

Original Research Article
**Self-orthogonal cyclic codes and
complementary-dual cyclic codes of length $p^n q^m$
over F_ℓ**

Author details: Xingxing Chang¹, Jian Gao^{2*}

¹*Common Courses, Hubei Industrial of Polytechnic, Shiyan, Hubei 442000,
China*

²*Chern Institute of Mathematics and LPMC, Nankai University, Tianjin
300071, China*

E-mail address: jiangao@mail.nankai.edu.cn, changxingxing2012@126.com

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 $(a_{N-1}, a_0, a_1, \dots, a_{N-2}) \in C$ for every $(a_0, a_1, \dots, a_{N-2}, a_{N-1}) \in C$. 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 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 $C \cap C^\perp = \{0\}$. 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 (see [14]). Using self-orthogonal cyclic codes, quantum codes can be construction, which have good parameters (see [15]). Cyclic codes over finite fields which are self-dual have been studied by many authors (see [8,9,10,12]). Recently, Bakshi-Raka [2] 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 [16] 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 (see [13]). 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 [5,6,7]). Sahni-Sehgal [11] have discussed cyclotomic cosets modulo $p^n q$ and the minimal cyclic codes of length $p^n q$ 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 $p^n q^m$ 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 $p^n q^m$. In Section 3, we explicitly determine generating polynomials and enumeration formulas of all self-orthogonal cyclic codes and complementary-dual cyclic codes of length $p^n q^m$ over F_ℓ by means of the factorization of $x^{p^n q^m} - 1$. 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 $p^n q^m$

Throughout this paper we take $R = F_\ell[x] / \langle x^{p^n q^m} - 1 \rangle$, 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 $0 \leq s \leq p^n q^m - 1$, let $C_s = \{s, s\ell, s\ell^2, \dots, s\ell^{n_s-1}\}$ be the ℓ -cyclotomic coset containing s , where $n_s = \{k \in \mathbb{N}^+ \mid s\ell^k \equiv s \pmod{p^n q^m}\}$. Let α be a primitive $p^n q^m$ -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

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

71 gives the factorization of $x^{p^n q^m} - 1$ into irreducible factors over F_ℓ , where s runs over a
 72 complete set of representatives from distinct ℓ -cyclotomic cosets modulo $p^n q^m$.
 73

74 For any integer $n \geq 1$, we denote by $\text{ord}_{\square_n^*}(\ell) = h$ the multiplicative order of ℓ in the
 75 multiplicative group $\square_n^*$, i.e. the order of ℓ modulo n . If $h = \phi(n)$, i.e. $\square_{p^{n-1}}^* = \langle \ell \rangle$, then ℓ is
 76 called a primitive root modulo n .
 77

78 **Lemma 1**[11, Lemma 5] There exists an integer a , $1 \leq a \leq pq$, satisfying $\gcd(a, pq\ell) = 1$
 79 and $a, a^2, a^3, \dots, a^{d-1} \notin S$, where $S = \{1, \ell, \ell^2, \dots, \ell^{\frac{\phi(pq)-1}{d}}\}$.
 80

81 **Lemma 2** There exists an integer a , $1 \leq a \leq pq$, satisfying $\gcd(a, pq\ell) = 1$ and
 82 $a^t \not\equiv \ell^k \pmod{pq}$ for any integer t, k ; $1 \leq t \leq d-1$ and $0 \leq k \leq \phi(pq)/d - 1$.
 83 Furthermore, for this fixed a and any $1 \leq i \leq n-1$, $0 \leq j \leq m-1$,

$$84 \quad \square_{p^{n-i}q^{m-j}}^* = \{ \langle \ell \rangle, \langle a\ell \rangle, \langle a^2\ell \rangle, \dots, \langle a^{d-1}\ell \rangle \}.$$

85 *Proof* Since $\ell \in \square_{p^{n-i}q^{m-j}}^*$, as $\square_{p^{n-i}q^{m-j}}^*$ is a commutative group, we obtain $\langle \ell \rangle \trianglelefteq \square_{p^{n-i}q^{m-j}}^*$.
 86

