1)^1 = 3$.

Example 4.20. Let $n = 14$, $p = 2$ and $m = 4$. Let ℓ be an integer such that $0 \leq \ell < m$. Note that $S_2(4) > S_2(\ell)$ for all $0 \leq \ell < 4$. By Corollary 4.18, we have that the number of 0-isodual cyclic codes of length 14 over $\mathbb{F}_{16}$ is

$$(1+2^1)^{\frac{1}{2}\sum_{j|7}\chi(j,\gcd(4,0))\frac{\phi(j)}{\mathrm{ord}_j(2^{\gcd(4,0)})}}.$$

Since

$$\begin{aligned}\frac{1}{2}\sum_{j|7}\chi(j,4)\frac{\phi(j)}{\mathrm{ord}_j(2^4)} &= \frac{1}{2}\left(\chi(1,4)\frac{\phi(1)}{\mathrm{ord}_1(16)}+\chi(7,4)\frac{\phi(7)}{\mathrm{ord}_7(16)}\right)\\ &= \frac{1}{2}\left(0+\frac{(1)(6)}{3}\right)\\ &= 1,\end{aligned}$$

the number of 0-isodual cyclic codes of length 14 over $\mathbb{F}_{16}$ is $(1+2^1)^1 = 3$. For $1 \leq \ell \leq 3$, by Corollary 4.18 we have that the number of ℓ-isodual cyclic codes of length 14 over $\mathbb{F}_{16}$ is

$$(1+2^1)^{\frac{1}{2}\sum_{j|7}\lambda(j,\gcd(4,\ell))\frac{\phi(j)}{\mathrm{ord}_j(2^{2\gcd(4,\ell)})}}.$$

If $\ell = 1$, then the number of 1-isodual cyclic codes of length 14 over $\mathbb{F}_{16}$ is

$$(1+2^1)^{\frac{1}{2}\sum_{j|7}\lambda(j,1)\frac{\phi(j)}{\mathrm{ord}_j(2^2)}}.$$

Since

$$\begin{aligned}\frac{1}{2}\sum_{j|7}\lambda(j,1)\frac{\phi(j)}{\mathrm{ord}_j(2^2)} &= \frac{1}{2}\left(\lambda(1,1)\frac{\phi(1)}{\mathrm{ord}_1(4)}+\lambda(7,1)\frac{\phi(7)}{\mathrm{ord}_7(4)}\right)\\ &= \frac{1}{2}\left(0+\frac{(1)(6)}{3}\right)\\ &= 1,\end{aligned}$$

the number of 1-isodual cyclic codes of length 14 over $\mathbb{F}_{16}$ is $(1+2^1)^1 = 3$. If $\ell = 2$, then the number of 2-isodual cyclic codes of length 14 over $\mathbb{F}_{16}$ is

$$(1+2^1)^{\frac{1}{2}\sum_{j|7}\lambda(j,2)\frac{\phi(j)}{\mathrm{ord}_j(2^4)}}.$$

Since

$$\begin{aligned}\frac{1}{2}\sum_{j|7}\lambda(j,2)\frac{\phi(j)}{\mathrm{ord}_j(2^4)} &= \frac{1}{2}\left(\lambda(1,2)\frac{\phi(1)}{\mathrm{ord}_1(16)}+\lambda(7,2)\frac{\phi(7)}{\mathrm{ord}_7(16)}\right)\\ &= \frac{1}{2}\left(0+\frac{(1)(6)}{3}\right)\\ &= 1,\end{aligned}$$

the number of 2-isodual cyclic codes of length 14 over $\mathbb{F}_{16}$ is $(1+2^1)^1 = 3$. If $\ell = 3$, then the number of 3-isodual cyclic codes of length 14 over $\mathbb{F}_{16}$ is

$$(1+2^1)^{\frac{1}{2}\sum_{j|7}\lambda(j,1)\frac{\phi(j)}{\mathrm{ord}_j(2^2)}}.$$

Since

$$\begin{aligned}\frac{1}{2}\sum_{j|7}\lambda(j,1)\frac{\phi(j)}{\mathrm{ord}_j(2^2)} &= \frac{1}{2}\left(\lambda(1,1)\frac{\phi(1)}{\mathrm{ord}_1(4)} + \lambda(7,1)\frac{\phi(7)}{\mathrm{ord}_7(4)}\right)\\ &= \frac{1}{2}\left(0 + \frac{(1)(6)}{3}\right)\\ &= 1,\end{aligned}$$

the number of 3-isodual cyclic codes of length 14 over $\mathbb{F}_{16}$ is $(1+2^1)^1 = 3$.

