Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 1, pp. 63–74
DOI : 10.47974/JDMSC-1569

Minimal and maximal cyclic codes of length $2p$

Lakhdar Heboub *
Douadi Mihoubi †
Department of Mathematics
Laboratory of Pure and Applied Mathematics
M'sila University
M'sila
Algeria

Abstract

In this paper, we compute the maximal and minimal codes of length $2p$ over finite fields $\mathbb{F}_q$ with p and q are distinct odd primes and $\phi(p) = p-1$ is the multiplicative order of q modulo $2p$. We show that, every cyclic code is a direct sum of minimal cyclic codes.

Subject Classification: *[2010] 94B05, 94B15, 13A15, 94B60, 12E20.*

Keywords: *Linear and cyclic codes, Cyclotomic classes, Decomposition of ideals in semi-simple algebras.*

1. Introduction

Cyclic codes over finite fields play a very important role in the theory of error correcting codes. These codes have rich algebraic structures given the importance of the mappings that define them: the linear and cyclic mappings between a finite vectors spaces over a finite fields. Moreover, the implementation of these codes can be efficiently encoded and decoded using shift registers. It is well known that any linear cyclic code C of length n over the finite field $\mathbb{F}_q$, is an ideal C in the principal ring $\mathbb{F}_q[x]/(x^n-1)$, that is $C = \langle g(x) \rangle$ with $g(x)$ is the nonzero monic polynomial of minimal degree in C that divides the polynomial $x^n - 1$. If $x^n - 1 = g_1 ... g_t$ is the complete factorization of $x^n - 1$ into different irreducible polynomials, then the cyclic codes $\langle g_i(x) \rangle$ generated by polynomials $g_i(x)$ are called maximal

* *E-mail:* **lakhdar.heboub@univ-msila.dz (Corresponding Author)**
† *E-mail:* **douadi.mihoubi@univ-msila.dz**

cyclic codes. On the other side $(x^n-1)/g_i(x)$ is a generator polynomial of a so called minimal or irreducible code. In [14], the authors study the minimal cyclic codes of length $2p^n$. In this paper, we are interested in the computation of all maximal and minimal cyclic codes of length $2p$, where p is an odd prime, over the finite fields $\mathbb{F}_q$ of q elements, where q is an odd prime distinct from p and $\phi(p)=p-1$ (ϕ denotes Euler's phi-function), is the multiplicative order of q modulo $2p$. In the same conditions as above, we show that each maximal cyclic code can be decomposed as an unique direct sum of three minimal cyclic codes. Finally, we show that each cyclic code of length $2p$ generated by the product of two distinct minimal polynomials, is the direct sum of two minimal cyclic codes. These cases are an examples of the well known structure theorem for ideals in semisimple algebras [15]. Finally, we note that the following authors Pankaj, Manju Pruth, Sunil Kumar and Mohand Ali Mohamed have investigated in the papers [9],[10],[11] and [8] on some special classes of cyclic linear codes.

The paper is divided in three sections. The first section is devoted to the introduction of the problem studied in this paper. In the second section, we give some preliminaries useful for the paper. Finally, in the third section we give the main results obtained with illustrative examples.

2. Preliminaries

In this section, we state some useful preliminaries that are needed to derive the main results of the paper. Let $\mathbb{F}_q$ be the finite field with q elements, where $q=p^n$ for some prime p, and let n be a positive integer co-prime to q. And let $\mathbb{F}_q^n$, $n\geq 2$, be the n-dimensional vector space of the n-tuples $(a_0,a_1,a_2,...,a_{n-1})$, with the usual operations of addition of n-tuples and scalar multiplication of n-tuples by the elements of $\mathbb{F}_q$. A cyclic code C of length n over $\mathbb{F}_q$ is a linear subspace of $\mathbb{F}_q^n$ with the property that, if $(a_0,a_1,a_2,...,a_{n-1})\in C$ then the cyclic shift $(a_{n-1},a_0,a_1,...,a_{n-2})$ is also in C, i.e, the linear code C is invariant under a linear cyclic mapping called a cyclic shift. We can also regard C as an ideal in the principal quotient ring $R_n := \mathbb{F}_q[x]/(x^n-1)$.

The mapping defined by

$$(a_0,a_1,a_2,...,a_{n-1})\mapsto a_0+a_1x+\cdots+a_{n-1}x^{n-1}$$

is an isomorphism between the vectors spaces $\mathbb{F}_q^n$ and R_n.