86 With the notation of Lemma 1, we have that

$$87 \quad \{1, \ell, \dots, \ell^{\frac{\phi(p^{n-i}q^{m-j})}{d}-1}, a, a\ell, \dots, a\ell^{\frac{\phi(p^{n-i}q^{m-j})}{d}-1}, \dots, a^{d-1}, a^{d-1}\ell, \dots, a^{d-1}\ell^{\frac{\phi(p^{n-i}q^{m-j})}{d}-1}\}$$

88 has $\phi(p^{n-i}q^{m-j})$ elements coprime to pq . It is sufficient to prove that they are all pairwise
 89 incongruent modulo $p^{n-i}q^{m-j}$. Let $a^l \ell^k \equiv a^r \ell^t \pmod{p^{n-i}q^{m-j}}$ with $0 \leq r \leq l \leq d-1$ and
 90 $0 \leq k, t \leq (\phi(p^{n-i}q^{m-j})/d) - 1$. Then $a^{l-r} \equiv \ell^{t-k} \pmod{p^{n-i}q^{m-j}}$, which implies that
 91 $a^{l-r} \equiv \ell^s \pmod{pq}$ where $s \equiv t - k \pmod{\phi(pq)/d}$. Therefore, $a^{l-r} \in S$ and $0 \leq l - r < d$.
 92 Consequently, $l = r$. Therefore, we get $\ell^k \equiv \ell^t \pmod{p^{n-i}q^{m-j}}$, where
 93 $0 \leq k, t \leq (\phi(p^{n-i}q^{m-j})/d) - 1$ and the order of ℓ modulo $p^{n-i}q^{m-j}$ is $\phi(p^{n-i}q^{m-j})/d$. Thus
 94 we have $k = t$, which implies that the set

$$95 \quad \{1, \ell, \dots, \ell^{\frac{\phi(p^{n-i}q^{m-j})}{d}-1}, a, a\ell, \dots, a\ell^{\frac{\phi(p^{n-i}q^{m-j})}{d}-1}, \dots, a^{d-1}, a^{d-1}\ell, \dots, a^{d-1}\ell^{\frac{\phi(p^{n-i}q^{m-j})}{d}-1}\}$$

96 forms a reduced residue system modulo $p^{n-i}q^{m-j}$.
 97

98 **Theorem 1** Let p, q, ℓ be distinct odd primes, $m, n \geq 1$ be positive integers,
 99 $\text{ord}_{\square_{p^n}^*}(\ell) = \phi(p^n)$ and $\text{ord}_{\square_{q^m}^*}(\ell) = \phi(q^m)$, where $d = \gcd(\phi(p^n), \phi(q^m))$, $p \nmid (q-1)$,
 100 $q \nmid (p-1)$ and a be as defined in Lemma 2. Then $dmn + m + n + 1$ ℓ -cyclotomic cosets
 101 modulo $p^n q^m$ are

$$102 \quad C_0 = \{0\},$$

$$103 \quad C_{p^i q^m} = \{p^i q^m, p^i q^m \ell, p^i q^m \ell^2, \dots, p^i q^m \ell^{\phi(p^{n-i})-1}\},$$

$$C_{p^n q^j} = \{p^n q^j, p^n q^j \ell, p^n q^j \ell^2, \dots, p^n q^j \ell^{\phi(q^{m-j})-1}\},$$

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

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

Proof Since $\ell \in \square_{p^n q^m}^*$, as $\square_{p^n q^m}^*$ is a commutative group, we obtain $\langle \ell \rangle \leq \square_{p^n q^m}^*$ and

$|\langle \ell \rangle| = \frac{\phi(p^n q^m)}{d}$. From Lemma 2, $\square_{p^n q^m}^* = \{\langle \ell \rangle, a \langle \ell \rangle, a^2 \langle \ell \rangle, \dots, a^{d-1} \langle \ell \rangle\}$. For

$w \in \square_{p^n q^m}^*$, let $\gcd(w, p^n q^m) = d$. Then $w \in \square_{p^n q^m}^*$ if $d=1$, and $w \in d \square_{p^n q^m}^*$ if $d \neq 1$.

