On self-dual cyclic codes over finite fields

Jia, Yan; Ling, San; Xing, Chaoping

2011

Jia, Y., Ling, S. & Xing, C. (2011). On Self-Dual Cyclic Codes over Finite Fields. IEEE Transactions on Information Theory, 57(4), 2243 - 2251.

https://hdl.handle.net/10356/94048

https://doi.org/10.1109/TIT.2010.2092415

On Self-Dual Cyclic Codes over Finite Fields

Yan Jia, San Ling, Chaoping Xing

Abstract

In coding theory, self-dual codes and cyclic codes are important classes of codes which have been extensively studied. The main objects of study in this paper are self-dual cyclic codes over finite fields, i.e., the intersection of these two classes. We show 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. We also show that, over a fixed field, the latter case occurs more frequently as the length grows.

Index Terms

self-dual, cyclic code, finite field, generator polynomial

I. Introduction

Cyclic codes and self-dual codes over finite fields are important classes of block codes that have been extensively studied, for their beautiful underlying algebraic structures, fascinating links to other objects such as polynomials and lattices, as well as practicality for use. The intersection of these two classes, i.e., self-dual cyclic codes over finite fields, forms the focus of the study in this paper. In particular, we investigate issues related to their existence, characterization and enumeration.

First, 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 $\mathbb{F}_q[x]/(x^n - 1)$, and 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 $x^n - 1$. Through obtaining a characterization of the generator polynomials of the self-dual cyclic codes, based on the irreducible factors of $x^n - 1$, 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 aforesaid 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.

This paper is organized as follows. After a brief introduction to the key notions and notations in Section 2, the conditions for the existence of self-dual cyclic codes are given in Section 3. In Section 4, we give a characterization of the generator polynomials of self-dual cyclic codes, which is then used in Section 5 for the enumeration formula. Section 6 deals with the asymptotic occurrence problem explained above. A summary and a brief discussion of open problems conclude the paper in Section 7.

II. Preliminaries

Let $\mathbb{F}_q$ denote the finite field of $q = p^m$ elements where p is a prime and m is 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 $\mathbb{F}_q$.

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

The *dual* 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. It is denoted by $\mathscr{C}^\perp$. In particular, if $\mathscr{C} = \mathscr{C}^\perp$, then $\mathscr{C}$ is called a *self-dual* code.

If $\mathscr{C}$ is an $[n, k]_q$ code, then $\mathscr{C}^\perp$ is an $[n, n-k]_q$ code. Obviously, a self-dual code $\mathscr{C}$ over $\mathbb{F}_q$ must be an $[n, \frac{n}{2}]_q$ code, which implies n must be even.

The authors are with Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371.

The research is partially supported by the Singapore National Research Foundation Competitive Research Program grant NRF-CRP2-2007-03 and the Singapore Ministry of Education under Research Grant T208B2206.

An $[n,k]_q$ code $\mathscr{C}$ is called *cyclic* provided that, for each codeword $\mathbf{c}=(c_0,c_1,\ldots,c_{n-1})$ in $\mathscr{C}$, the vector $(c_{n-1},c_0,\ldots,c_{n-2})$ is also a codeword in $\mathscr{C}$.

We briefly state some well-known facts regarding cyclic codes. For further details, [3] can be consulted. There is a one-to-one correspondence between the vectors $\mathbf{c}=(c_0,c_1,\ldots,c_{n-1})$ in $\mathbb{F}_q^n$ and the polynomials $c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$ in $\mathbb{F}_q[x]$ of degree at most $n-1$. Under this correspondence, a cyclic code $\mathscr{C}$ of length n over $\mathbb{F}_q$ can be regarded as a principal ideal in the quotient ring $\mathbf{R_n}=\mathbb{F}_q[x]/(x^n-1)$. Therefore, we also regard $\mathscr{C}$ as an ideal in $\mathbf{R_n}$. Among all the generators of the ideal $\mathscr{C}$, there is a unique monic one with minimal degree that divides x^n-1. It is called the *generator polynomial* of the cyclic code $\mathscr{C}$ and we denote it by $G(x)$. The dimension of $\mathscr{C}$ is $n-\deg G(x)$. Let

$$H(x)=(x^n-1)/G(x). \tag{1}$$

$H(x)$ is called the *check polynomial* of $\mathscr{C}$. Suppose that $H(x)=H_bx^b+\cdots+H_1x+H_0$, where b is the degree of $H(x)$ and H_i $(0\le i\le b)$ are coefficients from $\mathbb{F}_q$. Note that $H_b=1$ and $H_0\neq 0$. We define

$$\overleftarrow{H}(x)=x^{\deg H(x)}H(x^{-1})=H_0x^b+H_1x^{b-1}+\cdots+H_{b-1}x+H_b=x^bH(x^{-1}).$$

