British Journal of Mathematics & Computer Science
8(5): 401-410, 2015, Article no.BJMCS.2015.173
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

Self-Orthogonal Cyclic Codes and Complementary-dual Cyclic Codes of Length $p^n q^m$ over F_ℓ

Xingxing Chang[1] and Jian Gao[2*]

[1]*Common Courses Department, Hubei Industrial Polytechnic, Shiyan, Hubei 442000, China.*
[2]*Chern Institute of Mathematics and LPMC, Nankai University, Tianjin 300071, China.*

Article Information

DOI: 10.9734/BJMCS/2015/16892
Editor(s):
(1) Nikolaos Dimitriou Bagis, Department of Informatics and Mathematics, Aristotelian University of Thessaloniki, Greece.
Reviewers:
(1) Alexandre Ripamonti, Business Administration Department, University of Sao Paulo, Brazil.
(2) Anonymous, Poland.
Complete Peer review History: http://www.sciencedomain.org/review-history.php?iid=1034&id=6&aid=8962

Original Research Article

Received: 18 February 2015
Accepted: 11 March 2015
Published: 27 April 2015

Abstract

Let $F_\ell[x]/\langle x^{p^n q^m}-1\rangle$ and $d=\gcd(\phi(p^n),\phi(q^m))$, where p, q, ℓ are distinct odd primes, ℓ is a primitive root both modulo p^n and q^m, $p \nmid (q-1)$, $q \nmid p-1$. We obtain explicit expressions for all $dmn+m+n+1$ ℓ-cyclotomic cosets modulo $p^n q^m$. We explicitly determine generating polynomials and enumeration formulas of all self-orthogonal cyclic codes and complementary-dual cyclic codes of length $p^n q^m$ over F_ℓ. As an example, we give all self-orthogonal cyclic codes and complementary-dual cyclic codes of length 175 over F_3.

Keywords: Cyclotomic cosets; self-orthogonal; complementary-dual cyclic codes.

1 Introduction

Let F_ℓ be a finite field with ℓ elements and N be a positive integer coprime to ℓ. A linear code C is called cyclic if $(a_{N-1},a_0,a_1,\cdots,a_{N-2})\in C$ for every $(a_0,a_1,\cdots,a_{N-2},a_{N-1})\in C$. Let $F_\ell[x]/\langle x^N-1\rangle$. It is straightforward to show that a cyclic code of length N by viewing its codewords as polynomials is an ideal in R. For the linear code C of length N over F_ℓ the dual

**Corresponding author: jiangao@mail.nankai.edu.cn;*

code $C^{\perp}$ is defined as $C^{\perp}=\{u\in F_{\ell}^{N}\mid u\cdot v=0,\forall v\in C\}$. If C is a cyclic code, so is $C^{\perp}$. The code C is said to be self-orthogonal if $C\subseteq C^{\perp}$. The code C is said to be complementary-dual if $C\bigcap C^{\perp}=\{0\}$. The classes of self-orthogonal and complementary-dual codes have some attractive properties.

Self-orthogonal codes are closely related with the mathematical combination of design and lattice theory [1]. Using self-orthogonal cyclic codes, quantum codes can be construction, which have good parameters [2]. Cyclic codes over finite fields which are self-dual have been studied by many authors [3,4,5,6]. Recently, Bakshi-Raka [7] determined all the self-dual negacyclic codes of length 2^n over F_q, where q is a power of odd prime. Complementary-dual codes provide an optimum linear coding solution for the two-user binary adder channel. It was shown in [8] that asymptotically good complementary-dual exist and that complementary-dual codes have certain other attractive properties. Yang-Massy gave the necessary and sufficient condition for a cyclic code to be a complementary-dual code [9]. In recent years, Dinh has established the structure of the duals of all repeated-root constacyclic codes of lengths $3p^s$, $4p^s$ and $6p^s$ over F_{p^m}. By means of these structures, complementary-dual codes were obtained among them (see [10,11,12]). Sahni-Sehgal [13] have discussed cyclotomic cosets modulo p^nq and the minimal cyclic codes of length p^nq over F_ℓ, where p, q and ℓ are distinct odd primes, ℓ is a primitive root both modulo p^n and q, $d=\gcd(\phi(p^n),\phi(q))$, $p\nmid(q-1)$. In the direction of these previous researchers we obtain new results, which provide some theoretical basis of constructing good codes.