Chapter 5

ℓ-Complementary Dual Cyclic Codes

In this chapter, we focus on a generalization of complementary dual cyclic codes over $\mathbb{F}_{p^m}$, namely, ℓ-complementary dual cyclic codes, where $0 \leq \ell < m$. The characterization and enumeration of such codes are given together with some illustrative examples.

5.1 Characterization of ℓ-Complementary Dual Cyclic Codes

Recall that a linear code C of length n over $\mathbb{F}_{p^m}$ is called ℓ-complementary dual if $C \cap \theta^\ell(C^\perp) = \{0\}$. The characterization of ℓ-complementary dual cyclic codes is given as follows.

Lemma 5.1. *Assume that $x^n - 1 = g(x)h(x)$ in $\mathbb{F}_{p^m}[x]$, where $g(x)$ and $h(x)$ are monic polynomials. Let C be a cyclic code of length n over $\mathbb{F}_{p^m}$ with the generator polynomial $g(x)$ and let $0 \leq \ell < m$ be an integer. Then C is ℓ-complementary dual if and only if $\gcd(g(x), \theta^\ell(h^*(x))) = 1$.*

Proof. Note that the generator polynomial of the cyclic code $C \cap \theta^\ell(C^\perp)$ is $f(x) := \mathrm{lcm}(g(x), \theta^\ell(h^*(x)))$.

Assume that C is ℓ-complementary dual. Then we have $C \cap \theta^\ell(C^\perp) = \{0\}$. Then $f(x)$ has degree n and

$$\begin{aligned} f(x) &= \operatorname{lcm}(g(x), \theta^\ell(h^*(x))) \\ &= \frac{g(x)\theta^\ell(h^*(x))}{\gcd(g(x), \theta^\ell(h^*(x)))}. \end{aligned}$$

Since $g(x)\theta^\ell(h^*(x))$ has degree n, it follows that $\gcd(g(x), \theta^\ell(h^*(x))) = 1$.

Conversely, assume that $\gcd(g(x), \theta^\ell(h^*(x))) = 1$. Then

$$\begin{aligned} f(x) &= \operatorname{lcm}(g(x), \theta^\ell(h^*(x))) \\ &= \frac{g(x)\theta^\ell(h^*(x))}{\gcd(g(x), \theta^\ell(h^*(x)))} \\ &= g(x)\theta^\ell(h^*(x)), \end{aligned}$$

Hence, $\deg(f(x)) = n$. Since $f(x)$ is the generator polynomial of the cyclic code $C \cap \theta^\ell(C^\perp)$, we conclude that $f(x) = x^n - 1$, and hence, $C \cap \theta^\ell(C^\perp) = \{0\}$. Therefore, C is ℓ-complementary dual as desired. □

Theorem 5.2. *Let C be a cyclic code of length n over $\mathbb{F}_{p^m}$ with the generator polynomial $g(x)$ and let $0 \leq \ell < m$ be an integer. Then C is ℓ-complementary dual if and only if $g(x) = \theta^\ell(g^*(x))$ and every monic irreducible factor of $g(x)$ has the same multiplicity in $g(x)$ and in $x^n - 1$.*

Proof. Write $n = \bar{n}p^\nu$, where $p \nmid \bar{n}$ and $0 \leq \nu$ is an integer. Assume that $x^n - 1 = g(x)h(x)$ in $\mathbb{F}_{p^m}[x]$.