Then the *reciprocal polynomial* of $H(x)$ is

$$H^*(x)=H_0^{-1}\overleftarrow{H}(x).$$

In particular, if a polynomial is equal to its reciprocal polynomial over $\mathbb{F}_q$, then it is called *self-reciprocal* over $\mathbb{F}_q$. Notice that $H^*(x)$ is a monic polynomial and it divides x^n-1 over $\mathbb{F}_q$. Actually, $H^*(x)$ is the generator polynomial of $\mathscr{C}^\perp$, so the dimension of $\mathscr{C}^\perp$ is $n-\deg H(x)$. Therefore we have the following proposition.

Proposition 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 $H(x)$.

III. Existence of Self-Dual Cyclic Codes

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 1. *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,

$$\begin{array}{rrl} & G(x^{-1})H(x^{-1}) &= x^{-n}-1,\\ \Rightarrow & (G_0G^*(x))(H_0H^*(x)) &= 1-x^n,\\ \Rightarrow & G^*(x)H^*(x) &= x^n-1. \end{array} \tag{2}$$

By Proposition 1, we have

$$\begin{array}{rrl} & G(x) &= H^*(x),\\ \Rightarrow & \overleftarrow{G}(x) &= H_0^{-1}H(x),\\ \Rightarrow & G_0G^*(x) &= H_0^{-1}H(x),\\ \Rightarrow & G^*(x) &= -H(x). \end{array} \tag{3}$$

Therefore, we have $G^*(x)H^*(x)=-H(x)G(x)=-(x^n-1)$. Then by (2) and (3), 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 1, it is easy to check that the cyclic code with generator polynomial $x^{\frac{n}{2}}+1$ is self-dual. ∎

Theorem 1 gives a necessary and sufficient condition for the existence of self-dual cyclic codes.

The final part of the proof of Theorem 1 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 1. *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 $\mathscr{C}[n]_{2^m}$, or simply $\mathscr{C}$ without specifying the length n and the field $\mathbb{F}_{2^m}$ if no confusion arises.*

Throughout the rest of this paper, in view of Theorem 1, we assume that the integer n is even and $q=2^m$ for some positive integer m.

IV. 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

$$n = 2^{\nu(n)}\bar{n}, \tag{4}$$

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 [2, p. 2753]:

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

where $f_i(x)$ $(1 \le i \le s)$ are monic irreducible self-reciprocal polynomials over $\mathbb{F}_{2^m}$ while $h_j(x)$ and its reciprocal polynomial $h_j^*(x)$ $(1 \le j \le t)$ 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 2. *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 Equation* (4)*.*

Therefore,

$$x^n+1 = f_1(x)^{2^{\nu(n)}}\cdots f_{s(n,m)}(x)^{2^{\nu(n)}}h_1(x)^{2^{\nu(n)}}h_1^*(x)^{2^{\nu(n)}}\cdots h_{t(n,m)}(x)^{2^{\nu(n)}}h_{t(n,m)}^*(x)^{2^{\nu(n)}}. \tag{5}$$

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 2. *Let x^n+1 be factorized as in Equation* (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*

$$f_1(x)^{2^{\nu(n)-1}}\cdots f_s(x)^{2^{\nu(n)-1}}h_1(x)^{\beta_1}h_1^*(x)^{2^{\nu(n)}-\beta_1}\cdots h_t(x)^{\beta_t}h_t^*(x)^{2^{\nu(n)}-\beta_t}, \tag{6}$$

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

By Proposition 1, $\mathscr{C}$ is self-dual if and only if $G(x) = H^*(x)$, i.e.,

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

or, equivalently,

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

Therefore, $\mathscr{C}$ is self-dual if and only if its generator polynomial $G(x)$ is of the form as in Equation (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 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 $1 \le j \le t(n,m)$. Thus we immediately have the following corollary.