In this paper, we consider cyclic codes of length p^nq^m over F_ℓ, where p, q and ℓ are distinct odd primes, ℓ is a primitive root both modulo p^n and q^m, $d=\gcd(\phi(p^n),\phi(q^m))$, $p\nmid(q-1)$, $q\nmid p-1$. In Section 2, We use simple direct method obtain explicit expressions for all $dmn+m+n+1$ ℓ-cyclotomic cosets modulo p^nq^m. In Section 3, we explicitly determine generating polynomials and enumeration formulas of all self-orthogonal cyclic codes and complementary-dual cyclic codes of length p^nq^m over F_ℓ by means of the factorization of $x^{p^nq^m}-1$. At the end, as an example, we give all self-orthogonal cyclic codes and complementary-dual cyclic codes of length 175 over F_3.

2 ℓ-Cyclotomic Cosets Modulo p^nq^m

Throughout this paper we take $R=F_\ell[x]/\langle x^{p^nq^m}-1\rangle$, where p, q, ℓ are distinct odd primes, $m,n\geq 1$ are integers, ℓ is a primitive root both modulo p^n and q^m, $\gcd(\phi(p^n),\phi(q^m))=d\geq 2$, $p\nmid(q-1)$, $q\nmid p-1$. For $0\leq s\leq p^nq^m-1$, let $C_s=\{s,s\ell,s\ell^2,\cdots,s\ell^{n_s-1}\}$ be the ℓ-cyclotomic coset containing s, where $n_s=\{k\in Z^+ \mid s\ell^k\equiv s(\bmod p^nq^m)\}$. Let α be a primitive p^nq^m-th root of unity in some extension field of F_ℓ. It is well known that the polynomial

$$M_s(x)=\prod_{i\in C_s}(x-\alpha^i)$$

is the minimal polynomial of α^s over F_ℓ and

$$x^{p^n q^m} - 1 = \prod M_s(x)$$

gives the factorization of $x^{p^n q^m} - 1$ into irreducible factors over F_ℓ, where s runs over a complete set of representatives from distinct ℓ-cyclotomic cosets modulo $p^n q^m$.

For any integer $n \geq 1$, we denote by $ord_{Z_n^*}(\ell) = h$ the multiplicative order of ℓ in the multiplicative group Z_n^*, i.e. the order of ℓ modulo n. If $h = \phi(n)$, i.e. $Z_n^* = \langle \ell \rangle$, then ℓ is called a primitive root modulo n.

Lemma 1 [13, Lemma 5] There exists an integer a, $1 \leq a \leq pq$, satisfying $\gcd(a, pq\ell) = 1$ and $a, a^2, a^3, \cdots, a^{d-1} \notin S$, where $S = \{1, \ell, \ell^2, \cdots, \ell^{\frac{\phi(pq)}{d}-1}\}$.

Lemma 2 There exists an integer a, $1 \leq a \leq pq$, satisfying $\gcd(a, pq\ell) = 1$ and $a^t \not\equiv \ell^k (\bmod\, pq)$ for any integer t, k; $1 \leq t \leq d-1$ and $0 \leq k \leq \phi(pq)/d - 1$. Furthermore, for this fixed a and any $1 \leq i \leq n-1$, $0 \leq j \leq m-1$,

$$Z^*_{p^{n-i}q^{m-j}} = \{\langle \ell \rangle, a\langle \ell \rangle, a^2\langle \ell \rangle, \cdots, a^{d-1}\langle \ell \rangle\}.$$

Proof Since $\ell \in Z^*_{p^{n-i}q^{m-j}}$, as $Z^*_{p^{n-i}q^{m-j}}$ is a commutative group, we obtain $\langle \ell \rangle \trianglelefteq Z^*_{p^{n-i}q^{m-j}}$.

With the notation of Lemma 1, we have that

$$\{1, \ell, \cdots, \ell^{\frac{\phi(p^{n-i}q^{m-j})}{d}-1}, a, a\ell, \cdots, a\ell^{\frac{\phi(p^{n-i}q^{m-j})}{d}-1}, \cdots, a^{d-1}, a^{d-1}\ell, \cdots, a^{d-1}\ell^{\frac{\phi(p^{n-i}q^{m-j})}{d}-1}\}$$

has $\phi(p^{n-i}q^{m-j})$ elements coprime to pq. It is sufficient to prove that they are all pairwise incongruent modulo $p^{n-i}q^{m-j}$. Let $a^l\ell^k \equiv a^r\ell^t (\bmod\, p^{n-i}q^{m-j})$ with $0 \leq r \leq l \leq d-1$ and $0 \leq k, t \leq (\phi(p^{n-i}q^{m-j})/d) - 1$. Then $a^{l-r} \equiv \ell^{t-k} (\bmod\, p^{n-i}q^{m-j})$, which implies that $a^{l-r} \equiv \ell^s (\bmod\, pq)$ where $s \equiv t-k (\bmod\, \phi(pq)/d)$. Therefore, $a^{l-r} \in S$ and $0 \leq l-r < d$. Consequently, $l = r$. Therefore, we get $\ell^k \equiv \ell^t (\bmod\, p^{n-i}q^{m-j})$, where $0 \leq k, t \leq (\phi(p^{n-i}q^{m-j})/d) - 1$ and the order of ℓ modulo $p^{n-i}q^{m-j}$ is $\phi(p^{n-i}q^{m-j})/d$. Thus we have $k = t$, which implies that the set