Assume that C is ℓ-complementary dual. By Lemma 5.1, we have

$$\gcd(g(x), \theta^\ell(h^*(x))) = 1.$$

By Lemma 3.1, we have

$$g(x)h(x) = x^n - 1 = \theta^\ell(g^*(x))\theta^\ell(h^*(x)).$$

Then $g(x)|\theta^\ell(g^*(x))\theta^\ell(h^*(x))$. Since $\gcd(g(x), \theta^\ell(h^*(x))) = 1$, it follows that $g(x)|\theta^\ell(g^*(x))$. Since $g(x)$ and $\theta^\ell(g^*(x))$ are monic polynomials of the same degree, we have $g(x) = \theta^\ell(g^*(x))$. Consequently,

$$\gcd(\theta^\ell(g^*(x)), \theta^\ell(h^*(x))) = \gcd(g(x), \theta^\ell(h^*(x))) = 1.$$

Hence, $\gcd(g(x), h(x)) = 1$. Since $x^n - 1 = g(x)h(x) = (x^{\bar{n}} - 1)^{p^\nu}$, every monic irreducible factor of $g(x)$ has the same multiplicity in $g(x)$ and in $x^n - 1$.

Conversely, assume that $g(x) = \theta^\ell(g^*(x))$ and every monic irreducible factor of $g(x)$ has the same multiplicity in $g(x)$ and in $x^n - 1$. Since

$$g(x)h(x) = x^n - 1 = \theta^\ell(g^*(x))\theta^\ell(h^*(x)),$$

it follows that $h(x) = \theta^\ell(h^*(x))$. Since $g(x)h(x) = x^n - 1 = (x^{\bar{n}} - 1)^{p^\nu}$ and every monic irreducible factor of $g(x)$ has the same multiplicity in $g(x)$ and in $x^n - 1$, we have

$$1 = \gcd(g(x), h(x)) = \gcd(g(x), \theta^\ell(h^*(x))).$$

By Lemma 5.1, C is ℓ-complementary dual. □

In the case where $p \nmid n$, $x^n - 1$ contains no repeated irreducible factors in $\mathbb{F}_{p^m}[x]$, and hence, the next corollary follows.

Corollary 5.3. *Let $0 \leq \ell < m$ be an integer and let n be a positive integer such that $p \nmid n$. Let C be a cyclic code of length n over $\mathbb{F}_{p^m}$ with the generator polynomial $g(x)$. Then C is ℓ-complementary dual if and only if $g(x) = \theta^\ell(g^*(x))$.*

Example 5.4. Let $n = 7$, $p = 3$ and $m = 4$. Let α be a primitive element of $\mathbb{F}_{81} = \mathbb{F}_{3^4}$. The polynomial $x^7 - 1$ can be factorized into a product of monic irreducible polynomials over $\mathbb{F}_{81}$ of the form

$$x^7 - 1 = (x+2)(x^3 + \alpha^{10}x^2 + \alpha^{70}x + 2)(x^3 + \alpha^{30}x^2 + \alpha^{50}x + 2).$$

Then we have the following results.

i) Let $g_1(x) = x + 2$. Since 2 and 1 are fixed by θ^i for all $i = 0, 1, 2, 3$, we have

$$g_1^*(x) = 2(2x + 1) = x + 2,$$

and hence,

$$\theta^0(g_1^*(x)) = g_1(x),\ \theta^1(g_1^*(x)) = g_1(x),\ \theta^2(g_1^*(x)) = g_1(x)$$

and

$$\theta^3(g_1^*(x)) = g_1(x).$$

Therefore, the cyclic code of length 7 over $\mathbb{F}_{81}$ generated by $g_1(x)$ is 0-complementary (Euclidean complementary) dual, 1-complementary dual, 2-complementary (Hermitian complementary) dual and 3-complementary dual.

ii) Let $g_2(x) = x^3 + \alpha^{10}x^2 + \alpha^{70}x + 2$. Then we have

$$\begin{aligned}
\theta^0(g_2^*(x)) &= g_2^*(x) \\
&= 2(2x^3 + \alpha^{70}x^2 + \alpha^{10}x + 1) \\
&= x^3 + \alpha^{30}x^2 + \alpha^{50}x + 2 \\
&\neq g_2(x), \\
\theta^1(g_2^*(x)) &= \theta(2(2x^3 + \alpha^{70}x^2 + \alpha^{10}x + 1)) \\
&= \theta(x^3 + \alpha^{30}x^2 + \alpha^{50}x + 2) \\
&= x^3 + \alpha^{10}x^2 + \alpha^{70}x + 2 \\
&= g_2(x), \\
\theta^2(g_2^*(x)) &= \theta^2(2(2x^3 + \alpha^{70}x^2 + \alpha^{10}x + 1)) \\
&= \theta^2(x^3 + \alpha^{30}x^2 + \alpha^{50}x + 2) \\
&= x^3 + \alpha^{30}x^2 + \alpha^{50}x + 2 \\
&\neq g_2(x)
\end{aligned}$$