TABLE I
SELF-DUAL CYCLIC CODES OVER $\mathbb{F}_2$ OF LENGTHS UP TO 46

n	$\bar{n}$	$(2^{\nu(n)}+1)^{t(n,1)}$	$G(x)$	n	$\bar{n}$	$(2^{\nu(n)}+1)^{t(n,1)}$	$G(x)$
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	$1^4 0^6 1^6 0^2 1^2 0^2 1^2$
			$1^1 0^1 1^1 0^5 1^1 0^1 1^1 0^1 1^1 0^1 1^1$				$1^1 0^{22} 1^1$
							$1^2 0^2 1^2 0^2 1^6 0^6 1^4$

Corollary 1. *Let x^n+1 be factorized over $\mathbb{F}_{2^m}$ as in Equation* (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 1. 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 I 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 $1+x+x^2+x^3+x^6+x^7$.

Table II lists all self-dual cyclic codes of lengths up to 30 over $\mathbb{F}_4$. In Table II, 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 order. For example, $[w,w,1,1]$ means the generator polynomial is $w+wx+x^2+x^3$.

TABLE II
SELF-DUAL CYCLIC CODES OVER $\mathbb{F}_4$ OF LENGTH UP TO 30

n	$\bar{n}$	$(2^{\nu(n)}+1)^{t(n,2)}$	$G(x)$
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	$[1,1,1,1,0,0,1,1]$, $[1,0,0,0,0,0,0,1]$, $[1,1,0,0,1,1,1,1]$
16	1	1	$[1,0,0,0,0,0,0,0,1]$
18	9	9	$[w,w,w^2,w^2,0,0,w^2,w^2,1,1]$, $[w^2,w^2,1,w,w^2,1,w,w^2,1,1]$, $[1,1,w,w,0,0,w^2,w^2,1,1]$
			$[w^2,0,0,w^2,0,0,1,0,0,1]$, $[1,0,0,0,0,0,0,0,0,1]$, $[w,0,0,w,0,0,1,0,0,1]$
			$[1,1,w^2,w^2,0,0,w,w,1,1]$, $[w,w,1,w^2,w,1,w^2,w,1,1]$, $[w^2,w^2,w,w,0,0,w,w,1,1]$
20	5	1	$[1,0,0,0,0,0,0,0,0,0,1]$
22	11	3	$[1,1,w,w,1,1,1,1,w^2,w^2,1,1]$, $[1,0,0,0,0,0,0,0,0,0,0,1]$, $[1,1,w^2,w^2,1,1,1,1,w,w,1,1]$
24	3	9	$[w^2,0,0,0,w^2,0,0,0,1,0,0,0,1]$, $[1,1,w^2,w,0,w,1,w^2,0,w^2,w,1,1]$
			$[w,0,w,0,1,0,w^2,0,w,0,1,0,1]$, $[w^2,w^2,1,w,w^2,1,w,w^2,1,w,w^2,1,1]$
			$[1,0,0,0,0,0,0,0,0,0,0,0,1]$, $[w,w,1,w^2,w,1,w^2,w,1,w^2,w,1,1]$
			$[w^2,0,w^2,0,1,0,w,0,w^2,0,1,0,1]$, $[1,1,w,w^2,0,w^2,1,w,0,w,w^2,1,1]$
			$[w,0,0,0,w,0,0,0,1,0,0,0,1]$
26	13	1	$[1,0,0,0,0,0,0,0,0,0,0,0,0,0,1]$
28	7	5	$[1,0,1,0,1,0,1,0,0,0,0,0,1,0,1]$, $[1,1,1,1,0,0,1,0,1,1,1,0,0,1,1]$
			$[1,0,0,0,0,0,0,0,0,0,0,0,0,0,1]$, $[1,1,0,0,1,1,1,0,1,0,0,1,1,1,1]$
			$[1,0,1,0,0,0,0,0,1,0,1,0,1,0,1]$
30	15	27	$[w^2,0,w,0,1,w^2,0,w,w^2,1,1,0,0,w^2,0,1]$, $[w,1,1,1,0,w^2,1,w^2,0,w^2,0,0,w,1,w^2,1]$
			$[1,0,1,0,w^2,1,w,1,1,w^2,1,w,0,1,0,1]$, $[1,w,w^2,0,1,0,1,w,0,w^2,0,w^2,1,0,w,1]$
			$[w^2,w^2,1,w,w^2,1,w,w^2,1,w,w^2,1,w,w^2,1,1]$, $[w,w^2,w,1,0,0,w^2,0,w^2,w,w^2,0,w,w,w,1]$
			$[w,0,0,0,0,w,0,0,0,0,1,0,0,0,0,1]$, $[1,w^2,0,1,w,0,w,0,w^2,1,0,1,0,w,w^2,1]$
			$[w^2,0,1,0,0,w^2,w^2,1,w,0,1,w^2,0,w,0,1]$, $[1,1,0,1,1,1,1,1,0,0,0,1,0,0,1,1,1]$
			$[w^2,1,w,0,w^2,w^2,w,w^2,0,1,1,w^2,1,0,w,1]$, $[w,w,w^2,1,w,1,w^2,1,w,w^2,w,1,w,w^2,1,1]$
			$[w,1,w^2,0,w,w,w^2,w,0,1,1,w,1,0,w^2,1]$, $[1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1]$
			$[w^2,w,0,w^2,1,w^2,w^2,0,1,w,1,1,0,w,w^2,1]$, $[w^2,w^2,w,1,w^2,1,w,1,w^2,w,w^2,1,w^2,w,1,1]$
			$[w,w^2,0,w,1,w,w,0,1,w^2,1,1,0,w^2,w,1]$, $[1,1,1,0,0,1,0,0,0,1,1,1,1,0,1,1]$
			$[w,0,w^2,0,1,w,0,w^2,w,1,1,0,0,w,0,1]$, $[1,w^2,w,0,1,0,1,w^2,0,w,0,w,1,0,w^2,1]$
			$[w^2,0,0,0,0,w^2,0,0,0,0,1,0,0,0,0,1]$, $[w^2,1,1,1,0,w,1,w,0,w,0,0,w^2,1,w,1]$
			$[w,w,1,w^2,w,1,w^2,w,1,w^2,w,1,w^2,w,1,1]$, $[1,w,0,1,w^2,0,w^2,0,w,1,0,1,0,w^2,w,1]$
			$[1,0,1,0,w,1,w^2,1,1,w,1,w^2,0,1,0,1]$, $[w^2,w,w^2,1,0,0,w,0,w,w^2,w,0,w^2,w^2,w^2,1]$
			$[w,0,1,0,0,w,w,1,w^2,0,1,w,0,w^2,0,1]$