$$\{1, \ell, \cdots, \ell^{\frac{\phi(p^{n-i}q^{m-j})}{d}-1}, a, a\ell, \cdots, a\ell^{\frac{\phi(p^{n-i}q^{m-j})}{d}-1}, \cdots, a^{d-1}, a^{d-1}\ell, \cdots, a^{d-1}\ell^{\frac{\phi(p^{n-i}q^{m-j})}{d}-1}\}$$

forms a reduced residue system modulo $p^{n-i}q^{m-j}$.

Theorem 1 Let p , q , ℓ be distinct odd primes, $m,n \geq 1$ be positive integers, $ord_{Z^*_{p^n}}(\ell) = \phi(p^n)$ and $ord_{Z^*_{q^m}}(\ell) = \phi(q^m)$, where $d = \gcd(\phi(p^n), \phi(q^m))$, $p \nmid (q-1)$, $q \nmid (p-1)$ and a be as defined in Lemma 2. Then $dmn + m + n + 1$ ℓ-cyclotomic cosets modulo $p^n q^m$ are

$$C_0 = \{0\} \ ,$$
$$C_{p^i q^m} = \{p^i q^m, p^i q^m \ell, p^i q^m \ell^2, \cdots, p^i q^m \ell^{\phi(p^{n-i})-1}\},$$
$$C_{p^n q^j} = \{p^n q^j, p^n q^j \ell, p^n q^j \ell^2, \cdots, p^n q^j \ell^{\phi(q^{m-j})-1}\},$$
$$C_{a^k p^i q^j} = \{a^k p^i q^j, a^k p^i q^j \ell, a^k p^i q^j \ell^2, \cdots, a^k p^i q^j \ell^{\frac{\phi(p^{n-i} q^{m-j})}{d}-1}\},$$

where $0 \leq i \leq n-1,\ 0 \leq j \leq m-1,\ 0 \leq k \leq d-1.$

Proof Since $\ell \in Z^*_{p^n q^m}$, as $Z^*_{p^n q^m}$ is a commutative group, we obtain $\langle \ell \rangle \trianglelefteq Z^*_{p^n q^m}$ and $|\langle \ell \rangle| = \dfrac{\phi(p^n q^m)}{d}$. From Lemma 2, $Z^*_{p^n q^m} = \{\langle \ell \rangle, a\langle \ell \rangle, a^2 \langle \ell \rangle, \cdots, a^{d-1}\langle \ell \rangle\}$. For $w \in Z^*_{p^n q^m}$, let $\gcd(w, p^n q^m) = d$. Then $w \in Z^*_{p^n q^m}$ if $d = 1$, and $w \in dZ^*_{p^n q^m}$ if $d \neq 1$. Thus, $Z_{p^n q^m} = \bigcup_{d | p^n q^m} dZ^*_{p^n q^m}$ and $dZ^*_{p^n q^m} \cong Z^*_{\frac{p^n q^m}{d}}$, where $0 \leq i \leq n-1,\ 0 \leq j \leq m-1$. Since $\langle \ell \rangle = Z^*_{p^{n-i}}$ and $a \in Z^*_p$, then $a \in Z^*_{p^{n-i}}$. Therefore $a = \ell^{i_1}$, where $0 \leq i_1 \leq \phi(p^{n-i}) - 1$. Thus

$$p^i q^m Z^*_{p^n q^m} = C_{p^i q^m} = \{p^i q^m \langle \ell \rangle_{p^{n-i}}, p^i q^m a \langle \ell \rangle_{p^{n-i}}, \cdots, p^i q^m a^{d-1} \langle \ell \rangle_{p^{n-i}}\} = \{p^i q^m \langle \ell \rangle_{p^{n-i}}\}.$$

Similarly, we also have

$$p^n q^j Z^*_{p^n q^m} = C_{p^n q^j} = \{p^n q^j \langle \ell \rangle_{q^{m-j}}, p^n q^j a \langle \ell \rangle_{q^{m-j}}, \cdots, p^n q^j a^{d-1} \langle \ell \rangle_{q^{m-j}}\} = \{p^n q^j \langle \ell \rangle_{q^{m-j}}\}.$$

Clearly,

$$a^k p^i q^j Z^*_{p^n q^m} = \bigcup_{k=0}^{d-1} C_{a^k p^i q^j} = \{p^i q^j \langle \ell \rangle_{p^{n-i} q^{m-j}}, a p^i q^j \langle \ell \rangle_{p^{n-i} q^{m-j}}, \cdots, a^{d-1} p^i q^j \langle \ell \rangle_{p^{n-i} q^{m-j}}\},$$

Where $\langle \ell \rangle_m = \{1, \ell, \cdots, \ell^{m'-1}\}$ and $ord(\ell) = m' (\bmod \ell)$.