and

$$\begin{aligned}
\theta^3(g_2^*(x)) &= \theta^3(2(2x^3 + \alpha^{70}x^2 + \alpha^{10}x + 1)) \\
&= \theta^3(x^3 + \alpha^{30}x^2 + \alpha^{50}x + 2) \\
&= x^3 + \alpha^{10}x^2 + \alpha^{70}x + 2 \\
&= g_2(x).
\end{aligned}$$

Therefore, the cyclic code of length 7 over $\mathbb{F}_{81}$ generated by $g_2(x)$ is 1-complementary dual and 3-complementary dual but the code is neither

0-complementary (Euclidean complementary) dual nor 2-complementary (Hermitian complementary) dual.

iii) Let $g_3(x) = x^3 + \alpha^{30}x^2 + \alpha^{50}x + 2$. Similar to *ii*), we have

$$\theta^0(g_3^*(x)) \neq g_3(x),\ \theta^1(g_3^*(x)) = g_3(x),\ \theta^2(g_3^*(x)) \neq g_3(x),$$

and

$$\theta^3(g_3^*(x)) = g_3(x).$$

Therefore, the cyclic code of length 7 over $\mathbb{F}_{81}$ generated by $g_3(x)$ is 1-complementary dual and 3-complementary dual but the code is neither 0-complementary (Euclidean complementary) dual nor 2-complementary (Hermitian complementary) dual.

5.2 Enumeration of ℓ-Complementary Dual Cyclic Codes

In this section, we focus on the enumeration of ℓ-complementary dual cyclic codes of length n over $\mathbb{F}_{p^m}$.

An ℓ-complementary dual cyclic code becomes Eucidean complementary dual if $\ell = 0$ and it becomes Hermitian complementary dual if $m = 2\ell$. Here, we extend the study to the case where $m = 4\ell$ and focus on the enumeration of ℓ-complementary dual cyclic codes of length n over $\mathbb{F}_{p^{4\ell}}$.

Let $n = p^{\nu(n)}\bar{n}$ be a positive integer, where $p \nmid \bar{n}$ and $\nu(n) \geq 0$. Since $x^n - 1 = (x^{\bar{n}} - 1)^{p^{\nu(n)}}$, the number of ℓ-complementary dual cyclic codes of length n over $\mathbb{F}_{p^{4\ell}}$ is independent of $p^{\nu(n)}$ by Theorem 5.2. Therefore, the number of ℓ-complementary dual cyclic codes of length n over $\mathbb{F}_{p^{4\ell}}$ equals the number of divisors $g(x)$ of $x^{\bar{n}} - 1$ such that $g(x) = \theta^\ell(g^*(x))$ by Theorem 5.2.

We note that there does not exist $f(x) \in \mathbb{F}_{p^{4\ell}}[x]$ such that $f(x) \neq \theta^\ell(f^*(x))$ and $f(x) \neq \theta^{2\ell}(f(x))$ but $f(x) = \theta^{3\ell}(f^*(x))$. To see this, suppose that the statement is false. Then $f(x) = \theta^{4\ell}(f(x)) = \theta^{\ell}(\theta^{3\ell}(f(x))) = \theta^{\ell}(f^*(x))$, which is a contradiction. Then there exist nonnegative integers r, s and t such that the factorization of $x^{\bar{n}} - 1$ can be rearanged in the form of

$$x^{\bar{n}} - 1 = \prod_{i=1}^{r} f_i(x) \prod_{j=1}^{s} h_j(x)\theta^{\ell}(h_j^*(x)) \prod_{k=1}^{t} u_k(x)\theta^{\ell}(u_k^*(x))\theta^{2\ell}(u_k(x))\theta^{3\ell}(u_k^*(x)), \tag{5.1}$$

where $f_i(x)$'s, $h_j(x)$'s, and $u_k(x)$'s are distinct irreducible factors of $x^{\bar{n}} - 1$ such that

- $f_i(x) = \theta^{\ell}(f_i^*(x))$ for all $1 \leq i \leq r$,
- $h_j(x) \neq \theta^{\ell}(h_j^*(x))$ and $h_j(x) = \theta^{2\ell}(h_j(x))$ for all $1 \leq j \leq s$, and
- $u_k(x)$, $\theta^{\ell}(u_k^*(x))$, $\theta^{2\ell}(u_k(x))$, and $\theta^{3\ell}(u_k^*(x))$ are distinct for all $1 \leq k \leq t$.