V. 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 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 1, 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, [1] can be referred to. We adopt the same definitions and notations as in [1]. 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. *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 $ord_j(i)$, is defined to be the smallest integer e such that j divides i^e-1.*

Definition 4. *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 5. *Let χ be a function defined on the pair (j,m), with j odd, as follows:*

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

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

Lemma 1. *Let j be an odd positive integer. The jth cyclotomic polynomial $Q_j(x)$ factors into $\frac{\phi(j)}{e}$ distinct monic irreducible polynomials over $\mathbb{F}_{2^m}$ of the same degree e, where ϕ is the Euler function and $e = ord_j(2^m)$.*

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 [1, p. 65]. Hence we only show the second part.

Let $f(x)$ be any irreducible polynomial of degree e in the factorization of $Q_j(x)$ over $\mathbb{F}_{2^m}$, where e is the same as in the statement of the lemma. Then its reciprocal polynomial $f^*(x)$ is also irreducible and of degree e. 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

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

comprises all distinct roots of $f(x)$. Notice that even if $i > e-1$, $\xi^{2^{mi}}$ is also a root of $f(x)$. Here, we restrict i between 0 and $e-1$ 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 e roots of $f(x)$ are the e 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 $k \ge 0$, 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 1, 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. *Assume that $n = 2^{\nu(n)}\bar{n}$ and $x^n + 1$ is factorized as in* (5)*. Then the number of reciprocal polynomial pairs $t(n, m)$ is*

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

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

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

In particular, when 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 1 and the second part is from Corollary 1. 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 $k \ge 0$. 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 III and IV 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, 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 6. *Let $i \ge 0$ and $j \ge 1$ 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 7. *For each $r \ge 0$, let S_r^m be defined as $S_r^m := \{p : p$ is an odd prime and $2^r \parallel ord_p(2^m)\}$.*

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 [4, Theorem 1]. The following theorem follows immediately from [4, Theorem 1] when $a = 2^m$ and $b = 1$.