Finally, these are all the ℓ-cyclotomic cosets modulo $p^n q^m$ because of

$$|C_0| + |C_{p^i q^m}| + |C_{p^n q^j}| + |C_{a^k p^i q^j}|$$

$$=1+\sum_{i=0}^{n-1}\phi(p^{n-i})+\sum_{j=0}^{m-1}\phi(q^{m-j})+\sum_{i=0}^{n-1}\sum_{j=0}^{m-1}\sum_{k=0}^{d-1}\frac{\phi(p^{n-i}q^{m-j})}{d}$$
$$=1+p^n-1+q^m-1+d\times\frac{1}{d}\times(p^n-1)\times(q^m-1)$$
$$=p^nq^m.$$

The following Lemmas 3, 4 and 5 can be obtained easily by the results in [13]. Here, we omit these proofs.

Lemma 3 For each i, $0\le i\le n-1$, $-C_{p^iq^m}=C_{p^iq^m}$.

Lemma 4 For each j, $0\le j\le m-1$, $-C_{p^nq^j}=C_{p^nq^j}$.

Lemma 5 $-1\in C_1$ or $-1\in C_{a^{d/2}}$. If $-C_1=C_1$, then $-C_{a^kp^iq^j}=C_{a^kp^iq^j}$ and if $-C_1\in C_{a^{d/2}}$, then $-C_{a^kp^iq^j}=C_{a^{k+\frac{d}{2}}p^iq^j}$, for all i, j, k, $0\le i\le n-1$, $0\le j\le m-1$, $0\le k\le d-1$.

3 Cyclic Codes of Length p^nq^m Over F_ℓ

For any polynomial $f(x)=\sum_{i=0}^{r}a_ix^i$ of degree $r(a_r\ne 0)$ over F_ℓ, let $f^*(x)$ denote the reciprocal polynomial of $f(x)$ given by $f^*(x)=x^rf(\frac{1}{x})=\sum_{i=0}^{r}a_{r-i}x^i$. It is clear that $(fg)^*=f^*g^*$ for any polynomial $f(x),g(x)\in F_\ell[x]$. Let C be a cyclic code of length N over F_ℓ generated by $g(x)$. The annihilator of C, denoted by $ann(C)$ is the set of $ann(C)=\{f(x)\in F_\ell[x]/(x^n-1)\,|\,f(x)\cdot g(x)=0\}$. Put $h(x)=\frac{x^N-1}{g(x)}$. Clearly $ann(C)$ is an ideal in $F_\ell[x]/(x^n-1)$ generated by $h(x)$. It is well known that the dual code $C^\perp$ is $(ann(C))^*$ and is generated by $h^*(x)$.

Suppose that $f(x)$ is a monic polynomial of degree k with $f(0)=c\ne 0$. Then, by the momic reciprocal polynomial of $f(x)$, we mean the polynomial $\tilde{f}(x)=c^{-1}f^*(x)$.

Note that for any s, $M_{-s}(x)=\prod_{i\in C_{-s}}(x-\alpha^i)=\prod_{i\in C_s}(x-\alpha^{-i})$,

$$M_s^*(x)=x^{|C_s|}M_s^*(1/x)=\prod_{i\in C_s}(1-x\alpha^i)=M_s(0)\prod_{i\in C_s}(x-\alpha^{-i})=M_s(0)M_{-s}(x), \tag{1}$$

$$\tilde{M}_s(x) = \frac{1}{M_s(0)} M_s^*(x) = M_{-s}(x). \tag{2}$$

Let C be a cyclic code of length $p^n q^m$ over F_ℓ. We have $C = \langle g(x) \rangle$. And for $0 \le i \le n-1$, $0 \le j \le m-1$, $0 \le k \le d-1$, ε_0, $\varepsilon_{i,m}$, $\varepsilon_{n,j}$, $\varepsilon_{k,i,j} \in \{0,1\}$, we have

$$g(x) = (x-1)^{\varepsilon_0} \prod_{i=0}^{n-1} (M_{p^i q^m}(x))^{\varepsilon_{i,m}} \prod_{j=0}^{m-1} (M_{p^n q^j}(x))^{\varepsilon_{n,j}} \prod_{k=0}^{d-1} \prod_{i=0}^{n-1} \prod_{j=0}^{m-1} (M_{a^k p^i q^j}(x))^{\varepsilon_{k,i,j}} \tag{3}$$