The empty product in (5.1) will be regarded as 1.

It is not difficult to see that a divisor $g(x)$ of $x^{\bar{n}} - 1$ has the property that $g(x) = \theta^{\ell}(g^*(x))$ if and only if

$$\begin{aligned} g(x) = &\prod_{i=1}^{r} (f_i(x))^{A_i} \prod_{j=1}^{s} \left(h_j(x)\theta^{\ell}(h_j^*(x))\right)^{B_j} \\ &\times \prod_{k=1}^{t} \left(u_k(x)\theta^{\ell}(u_k^*(x))\theta^{2\ell}(u_k(x))\theta^{3\ell}(u_k^*(x))\right)^{C_k}, \end{aligned}$$

where A_i's, B_j's, and C_k's are in $\{0, 1\}$.

From the discussion above and Theorem 5.2, the next theorem follows.

Theorem 5.5. *Let $n = p^{\nu(n)}\bar{n}$ be such that $p \nmid \bar{n}$ and let ℓ be a positive integer. If $x^{\bar{n}} - 1$ is decomposed as in (5.1), then the number of ℓ-complementary dual cyclic codes of length n over $\mathbb{F}_{p^{4\ell}}$ is 2^{r+s+t}, where r, s, and t are defined in (5.1).*

The rest of this section, we devote for the determination the values of r, s, and t in (5.1).

Definition 5.6. Let $\bar{n}$ be a positive integers such that $p \nmid \bar{n}$ and let $a \geq 0$ be an integer. The cyclotomic coset of $p^{4\ell}$ modulo $\bar{n}$ containing a is defined to be

$$C_{p^{4\ell}}(a) = \{a \cdot p^{4\ell j} \mod \bar{n} \mid j = 0, 1, 2, \dots\}.$$

For a given irreducible polynomial $f(x) \in \mathbb{F}_{p^{4\ell}}[x]$, it is well known [7] that $f(x) = \prod_{i \in C_{p^{4\ell}}(a)} (x - \alpha^i)$ for some interger $a \geq 0$ and α in some extension field of $\mathbb{F}_{p^{4\ell}}$. In this case, we say that $f(x)$ is induced by $C_{p^{4\ell}}(a)$.

Lemma 5.7. *Let $f(x)$ be an irreducible polynomial in $\mathbb{F}_{p^{4\ell}}[x]$ and let $a \geq 0$ be an integer. Then $f(x)$ is induced by $C_{p^{4\ell}}(a)$ if and only if $\theta^\ell(f^*(x))$ is induced by $C_{p^{4\ell}}(-p^\ell a)$.*

Proof. Assume that $f(x) = \prod_{i \in C_{p^{4\ell}}(a)} (x - \alpha^i)$ for some α in some extension field of $\mathbb{F}_{p^{4\ell}}$. Then

$$\begin{aligned} f^*(x) &= x^{|C_{p^{4\ell}}(a)|} \prod_{i \in C_{p^{4\ell}}(a)} (-\alpha^i)^{-1} \prod_{i \in C_{p^{4\ell}}(a)} \left(\frac{1}{x} - \alpha^i\right) \\ &= \prod_{i \in C_{p^{4\ell}}(a)} (-\alpha^i)^{-1} \prod_{i \in C_{p^{4\ell}}(a)} (1 - \alpha^i x) \\ &= \prod_{i \in C_{p^{4\ell}}(a)} (-\alpha^{-i} + x) \\ &= \prod_{i \in C_{p^{4\ell}}(-a)} (x - \alpha^i). \end{aligned}$$