Thus, $\square_{p^n q^m} = \bigcup_{d|p^n q^m} d \square_{p^n q^m}^*$ and $d \square_{p^n q^m}^* \cong \square_{\frac{p^n q^m}{d}}^*$, where $0 \leq i \leq n-1$, $0 \leq j \leq m-1$.

Since $\langle \ell \rangle = \square_{p^{n-i}}^*$ and $a \in \square_p^*$, then $a \in \square_{p^{n-i}}^*$. Therefore $a = \ell^{i_1}$, where

$0 \leq i_1 \leq \phi(p^{n-i})-1$. Thus

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

114

115 Similarly, we also have

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

117

118 Clearly,

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

120 , where $\langle \ell \rangle_m = \{1, \ell, \dots, \ell^{m'-1}\}$ and $\text{ord}(\ell) = m' \pmod{\ell}$.

121

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

$$\begin{aligned} & |C_0| + |C_{p^i q^m}| + |C_{p^n q^j}| + |C_{a^k p^i q^j}| \\ &= 1 + \sum_{i=0}^{n-1} \phi(p^{n-i}) + \sum_{j=0}^{m-1} \phi(q^{m-j}) + \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \sum_{k=0}^{d-1} \frac{\phi(p^{n-i} q^{m-j})}{d} \\ &= 1 + p^n - 1 + q^m - 1 + d \times \frac{1}{d} \times (p^n - 1) \times (q^m - 1) \\ &= p^n q^m. \end{aligned}$$

126

127 The following Lemmas 3, 4 and 5 can be obtained easily by the results in [11]. Here, we omit
128 these proofs.

129

130 **Lemma 3** For each i , $0 \leq i \leq n-1$, $-C_{p^i q^m} = C_{p^i q^m}$.

131

132 **Lemma 4** For each j , $0 \leq j \leq m-1$, $-C_{p^n q^j} = C_{p^n q^j}$.

133

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

136

137 **3. CYCLIC CODES OF LENGTH $p^n q^m$ OVER F_ℓ**

138

139 For any polynomial $f(x) = \sum_{i=0}^r a_i x^i$ of degree $r (a_r \neq 0)$ over F_ℓ , let $f^*(x)$ denote the

140 reciprocal polynomial of $f(x)$ given by $f^*(x) = x^r f(\frac{1}{x}) = \sum_{i=0}^r a_{r-i} x^i$. It is clear

141 that $(fg)^* = f^* g^*$ for any polynomial $f(x), g(x) \in F_\ell[x]$. Let C be a cyclic code of length

142 N over F_ℓ generated by $g(x)$. The annihilator of C , denoted by $\text{ann}(C)$ is the set of

143 $\text{ann}(C) = \{f(x) \in F_\ell[x] / (x^N - 1) \mid f(x) \cdot g(x) = 0\}$. Put $h(x) = \frac{x^N - 1}{g(x)}$. Clearly $\text{ann}(C)$ is

144 an ideal in $F_\ell[x] / (x^N - 1)$ generated by $h(x)$. It is well known that the dual code $C^\perp$

145 is $(\text{ann}(C))^*$ and is generated by $h^*(x)$.

146

147 Suppose that $f(x)$ is a monic polynomial of degree k with $f(0) = c \neq 0$. Then, by the

148 monic reciprocal polynomial of $f(x)$, we mean the polynomial $\tilde{f}(x) = c^{-1} f^*(x)$.