Therefore,

$$h(x) = (x-1)^{1-\varepsilon_0} \prod_{i=0}^{n-1} (M_{p^i q^m}(x))^{1-\varepsilon_{i,m}} \prod_{j=0}^{m-1} (M_{p^n q^j}(x))^{1-\varepsilon_{n,j}} \prod_{k=0}^{d-1} \prod_{i=0}^{n-1} \prod_{j=0}^{m-1} (M_{a^k p^i q^j}(x))^{1-\varepsilon_{k,i,j}}$$

Using equation (1) we get, for some nonzero element $\gamma \in F_\ell$,

$$h^*(x) = \gamma (x-1)^{1-\varepsilon_0} \prod_{i=0}^{n-1} (M_{-p^i q^m}(x))^{1-\varepsilon_{i,m}} \prod_{j=0}^{m-1} (M_{-p^n q^j}(x))^{1-\varepsilon_{n,j}} \prod_{k=0}^{d-1} \prod_{i=0}^{n-1} \prod_{j=0}^{m-1} (M_{-a^k p^i q^j}(x))^{1-\varepsilon_{k,i,j}}.$$

(i) If $-C_1 = C_1$, from Lemmas 3, 4 and 5, we get

$$h^*(x) = \gamma (x-1)^{1-\varepsilon_0} \prod_{i=0}^{n-1} (M_{p^i q^m}(x))^{1-\varepsilon_{i,m}} \prod_{j=0}^{m-1} (M_{p^n q^j}(x))^{1-\varepsilon_{n,j}} \prod_{k=0}^{d-1} \prod_{i=0}^{n-1} \prod_{j=0}^{m-1} (M_{a^k p^i q^j}(x))^{1-\varepsilon_{k,i,j}}. \tag{4}$$

(ii) If $-C_1 = C_{a^{d/2}}$, from Lemmas 3, 4 and 5, we get

$$h^*(x) = \gamma (x-1)^{1-\varepsilon_0} \prod_{i=0}^{n-1} (M_{p^i q^2}(x))^{1-\varepsilon_{i,2}} \prod_{j=0}^{m-1} (M_{p^n q^j}(x))^{1-\varepsilon_{n,j}} \prod_{k=0}^{d-1} \prod_{i=0}^{n-1} \prod_{j=0}^{m-1} (M_{a^{k+\frac{d}{2}} p^i q^j}(x))^{1-\varepsilon_{k,i,j}}. \tag{5}$$

Let $S = \{\varepsilon_0, \varepsilon_{i,m}, \varepsilon_{n,j}, \varepsilon_{k,i,j} \mid 0 \le i \le n-1, 0 \le j \le m-1, 0 \le k \le d-1\}$ and

$$S' = \{\varepsilon_0, \varepsilon_{i,m}, \varepsilon_{n,j} \mid 0 \le i \le n-1, 0 \le j \le m-1\}$$

3.1 Self-orthogonal Cyclic Codes of Length $p^n q^m$ over F_ℓ

Theorem 2 For p, q, ℓ be distinct odd primes, $m, n \ge 1$ are integers, ℓ is a primitive root both modulo p^n and q^m, $\gcd(\phi(p^n), \phi(q^m)) = d \ge 2$, $p \nmid (q-1)$, $q \nmid (p-1)$, $0 \le i \le n-1$, $0 \le j \le m-1$ and $0 \le k \le d-1$.

(i) If $-C_1 = C_1$, then the self-orthogonal cyclic codes of length $p^n q^m$ over F_ℓ are $C = 0$.

(ii) If $-C_1 = C_{a^{d/2}}$, then there are precisely $3^{\frac{dmn}{2}}$ self-orthogonal cyclic codes of length $p^n q^m$ over F_ℓ given by

$$\left\langle (x-1)^{\varepsilon_0} \prod_{i=0}^{n-1} (M_{p^i q^m}(x))^{\varepsilon_{i,m}} \prod_{j=0}^{m-1} (M_{p^n q^j}(x))^{\varepsilon_{n,j}} \prod_{k=0}^{d-1} \prod_{i=0}^{n-1} \prod_{j=0}^{m-1} (M_{a^k p^i q^j}(x))^{\varepsilon_{k,i,j}} \right\rangle$$

where ε_0, $\varepsilon_{i,m}$, $\varepsilon_{n,j}$ are always equal to 1 and at least one of $\varepsilon_{k,i,j}$ and $\varepsilon_{k+\frac{d}{2},i,j}$ is 1 for each i, j, k ($k+\dfrac{d}{2}$ is modulo d).