Hence,

$$\begin{aligned} \theta^\ell(f^*(x)) &= \prod_{i \in C_{p^{4\ell}}(-a)} \left(x - \theta^\ell(\alpha^i)\right) \\ &= \prod_{i \in C_{p^{4\ell}}(-a)} \left(x - (\alpha^{ip^\ell})\right) \\ &= \prod_{i \in C_{p^{4\ell}}(-p^\ell a)} (x - \alpha^i). \end{aligned}$$

The converse can be obtained by using similar arguments. □

Definition 5.8. Let $\xi, \sigma : \{p^i \mid i \in \mathbb{N}\} \times \mathbb{N} \to \{0,1\}$ be defined by

$$\xi(p^i, d) = \begin{cases} 0 & \text{if there exists } M \in \mathbb{N} \text{ such that } d|(p^{i(4M-1)}+1), \\ 1 & \text{if for all } M \in \mathbb{N}, d \nmid (p^{i(4M-1)}+1), \end{cases}$$

and

$$\sigma(p^i, d) = \begin{cases} 0 & \text{if there exists } M \in \mathbb{N} \text{ such that } d|(p^{i(2M-1)}-1), \\ 1 & \text{if for all } M \in \mathbb{N}, d \nmid (p^{i(2M-1)}-1). \end{cases}$$

Lemma 5.9. *Let $\bar{n}$ be a positive integer such that $p \nmid \bar{n}$. If $x^{\bar{n}}-1$ is decomposed as in* (5.1)*, then*

$$r = \sum_{d|\bar{n}} (1-\xi(p^\ell, d)) \frac{\phi(d)}{ord_d(p^{4\ell})}.$$

Proof. Let $d|\bar{n}$ be a positive integer. For each element $0 \leq a < \bar{n}$ of order d modulo $\bar{n}$, let $f(x)$ be induced by $C_{p^{4\ell}}(a)$. Then $f(x) = \theta^\ell(f^*(x))$ if and only if $C_{p^{4\ell}}(a) = C_{p^{4\ell}}(-p^\ell a)$ by Lemma 5.7. Equivalently, there exists $M \in \mathbb{N}$ such that $d|p^{4\ell M} + p^\ell$, i.e., $d|p^\ell \left(p^{\ell(4M-1)}+1\right)$. Since $\gcd(d, p^\ell) = 1$, we have that $f(x) = \theta^\ell(f^*(x))$ if and only if there exists $M \in \mathbb{N}$ such that $d| \left(p^{\ell(4M-1)}+1\right)$.

Note that the number of elements in $\{0,1,2,\ldots,\bar{n}-1\}$ of order d modulo $\bar{n}$ is $\phi(d)$ and the degree of the polynomial induced by $C_{p^{4\ell}}(a)$ is $|C_{p^{4\ell}}(a)| = \mathrm{ord}_d(p^{4\ell})$ for every element a of order d modulo $\bar{n}$. Hence, the number of irreducible factor of $x^{\bar{n}}-1$ of degree $\mathrm{ord}_d(p^{4\ell})$ is $\frac{\phi(d)}{\mathrm{ord}_d(p^{4\ell})}$.

By the definition of ξ, we have

$$r = \sum_{d|\bar{n}} (1-\xi(p^\ell, d)) \frac{\phi(d)}{\mathrm{ord}_d(p^{4\ell})}$$

as desired. □

Lemma 5.10. *Let $\bar{n}$ be a positive integer such that $p \nmid \bar{n}$. If $x^{\bar{n}}-1$ is decomposed as in* (5.1)*, then*

$$s = \sum_{d|\bar{n}} \xi(p^\ell, d)(1-\sigma(p^{2\ell}, d)) \frac{\phi(d)}{2ord_d(p^{4\ell})}.$$

Proof. Let $d|\bar{n}$ be a positive integer. For each element $0 \leq a < \bar{n}$ of order d modulo $\bar{n}$, let $h(x)$ be induced by $C_{p^{4\ell}}(a)$. Then $h(x) \neq \theta^{\ell}(h^*(x))$ and $h(x) = \theta^{2\ell}(h(x))$ if and only if $C_{p^{4\ell}}(a) \neq C_{p^{4\ell}}(-p^{\ell}a)$ and $C_{p^{4\ell}}(a) = C_{p^{4\ell}}(p^{2\ell}a)$ by Lemma 5.7. Equivalently, $d \nmid (p^{4\ell M} + p^{\ell})$ for all $M \in \mathbb{N}$ and there exists $N \in \mathbb{N}$ such that $d|(p^{4\ell N} - p^{2\ell})$. Since $\gcd(d, p^{\ell}) = 1$, we have that $h(x) \neq \theta^{\ell}(h^*(x))$ and $h(x) = \theta^{2\ell}(h(x))$ if and only if $d \nmid (p^{\ell(4M-1)} + 1)$ for all $M \in \mathbb{N}$ and there exists $N \in \mathbb{N}$ such that $d|(p^{2\ell(2N-1)} - 1)$.