149

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

151 $M_s^*(x) = x^{|C_s|} M_s^*(1/x) = \prod_{i \in C_s} (1 - x \alpha^i) = M_s(0) \prod_{i \in C_s} (x - \alpha^{-i}) = M_s(0) M_{-s}(x)$,

152 (1)

153
$$\tilde{M}_s(x) = \frac{1}{M_s(0)} M_s^*(x) = M_{-s}(x).$$

154 (2)

155 Let C be a cyclic code of length $p^n q^m$ over F_ℓ . We have $C = \langle g(x) \rangle$. And for

156 $0 \leq i \leq n-1, 0 \leq j \leq m-1, 0 \leq k \leq d-1$, $\varepsilon_0, \varepsilon_{i,m}, \varepsilon_{n,j}, \varepsilon_{k,i,j} \in \{0,1\}$, we have

157
$$g(x) = (x-1)^{\varepsilon_0} \prod_{i=0}^{n-1} (M_{p^i q^m}(x))^{\varepsilon_{i,m}} \prod_{j=0}^{m-1} (M_{p^n q^j}(x))^{\varepsilon_{n,j}} \prod_{k=0}^{d-1} \prod_{i=0}^{n-1} \prod_{j=0}^{m-1} (M_{a^k p^i q^j}(x))^{\varepsilon_{k,i,j}} \quad (3)$$

158 Therefore,

159
$$h(x) = (x-1)^{1-\varepsilon_0} \prod_{i=0}^{n-1} (M_{p^i q^m}(x))^{1-\varepsilon_{i,m}} \prod_{j=0}^{m-1} (M_{p^n q^j}(x))^{1-\varepsilon_{n,j}} \prod_{k=0}^{d-1} \prod_{i=0}^{n-1} \prod_{j=0}^{m-1} (M_{a^k p^i q^j}(x))^{1-\varepsilon_{k,i,j}}$$

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

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

162

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

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

165

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

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

168

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

170 $S' = \{\varepsilon_0, \varepsilon_{i,m}, \varepsilon_{n,j} \mid 0 \leq i \leq n-1, 0 \leq j \leq m-1\}$

171

172 3.1 Self-orthogonal cyclic codes of length $p^n q^m$ over F_ℓ

173

174 **Theorem 2** For p, q, ℓ be distinct odd primes, $m, n \geq 1$ are integers, ℓ is a primitive root

175 both modulo p^n and q^m , $\gcd(\phi(p^n), \phi(q^m)) = d \geq 2$, $p \nmid (q-1)$, $q \nmid (p-1)$,

176 $0 \leq i \leq n-1$, $0 \leq j \leq m-1$ and $0 \leq k \leq d-1$.

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

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

179 over F_ℓ given by

$$180 \left\langle (x-1)^{\varepsilon_0} \prod_{i=0}^{n-1} (M_{p^i q^m}(x))^{\varepsilon_{i,m}} \prod_{j=0}^{m-1} (M_{p^n q^j}(x))^{\varepsilon_{n,j}} \prod_{k=0}^{d-1} \prod_{i=0}^{n-1} \prod_{j=0}^{m-1} (M_{a^k p^i q^j}(x))^{\varepsilon_{k,i,j}} \right\rangle$$

181 where $\varepsilon_0, \varepsilon_{i,m}, \varepsilon_{n,j}$ 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

182 each i, j, k ($k + \frac{d}{2}$ is modulo d).

183 *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

184 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

185 $h^*(x)$ see equation (3),(4)). This is possible if and only if $\varepsilon_s \geq 1 - \varepsilon_s$ and $\varepsilon_s \in \{0, 1\}$,

186 where $\varepsilon_s \in S$. Consequently, $\varepsilon_s = 1$. Therefore $C = 0$.

187

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

191

192 3.2 Complementary-dual cyclic codes of length $p^n q^m$ over F_ℓ

193

194 **Lemma 6**[13, Theorem] If $g(x)$ is the generator polynomial of a cyclic code C of length N
 195 over F_ℓ , then C is a complementary-dual code if and only if $g(x)$ is self-reciprocal (i.e.
 196 $\tilde{g}(x) = g(x)$) and all the monic irreducible factors of $g(x)$ have the same multiplicity in
 197 $g(x)$ and in $x^N - 1$.

198

199 **Theorem 3** For p, q, ℓ be distinct odd primes, $m, n \geq 1$ are integers, ℓ is a primitive root
 200 both modulo p^n and q^m , $\gcd(\phi(p^n), \phi(q^m)) = d \geq 2$, $p \nmid (q-1)$, $q \nmid (p-1)$,
 201 $0 \leq i \leq n-1$, $0 \leq j \leq m-1$ and $0 \leq k \leq d-1$.