Proof (i) Let C be a self-orthogonal cyclic code of length $p^n q^m$ over F_ℓ. If $-C_1 = C_1$, then we have $C = \langle g(x) \rangle$ .Since $C \subseteq C^\perp$, it follows that $h^*(x) \mid g(x)$ (expression of $g(x)$ and $h^*(x)$ see equation (3),(4)). This is possible if and only if $\varepsilon_s \ge 1 - \varepsilon_s$ and $\varepsilon_s \in \{0,1\}$, where $\varepsilon_s \in S$. Consequently, $\varepsilon_s = 1$. Therefore $C = 0$.

(ii) If $-C_1 = C_{a^{d/2}}$, we have $C = \langle g(x) \rangle$, $h^*(x) \mid g(x)$ (expression of $g(x)$ and $h^*(x)$ see equation(3),(5)). This is possible if and only if $\varepsilon_{s'} \ge 1 - \varepsilon_{s'}$, and $\varepsilon_{s'} \in \{0,1\}$, where $\varepsilon_{s'} \in S'$. Consequently, $\varepsilon_{s'} = 1$ and $\varepsilon_{k,i,j} + \varepsilon_{k+\frac{d}{2},i,j} \ge 1$.

3.2 Complementary-dual Cyclic Codes of Length $p^n q^m$ over F_ℓ

Lemma 6 [9, Theorem] If $g(x)$ is the generator polynomial of a cyclic code C of length N over F_ℓ, then C is a complementary-dual code if and only if $g(x)$ is self-reciprocial (i.e. $\tilde{g}(x) = g(x)$) and all the monic irreducible factors of $g(x)$ have the same multiplicity in $g(x)$ and in $x^N - 1$.

Theorem 3 For p, q, ℓ be distinct odd primes, $m, n \ge 1$ are integers, ℓ is a primitive root both modulo p^n and q^m, $\gcd(\phi(p^n), \phi(q^m)) = d \ge 2$, $p \nmid (q-1)$, $q \nmid (p-1)$, $0 \le i \le n-1$, $0 \le j \le m-1$ and $0 \le k \le d-1$.

(i) If $-C_1 = C_1$, then there are precisely $2^{dmn+m+n+1}$ complementary-dual cyclic codes of length $p^n q^m$ over F_ℓ given by

$$\left\langle (x-1)^{\varepsilon_0} \prod_{i=0}^{n-1} (M_{p^i q^m}(x))^{\varepsilon_{i,m}} \prod_{j=0}^{m-1} (M_{p^n q^j}(x))^{\varepsilon_{n,j}} \prod_{k=0}^{d-1} \prod_{i=0}^{n-1} \prod_{j=0}^{m-1} (M_{a^k p^i q^j}(x))^{\varepsilon_{k,i,j}} \right\rangle,$$

where $\varepsilon_0, \varepsilon_{i,m}, \varepsilon_{n,j}, \varepsilon_{k,i,j} \in \{0,1\}$.

(ii) If $-C_1 = C_{a^{d/2}}$, then there are precisely $2^{\frac{dmn}{2}+m+n+1}$ complementary-dual cyclic codes of length $p^n q^m$ over F_ℓ given by

$$\left\langle (x-1)^{\varepsilon_0} \prod_{i=0}^{n-1} (M_{p^i q^m}(x))^{\varepsilon_{i,m}} \prod_{j=0}^{m-1} (M_{p^n q^j}(x))^{\varepsilon_{n,j}} \prod_{k=0}^{d-1} \prod_{i=0}^{n-1} \prod_{j=0}^{m-1} (M_{a^k p^i q^j}(x))^{\varepsilon_{k,i,j}} \right\rangle,$$

where $\varepsilon_0, \varepsilon_{i,m}, \varepsilon_{n,j}, \varepsilon_{k,i,j} \in \{0,1\}$, and $\varepsilon_{k,i,j} = \varepsilon_{k+\frac{d}{2},i,j}$ ($k+\frac{d}{2}$ is modulo d).

Proof (i) From Lemmas 3, 4, and 5, if $-C_1 = C_1$, we get $M_1(x) = M_{-1}(x)$, $M_{p^i q^m}(x) = M_{-p^i q^m}(x)$, $M_{p^n q^j}(x) = M_{-p^n q^j}(x)$, $M_{a^k p^i q^j}(x) = M_{-a^k p^i q^j}(x)$, but $\tilde{M}_s(x) = M_{-s}(x)$ (see equation (1)), where $\varepsilon_s \in S$, so $\tilde{M}_1(x) = M_1(x)$, $\tilde{M}_{p^i q^m}(x) = M_{p^i q^m}(x)$, $\tilde{M}_{p^n q^j}(x) = M_{p^n q^j}(x)$, $\tilde{M}_{a^k p^i q^j}(x) = M_{a^k p^i q^j}(x)$.