From the proof of Lemma 5.9, for each $d|\bar{n}$, the number of irreducible factor of $x^{\bar{n}} - 1$ of degree $\mathrm{ord}_d(p^{4\ell})$ is $\frac{\phi(d)}{\mathrm{ord}_d(p^{4\ell})}$.

By the definitions of ξ and σ, we have

$$s = \sum_{d|\bar{n}} \xi(p^{\ell}, d)(1 - \sigma(p^{2\ell}, d)) \frac{\phi(d)}{2\mathrm{ord}_d(p^{4\ell})}$$

as desired. □

Lemma 5.11. *Let $\bar{n}$ be a positive integer such that $p \nmid \bar{n}$. If $x^{\bar{n}} - 1$ is decomposed as in* (5.1), *then*

$$t = \sum_{d|\bar{n}} \sigma(p^{2\ell}, d) \frac{\phi(d)}{4ord_d(p^{4\ell})}.$$

Proof. Let $d|\bar{n}$ be a positive integer. For each element $0 \leq a < \bar{n}$ of order d modulo $\bar{n}$, let $h(x)$ be induced by $C_{p^{4\ell}}(a)$. We note that the statement $u(x)$, $\theta^{\ell}(u^*(x))$, $\theta^{2\ell}(u_k(x))$, and $\theta^{3\ell}(u^*(x))$ are distinct is equivalent to $u(x) \neq \theta^{2\ell}(u(x))$. Then $u(x) \neq \theta^{2\ell}(u(x))$ if and only if $C_{p^{4\ell}}(a) \neq C_{p^{4\ell}}(p^{2\ell}a)$ by Lemma 5.7. Equivalently, $d \nmid (p^{4\ell M} - p^{2\ell})$ for all $M \in \mathbb{N}$. Since $\gcd(d, p^{\ell}) = 1$, we have that $h(x) \neq \theta^{2\ell}(h(x))$ if and only if $d \nmid (p^{2\ell(2M-1)} - 1)$ for all $M \in \mathbb{N}$.

From the proof of Lemma 5.9, the number of irreducible factor of $x^{\bar{n}} - 1$ of degree $\mathrm{ord}_d(p^{4\ell})$ is $\frac{\phi(d)}{\mathrm{ord}_d(p^{4\ell})}$.

By the definition of σ, we have

$$t = \sum_{d|\bar{n}} \sigma(p^{2\ell}, d) \frac{\phi(d)}{4\mathrm{ord}_d(p^{4\ell})}.$$

□

The results can be sumarized as follows.

Theorem 5.12. *Let $n = p^{\nu(n)}\bar{n}$ be such that $p \nmid \bar{n}$ and let ℓ be a positive integer. Then the number of ℓ-complementary dual cyclic codes of length n over $\mathbb{F}_{p^{4\ell}}$ is 2^{r+s+t}, where*

$$r = \sum_{d|\bar{n}} (1 - \xi(p^{\ell}, d))\frac{\phi(d)}{ord_d(p^{4\ell})},$$

$$s = \sum_{d|\bar{n}} \xi(p^{\ell}, d)(1 - \sigma(p^{2\ell}, d))\frac{\phi(d)}{2ord_d(p^{4\ell})},$$

and

$$t = \sum_{d|\bar{n}} \sigma(p^{2\ell}, d)\frac{\phi(d)}{4ord_d(p^{4\ell})}.$$

Example 5.13. Let $n = 24$, $p = 2$ and $\ell = 1$. Then $\bar{n} = 3$ and the number of 1-complementary dual cyclic codes of length 24 over $\mathbb{F}_{16}$ is 2^{r+s+t}, where