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

$$204 \left\langle (x-1)^{\varepsilon_0} \prod_{i=0}^{n-1} (M_{p^i q^m}(x))^{\varepsilon_{i,m}} \prod_{j=0}^{m-1} (M_{p^n q^j}(x))^{\varepsilon_{n,j}} \prod_{k=0}^{d-1} \prod_{i=0}^{n-1} \prod_{j=0}^{m-1} (M_{a^k p^i q^j}(x))^{\varepsilon_{k,i,j}} \right\rangle,$$

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

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

$$208 \left\langle (x-1)^{\varepsilon_0} \prod_{i=0}^{n-1} (M_{p^i q^m}(x))^{\varepsilon_{i,m}} \prod_{j=0}^{m-1} (M_{p^n q^j}(x))^{\varepsilon_{n,j}} \prod_{k=0}^{d-1} \prod_{i=0}^{n-1} \prod_{j=0}^{m-1} (M_{a^k p^i q^j}(x))^{\varepsilon_{k,i,j}} \right\rangle,$$

209 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).

210 *Proof* (i) From Lemmas 3, 4, and 5, if $-C_1 = C_1$, we get $M_1(x) = M_{-1}(x)$,
 211 $M_{p^i q^m}(x) = M_{-p^i q^m}(x)$, $M_{p^n q^j}(x) = M_{-p^n q^j}(x)$, $M_{a^k p^i q^j}(x) = M_{-a^k p^i q^j}(x)$, but
 212 $\tilde{M}_s(x) = M_{-s}(x)$ (see equation (1)), where $\varepsilon_s \in S$, so $\tilde{M}_1(x) = M_1(x)$,
 213 $\tilde{M}_{p^i q^m}(x) = M_{p^i q^m}(x)$, $\tilde{M}_{p^n q^j}(x) = M_{p^n q^j}(x)$, $\tilde{M}_{a^k p^i q^j}(x) = M_{a^k p^i q^j}(x)$.

214 Then by Lemma 7, complementary-dual cyclic codes of length $p^n q^m$ over F_ℓ are

$$215 \left\langle (x-1)^{\varepsilon_0} \prod_{i=0}^{n-1} (M_{p^i q^m}(x))^{\varepsilon_{i,m}} \prod_{j=0}^{m-1} (M_{p^n q^j}(x))^{\varepsilon_{n,j}} \prod_{k=0}^{d-1} \prod_{i=0}^{n-1} \prod_{j=0}^{m-1} (M_{a^k p^i q^j}(x))^{\varepsilon_{k,i,j}} \right\rangle.$$

216

(ii) From Lemmas 4, 5 and 6, 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 7, 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).

224

225 4. AN EXAMPLE

226

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

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

229 $C_0 = \{0\}$,

$C_1 = \{1, 3, 4, 9, 11, 12, 13, 16, 17, 27, 29, 33, 36, 38, 39, 44, 46, 47, 48, 51, 52, 62, 64, 68, 71,$
 230 $73, 74, 79, 81, 82, 83, 86, 87, 97, 99, 103, 106, 108, 109, 114, 116, 117, 118, 121, 122,$
 $132, 134, 138, 141, 143, 144, 149, 151, 152, 153, 156, 157, 167, 169, 173\},$

231 $C_5 = \{5, 15, 20, 45, 55, 60, 65, 80, 85, 135, 145, 165\},$

232 $C_7 = \{7, 14, 21, 28, 42, 49, 56, 63, 77, 84, 91, 98, 112, 119, 126, 133, 147, 154, 161, 168\}$

$C_{19} = \{2, 6, 8, 18, 19, 22, 23, 24, 26, 31, 32, 34, 37, 41, 43, 53, 54, 57, 58, 59, 61, 66, 67, 69,$
 233 $72, 76, 78, 88, 89, 92, 93, 94, 96, 101, 102, 104, 107, 111, 113, 123, 124, 127, 128, 129,$
 $131, 136, 137, 139, 142, 146, 148, 158, 159, 162, 163, 164, 166, 171, 172, 174\},$