Then by Lemma 6, complementary-dual cyclic codes of length $p^n q^m$ over F_ℓ are

$$\left\langle (x-1)^{\varepsilon_0} \prod_{i=0}^{n-1} (M_{p^i q^m}(x))^{\varepsilon_{i,m}} \prod_{j=0}^{m-1} (M_{p^n q^j}(x))^{\varepsilon_{n,j}} \prod_{k=0}^{d-1} \prod_{i=0}^{n-1} \prod_{j=0}^{m-1} (M_{a^k p^i q^j}(x))^{\varepsilon_{k,i,j}} \right\rangle.$$

(ii) From Lemmas 3, 4 and 5, if $-C_1 = C_{a^{d/2}}$, we have $M_1(x) = M_{-1}(x)$, $M_{p^i q^m}(x) = M_{-p^i q^m}(x)$, $M_{p^n q^j}(x) = M_{-p^n q^j}(x)$, $M_{-a^k p^i q^j}(x) = M_{a^{k+\frac{d}{2}} p^i q^j}(x)$. However, $\tilde{M}_s(x) = M_{-s}(x)$ (see equation (2)), where $\varepsilon_s \in S$, which implies that $\tilde{M}_1(x) = M_1(x)$, $\tilde{M}_{p^i q^m}(x) = M_{p^i q^m}(x)$, $\tilde{M}_{p^n q^j}(x) = M_{p^n q^j}(x)$ and $\tilde{M}_{a^k p^i q^j}(x) = M_{a^{k+\frac{d}{2}} p^i q^j}(x)$.

Then by Lemma 6, complementary-dual cyclic codes of length $p^n q^m$ over F_ℓ are

$$\left\langle (x-1)^{\varepsilon_0} \prod_{i=0}^{n-1} (M_{p^i q^m}(x))^{\varepsilon_{i,m}} \prod_{j=0}^{m-1} (M_{p^n q^j}(x))^{\varepsilon_{n,j}} \prod_{k=0}^{d-1} \prod_{i=0}^{n-1} \prod_{j=0}^{m-1} (M_{a^k p^i q^j}(x))^{\varepsilon_{k,i,j}} \right\rangle,$$

where $\varepsilon_0, \varepsilon_{i,m}, \varepsilon_{n,j}, \varepsilon_{k,i,j} \in \{0,1\}$, and $\varepsilon_{k,i,j} = \varepsilon_{k+\frac{d}{2},i,j}$ ($k+\frac{d}{2}$ is modulo d).

4 An Example

Take $\ell = 3$, $p = 7$, $q = 5$, $n = 1$, $m = 2$. Then $d = 2$, $a = 19$, $-1 \in C_{a^{d/2}}$.

(a) The eight 3-cyclotomic cosets modulo 175 are

$C_0 = \{0\}$,
$C_1 = \{1, 3, 4, 9, 11, 12, 13, 16, 17, 27, 29, 33, 36, 38, 39, 44, 46, 47, 48, 51, 52, 62, 64, 68, 71, 73, 74, 79, 81, 82, 83, 86, 87, 97, 99, 103, 106, 108, 109, 114, 116, 117, 118, 121, 122, 132, 134, 138, 141, 143, 144, 149, 151, 152, 153, 156, 157, 167, 169, 173\}$,
$C_5 = \{5, 15, 20, 45, 55, 60, 65, 80, 85, 135, 145, 165\}$,
$C_7 = \{7, 14, 21, 28, 42, 49, 56, 63, 77, 84, 91, 98, 112, 119, 126, 133, 147, 154, 161, 168\}$
$C_{19} = \{2, 6, 8, 18, 19, 22, 23, 24, 26, 31, 32, 34, 37, 41, 43, 53, 54, 57, 58, 59, 61, 66, 67, 69, 72, 76, 78, 88, 89, 92, 93, 94, 96, 101, 102, 104, 107, 111, 113, 123, 124, 127, 128, 129, 131, 136, 137, 139, 142, 146, 148, 158, 159, 162, 163, 164, 166, 171, 172, 174\}$,
$C_{25} = \{25, 50, 75, 100, 125, 150\}$, $C_{35} = \{35, 70, 105, 140\}$,
$C_{95} = \{10, 30, 40, 90, 95, 110, 115, 120, 130, 155, 160, 170\}$.