Theorem 4. *Let j be an odd positive integer and m a positive integer. Then $\chi(j, m) = 0$ if and only if there exists $e \ge 1$ such that $p \in S_e^m$ 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 $r \ge 1$, i.e., $ord_p(2^m)$ is even.*

By Theorem 4, if $p \in S_0^m$, then $\chi(p, m) = 1$. Moreover, we have

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

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

Generally, for every prime p, there exists $e_p \ge 0$, dependent on p, such that $p \in S_{e_p}^m$. We have $\chi(j, m) = 0$ if and only if these e_p's are all equal and positive for each prime p dividing j. Thus, by Theorem 4, we can determine the value of $\chi(j, m)$ as soon

TABLE III
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 IV
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						

as we know the value of e_p for each prime factor p of j. Given any m, the following proposition characterizes the e_p's for all odd primes p except for those congruent to 1 modulo 8.

Proposition 2. *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 4. 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

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

1) Case 1a: Let $p \equiv 3 \pmod 8$ and let m be odd. By Equation (7), we have
$$2^{m\frac{p-1}{2}} \equiv (-1)^m \equiv -1 \pmod p.$$
From this, we find that $\text{ord}_p(2^m)$ divides $p-1$ but not $\frac{p-1}{2}$. Since $2 \parallel p-1$, we have $2 \parallel \text{ord}_p(2^m)$. Therefore, we have $p \in S_1^m$.
2) Case 1b: Let $p \equiv 3 \pmod 8$ and let m be even. By Equation (7), we have
$$2^{m\frac{p-1}{2}} \equiv (-1)^m \equiv 1 \pmod p.$$
Then $\text{ord}_p(2^m)$ divides $\frac{p-1}{2}$. Since $\frac{p-1}{2}$ is odd, by Theorem 4, we have $p \in S_0^m$.
3) Case 2a: Let $p \equiv 5 \pmod 8$ and let m be odd. By Equation (7), we have
$$2^{m\frac{p-1}{2}} \equiv -1 \pmod p.$$
From this congruence, we find that $\text{ord}_p(2^m)$ divides $p-1$ but not $\frac{p-1}{2}$. Since $4 \parallel p-1$, we have $4 \parallel \text{ord}_p(2^m)$. Therefore, we have $p \in S_2^m$.
4) Case 2b: Let $p \equiv 5 \pmod 8$ and $m \equiv 2 \pmod 4$. By Equation (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, $\text{ord}_p(2^m)$ divides $\frac{p-1}{2}$ but not $\frac{p-1}{4}$. Since $2 \parallel \frac{p-1}{2}$, we have $2 \parallel \text{ord}_p(2^m)$. 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 $\text{ord}_p(2^m)$ 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 Equation (7), we have
$$2^{m\frac{p-1}{2}} \equiv 1^m \equiv 1 \pmod p,$$
for any m. Then $\text{ord}_p(2^m)$ divides $\frac{p-1}{2}$. Since $\frac{p-1}{2}$ is odd, we have $p \in S_0^m$.

■

Proposition 2 covers the cases for odd primes $p \equiv 3, 5$, 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 [4, Theorem 6]. We quote the result here without proof.

Proposition 3. *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 [4] that when $m = 1$, i.e. in the binary case, the smallest odd prime that is not covered by the cases in Propositions 2 and 3 is 337 and the density of the primes not covered is $1/32$.

By Proposition 2, since the sets $S_{e_p}^m$'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 4 and Proposition 2.

Theorem 5. *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 and 5, we immediately derive the following corollary.

Corollary 2. *Let $n = 2^{\nu(n)}\bar{n}$ as in (4). 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.*

VI. 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 1, we know that, when n is even, the trivial self-dual cyclic code always exists. From Theorem 3, 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 *non-unique case*. For a given field $\mathbb{F}_{2^m}$, we next discuss the distribution of the unique case as n varies.

Definition 8. *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 [4, Theorems 2 and 5] without proof here, is a more general result concerning the function $S^m(y)$.