234 $C_{25} = \{25, 50, 75, 100, 125, 150\}, C_{35} = \{35, 70, 105, 140\},$

235 $C_{95} = \{10, 30, 40, 90, 95, 110, 115, 120, 130, 155, 160, 170\}.$

236

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

238 $\langle M_0(x)M_{25}(x)M_7(x)M_{35}(x)M_1(x)M_{19}(x)M_5(x)M_{95}(x) \rangle,$

239 $\langle M_0(x)M_{25}(x)M_7(x)M_{35}(x)M_1(x)M_5(x) \rangle,$

240 $\langle M_0(x)M_{25}(x)M_7(x)M_{35}(x)M_1(x)M_{95}(x) \rangle,$

241 $\langle M_0(x)M_{25}(x)M_7(x)M_{35}(x)M_{19}(x)M_5(x) \rangle,$

242 $\langle M_0(x)M_{25}(x)M_7(x)M_{35}(x)M_{19}(x)M_{95}(x) \rangle,$

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

247

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

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

250 where $\varepsilon_0, \varepsilon_{0,0,0}, \varepsilon_{0,0,1}, \varepsilon_{1,0}, \varepsilon_{0,2}, \varepsilon_{1,1} \in \{0,1\}$.

251

252 5 CONCLUSION

253

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

259

260 REFERENCES

261

- 262 1. G. Bakshi, M. Raka, Minimal cyclic codes of length $p^n q$. Finite Fields Appl. 9(2003) 432-
263 448.
- 264 2. G. Bakshi, M. Raka, A class of constacyclic codes over a finite field, Finite Fields Appl.
265 18(2012) 362-377.
- 266 3. G. Bakshi, M. Raka, Self-dual and self-orthogonal negacyclic codes of length $2p^s$ over a
267 finite field, Finite Fields Appl. 19(2013) 39-54.
- 268 4. H. Dinh, Repeated-root constacyclic codes of length $2p^s$, Finite Fields Appl. 18(2012)
269 133-143.
- 270 5. H. Dinh, Struture of repeated-root constacyclic codes of length $3p^s$ and their duals,
271 Discrete Math. 313(2013), 983-991.
- 272 6. H. Dinh, On repeated-root constacyclic codes of length $4p^s$, Asian-European Journal of
273 Math. 6(2013).
- 274 7. H. Dinh, Repeated-root cyclic and negacyclic codes of length $6p^s$, MAS Contemporary
275 Mathematics. 609(2014), 69-87.
- 276 8. B. Heijne, J. Top, On the minimal distance of binary self-dual cyclic codes, IEEE Trans.
277 Inform. Theory 55(11)(2009) 4860-4863.
- 278 9. Y. Jia, S. Ling, C. Xing, On self-dual cyclic codes over finite fields, IEEE Trans. Inform.
279 Theory 57(2011) 2243-2251.

- 280 10. X. Kai, S. Zhu, On cyclic self-dual codes, Appl. Algebra Engrg. Comm. Comput.
281 19(6)(2008) 509-525.
- 282 11. A. Sahni, P. Sehgal, Minimal cyclic codes of length $p^n q$. Finite Field Appl. 18(2012)
283 1017-1036.
- 284 12. N. Sloane, J. Thompson, Cyclic self-dual codes, IEEE Trans. Inform. Theory 29(1983)
285 364-367.
- 286 13. X. Yang, J. Massey, The condition for a cyclic code to have a complementary dual,
287 Discrete Math. 126(1994) 391-393.
- 288 14. Z.-X. Wan, A characteristic property of self-orthogonal codes and its application to
289 lattices, Bull. Belg. Math. Soc. 5 (1998), 477-482.
- 290 15. C. Gang, L. Ruihu, Construction of self-orthogonal codes with dual distance three on
291 ternary field, Computer Engineering and Application. Theory 47(2011) 38-39.
- 292 16. J.L. Massey, Linear codes with complementary duals, Discrete Math. 106/107 (1992)
293 337-342.
- 294
- 295
- 296
- 297