$$\begin{aligned} r &= \sum_{d|\bar{n}} (1 - \xi(p^{\ell}, d))\frac{\phi(d)}{\mathrm{ord}_d(p^{4\ell})} \\ &= (1-0)\frac{\phi(1)}{\mathrm{ord}_1(2^4)} + (1-0)\frac{\phi(3)}{\mathrm{ord}_3(2^4)} \\ &= 1 + 2 = 3, \end{aligned}$$

$$s = \sum_{d|\bar{n}} \xi(p^{\ell}, d)(1 - \sigma(p^{2\ell}, d))\frac{\phi(d)}{2\mathrm{ord}_d(p^{4\ell})} = 0,$$

and

$$t = \sum_{d|\bar{n}} \sigma(p^{2\ell}, d)\frac{\phi(d)}{4\mathrm{ord}_d(p^{4\ell})} = 0.$$

Hence, the number of 1-complementary dual cyclic codes of length 24 over $\mathbb{F}_{16}$ is $2^3 = 8$.

Example 5.14. Let $n = 18$, $p = 3$ and $\ell = 1$. Then $\bar{n} = 2$ and the number of 1-complementary dual cyclic codes of length 18 over $\mathbb{F}_{81}$ is 2^{r+s+t}, where

$$\begin{aligned} r &= \sum_{d|\bar{n}} (1 - \xi(p^{\ell}, d))\frac{\phi(d)}{\mathrm{ord}_d(p^{4\ell})} \\ &= (1-0)\frac{\phi(1)}{\mathrm{ord}_1(3^4)} + (1-0)\frac{\phi(2)}{\mathrm{ord}_2(3^4)} \\ &= 1 + 1 = 2, \end{aligned}$$

$$s = \sum_{d|\bar{n}} \xi(p^{\ell}, d)(1 - \sigma(p^{2\ell}, d)) \frac{\phi(d)}{2\mathrm{ord}_d(p^{4\ell})} = 0,$$

and

$$t = \sum_{d|\bar{n}} \sigma(p^{2\ell}, d) \frac{\phi(d)}{4\mathrm{ord}_d(p^{4\ell})} = 0.$$

Therefore, the number of 1-complementary dual cyclic codes of length 18 over $\mathbb{F}_{81}$ is $2^2 = 4$.

References

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

[2] Y. Jia, S. Ling, and C. Xing, On self-dual cyclic codes over finite fields, *IEEE Trans. Inform. Theory,* vol. 57, pp. 2243–2251, 2011.

[3] S. Jitman, S. Ling, and P. Sole, Hermitian self-dual abelian codes, *IEEE Trans. Inform. Theory,* vol. 60, pp. 1496–1507, 2014.

[4] X. Kai and S. Zhu, On cyclic self-dual codes, *AAECC*, vol. 19, pp. 509–525, 2008.

[5] A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli, Nonbinary stabilizer codes over finite fields, *IEEE Trans. Info. Theory,* vol. 52, pp. 4892–4914, 2006.

[6] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press, 1997.

[7] S. Ling, C. Xing, *Coding Theory : A First Course*, Cambridge University Press, 2004.

[8] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Elsevier/North-Holland, Amsterdam, 1977.

[9] J. L. Massey, Linear codes with complementary duals, *Discrete Mathematics*, vol. 106-107 pp. 337–342, 1992.

[10] G. Nebe, E. M. Rains, and N. J. A. Sloane, *Self-Dual Codes and Invariant Theory,* Algorithms and Computation in Mathematics vol. 17. Berlin, Heidelberg: Springer-Verlag, 2006.

[11] E. Sangwisut, S. Jitman, S. Ling, and P. Udomkavanich, Hulls of cyclic and negacyclic codes over finite fields, *Finite Field and Their Applications*, vol. 33, pp. 232–257, 2015.

[12] X. Yang, J. L. Massey, The condition for a cyclic code to have a complementary dual, *Discrete Mathematics*, vol. 126, pp. 391–393, 1994.

Biography

Name	Miss Jareena Tharnnukhroh
Address	163 Puttharaksa Road, Huaichorakha, Muang Nakhon Pathom, 73000
Date of Birth	17 September 1990
Education	
2012	Bachelor of Science in Mathematics, Silpakorn University
2015	Master of Science in Mathematics, Silpakorn University