(b) 9 self-orthogonal cyclic codes of length 175 over F_3 are

$$\langle M_0(x)M_{25}(x)M_7(x)M_{35}(x)M_1(x)M_{19}(x)M_5(x)M_{95}(x)\rangle,$$
$$\langle M_0(x)M_{25}(x)M_7(x)M_{35}(x)M_1(x)M_5(x)\rangle,$$
$$\langle M_0(x)M_{25}(x)M_7(x)M_{35}(x)M_1(x)M_{95}(x)\rangle,$$
$$\langle M_0(x)M_{25}(x)M_7(x)M_{35}(x)M_{19}(x)M_5(x)\rangle,$$
$$\langle M_0(x)M_{25}(x)M_7(x)M_{35}(x)M_{19}(x)M_{95}(x)\rangle,$$
$$\langle M_0(x)M_{25}(x)M_7(x)M_{35}(x)M_1(x)M_{19}(x)M_5(x)\rangle,$$
$$\langle M_0(x)M_{25}(x)M_7(x)M_{35}(x)M_1(x)M_{19}(x)M_{95}(x)\rangle,$$
$$\langle M_0(x)M_{25}(x)M_7(x)M_{35}(x)M_1(x)M_5(x)M_{95}(x)\rangle,$$
$$\langle M_0(x)M_{25}(x)M_7(x)M_{35}(x)M_{19}(x)M_5(x)M_{95}(x)\rangle.$$

(c) 64 complementary-dual cyclic codes codes of length 175 over F_3 are

$$\Big\langle (x-1)^{\varepsilon_0}(x^{120} - x^{115} + x^{95} - x^{90} + x^{85} - x^{80} + x^{70} - x^{65} + x^{60} - x^{55} + x^{50} - x^{40} + x^{35} - x^{30} + x^{25} - x^5 + 1)^{\varepsilon_{0,0,0}}(x^{24} - x^{23} + x^{19} - x^{18} + x^{17} - x^{16} + x^{14} - x^{13} + x^{12} - x^{11} + x^{10} - x^8 + x^7 - x^6 + x^5 - x + 1)^{\varepsilon_{0,0,1}}(1 + x^5 + x^{10} + x^{15} + x^{20})^{\varepsilon_{1,0}}(1 + x + x^2 + x^3 + x^4 + x^5 + x^6)^{\varepsilon_{0,2}}(1 + x + x^2 + x^3 + x^4)^{\varepsilon_{1,1}} \Big\rangle$$

where ε_0, $\varepsilon_{0,0,0}$, $\varepsilon_{0,0,1}$, $\varepsilon_{1,0}$, $\varepsilon_{0,2}$, $\varepsilon_{1,1} \in \{0,1\}$.

5 Conclusion

In this paper, we mainly consider cyclic codes of length $p^n q^m$ over F_ℓ. We explicitly determine generating polynomials and enumeration formulas of all self-orthogonal cyclic codes and complementary-dual cyclic codes of length $p^n q^m$ over F_ℓ. Construction of good self-orthogonal cyclic codes and complementary-dual cyclic codes of length $p^n q^m$ over F_ℓ may be interesting.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Wan ZX. A characteristic property of self-orthogonal codes and its application to lattices. Bull. Belg. Math. Soc. 1998;5:477-482.

[2] Gang C, Ruihu L. Construction of self-orthogonal codes with dual distance three on ternary field. Computer Engineering and Application. Theory. 2011;47:38-39.

[3] Heijne B, Top J. On the minimal distance of binary self-dual cyclic codes. IEEE Trans. Inform. Theory. 2009;55(11):4860-4863.

[4] Jia Y, Ling S, Xing C. On self-dual cyclic codes over finite fields. IEEE Trans. Inform. Theory. 2011;57:2243-2251.

[5] Kai X, Zhu S. On cyclic self-dual codes. Appl. Algebra Engrg. Comm. Comput. 2008;19(6):509-525.

[6] Sloane N, Thompson J. Cyclic self-dual codes. IEEE Trans. Inform. Theory. 1983;29:364-367.

[7] Bakshi G, Raka M. A class of constacyclic codes over a finite field. Finite Fields Appl. 2012;18:362-377.

[8] Massey JL. Linear codes with complementary duals. Discrete Math. 1992;106/107:337-342.

[9] Yang X, Massey J. The condition for a cyclic code to have a complementary dual. Discrete Math. 1994;126:391-393.

[10] Dinh H. Struture of repeated-root constacyclic codes of length $3p^s$ and their duals. Discrete Math. 2013;313:983-991.

[11] Dinh H. On repeated-root constacyclic codes of length $4p^s$. Asian-European Journal of Math. 2013;6.

[12] Dinh H. Repeated-root cyclic and negacyclic codes of length $6p^s$. MAS Contemporary Mathematics. 2014;609:69-87.

[13] Sahni A, Sehgal P. Minimal cyclic codes of length $p^n q$. Finite Field Appl. 2012;18:1017-1036.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
www.sciencedomain.org/review-history.php?iid=1034&id=6&aid=8962