Theorem 6. *Let a and b be two coprime positive integers. Let S denote the set of integers $m > 1$ such that m divides $a^k + b^k$ for some $k \geq 1$. 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 λ' be the largest number such that $\psi = u^{2^{\lambda'}}$, where u is a rational number. If $u = 2u_1^2$ with rational u_1 and $\lambda' = 0$, then

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

If $u = 2u_1^2$ with rational u_1 and $\lambda' = 1$, then

$$\delta_r = \begin{cases} \frac{7}{12}, & \text{if } r = 1, \\ \frac{8}{24}, & \text{if } r = 2, \\ \frac{1}{24} \cdot \frac{1}{2^{r-3}}, & \text{if } r \geq 3. \end{cases} \tag{9}$$

If $u = 2u_1^2$ with rational u_1 and $\lambda' \geq 2$, then

$$\delta_r = \begin{cases} 1 - \frac{1}{3} \cdot \frac{1}{2^{\lambda'}}, & \text{if } r = 1, \\ \frac{1}{3} \cdot \frac{1}{2^{\lambda'+r-1}}, & \text{if } r \geq 2. \end{cases} \tag{10}$$

We apply the above theorem to our case.

Theorem 7. *Let m be a positive integer and let λ be the integer such that $2^\lambda \parallel m$. 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 6: if $\lambda = 0$, then they are given in Equation (8)*; if $\lambda = 1$, then they are given in Equation* (9)*; if $\lambda \geq 2$, then they are given in Equation* (10)*.*

Proof: This theorem is just an application of Theorem 6 with $a = 2^m$ and $b = 1$. The function $S^m(y)$ here is just the function $S(y)$ in Theorem 6.

Suppose that λ' is the largest integer such that

$$2^m = u^{2^{\lambda'}}, \tag{11}$$

with rational $u = \frac{v}{w}$, where $\gcd(v, w) = 1$. Now it remains to show that λ' defined here is just the integer λ in the statement of the theorem, and u can be expressed as $2u_1^2$ with rational u_1. Then the result immediately follows from Theorem 6. From (11, we have

$$2^m w^{2^{\lambda'}} = v^{2^{\lambda'}}.$$

Then 2^m divides $v^{2^{\lambda'}}$ and hence 2 divides v. Since $\gcd(v, w) = 1$, w is not divisible by 2. Put $v = 2^i v_1$ with v_1 odd. Then

$$2^m w^{2^{\lambda'}} = 2^{2^{\lambda'} i} v_1^{2^{\lambda'}}.$$

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

$$m = 2^{\lambda'} i,$$
$$w = v_1.$$

Since $\gcd(v_1, w) = 1$ for $\gcd(v, w) = 1$, we have $v_1 = w = 1$ and thus $u = v = 2^i$. By Equation (11), the following holds:

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

We claim that the integer i is odd, for otherwise, we can write $2^m = (2^{\frac{i}{2}})^{2^{\lambda'+1}}$, contradicting the maximality of λ'. Therefore, the integer λ defined in this theorem is the same as the integer λ' defined in Theorem 6. Let $u_1 = 2^{\frac{i-1}{2}}$ for i is odd. Then $u = 2(u_1)^2$. 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.

VII. Conclusion and Future Work

In this paper, 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 non-existence 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).

In this paper, 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 2 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 2 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. Note that there are no binary "Type II" self-dual cyclic codes (see [8, Corollary 2]). After completion of our paper, we found that a portion of the results in the current paper was obtained in [11].

References

[1] R. Lidl and H. Niederreiter, Finite Fields, Cambridge Univ. Press, Cambridge, 1997

[2] 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

[3] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland Mathematical Library, 2003

[4] P. Moree, On the divisors of $a^k + b^k$, Acta Arithmetica, LXXX.3, pp. 197–212, 1997

[5] V. Pless, P. Solé, Z. Qian, Cyclic self-dual Z_4-codes, IEEE International Symposium on Information Theory-Proceedings, p. 200, 1997

[6] M. K. Siu, When is -1 a power of 2?, Math. Mag., vol. 48, no. 5, pp. 284–286, 1975

[7] 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

[8] 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

[9] K. Wiertalak, On the density of some sets of primes. I, II, Acta Arith., vol. 34, pp. 183-196 & pp. 197–210, 1977/78

[10] J. L. Yucas and G. L. Mullen, Self-reciprocal irreducible polynomials over finite fields, Designs, Codes and Cryptography, vol. 33, pp. 275–281, 2004

[11] X. Kai and S. Zhu, "On cyclic self-dual codes," AAECC, vol. 19, pp. 275-281, 2004.