It is known that any ideal C in R_n is generated by an unique monic polynomial $g(x)$ of the least degree in C. We can prove that the polynomial $g(x)$ is a divisor of (x^n-1), and is called the generating polynomial of the code C. The integer $k = n - \deg g(x)$ is called the dimension of the subspace C. A minimal ideal in R_n, is called an irreducible cyclic code of length n over $\mathbb{F}_q$. Again, a maximal ideal in R_n, is called a maximal cyclic code of length n over $\mathbb{F}_q$. Given the set of integers $S = \{0,1,2,...,n-1\}$. For $a,b \in S$, we say that $a \sim b$ if $a \equiv bq^i \pmod n$ for some integer $i \geq 0$. The relation $\sim$ is an equivalence relation on the set S and partitions the set S into disjoint equivalence classes called the q-cyclotomic cosets. For $s \in S$, the class of s denoted by C_s is given by $C_s := \{s, sq, sq^2, ..., sq^{n_s-1}\}$, where n_s is the smallest positive integer such that $sq^{n_s} \equiv s \pmod n$.

We recall that to factor x^n-1 over $\mathbb{F}_q$, it is necessary to find an extension of the field $\mathbb{F}_q$ which contains all the roots of the polynomial x^n-1, i.e, the polynomial x^n-1 can be factorised as $x^n-1 = \prod_{i=0}^{n-1}(x-\alpha_i)$ with α_i is n-th root of unity. In addition, if α is a primitive n-th root of unity in some extension field of $\mathbb{F}_q$ then, $x^n-1 = \prod_{i=0}^{n-1}(x-\alpha^i)$. For more information see, for example, [4], [6] and [1].

The following standard notions and definitions in cyclic codes can been seen in some famous books in coding theory. For the notion of minimal polynomial see, for example, the book of Huffman and Pless [4, section 3.7] or S. L. Chaoping Xing [2, section 3.4]. For the notions of minimal and maximal codes see, for example, J. H. Van Lint, G. Vander Geer [15, section 4] or R. Lidl, H.Niederreiter [6, chapter 8, section 2].

Definition 1 : If α is a primitive n-th root of unity in some extension field of $\mathbb{F}_q$., then the polynomial $m_s(x) = \prod_{j \in C_s}(x-\alpha^j)$ is called the minimal polynomial of α^s over $\mathbb{F}_q$.

The $x^n-1 = \prod_s m_s(x)$ gives the factorization of x^n-1 into irreducible factors over $\mathbb{F}_q$, where s runs over the complete set of representatives from distinct q-cyclotomic cosets modulo n.

Definition 2 : The cyclic code $\widehat{m_s}$ in R_n generated by $\frac{(x^n-1)}{m_s(x)}$ is called a minimal cyclic code of length n over $\mathbb{F}_q$. Minimal cyclic codes are also called irreducible cyclic codes.

Definition 3 : The cyclic code M_s in R_n, generated by $m_s(x)$, is called a maximal cyclic code of length n over $\mathbb{F}_q$.

3. Determination of minimal and maximal cyclic codes of length $2p$ with p is an odd prime

In the paper [14], the authors investigated in the computation of the minimal cyclic codes of length and $2p^n$ with $n \geq 1$ is an integer, over the finite fields $\mathbb{F}_q$ where q is a power of an odd prime number and $\gcd(p,q)=1$. The authors obtains $2n+2$ q-cyclotomic cosets modulo $2p^n$. In this paper, we determine in the special case $n=1$ and q is an odd prime, the minimal cyclic codes and the maximal cyclic codes of length $2p$ over $\mathbb{F}_q$, with $\phi(p)=p-1$ is the multiplicative order of q modulo $2p$.

Proposition 4 : Given the set of integers $S=\{0,1,2,...,2p-1\}$ and $\phi(p)$ is the multiplicative order of q modulo $2p$. Then S, can be partitioned into 4 q-cyclotomic cosets given by, $C_0 := \{0\}, C_p := \{p\}$, $C_1 := \{1,\ q,\ q^2,...,q^{p-2}\}$, $C_2 := \{2,\ 2q,\ 2q^2,...,2q^{p-2}\}$.

Proof : For $s \in S$, the class of s denoted by C_s is given by

$C_s := \{s, sq, sq^2,..., sq^{n_s-1}\}$ modulo $2p$.

For $s=0$, we have $C_0 = \{0,\ 0q,\ 0q^2,\ ...,\ 0q^{n_s-1}\} = \{0\}$. And for $s=1$, we will show that we have $C_1 := \{1,\ 1\times q,\ 1\times q^2,\ ...,\ 1\times q^{n_s-1}\} = \{1,\ q,\ q^2,...,q^{p-2}\}$ with $n_s = p-1$. Suppose in the contrary, there is an integers i, j with $0 \leq i < j \leq p-2$ and $q^i = q^j$. Multiplying both sides by q^{-j}, we obtain $q^i q^{-j} (\mathrm{mod}\, 2p) \equiv q^j q^{-j} (\mathrm{mod}\, 2p) \equiv q^0 (\mathrm{mod}\, 2p) \equiv 1 (\mathrm{mod}\, 2p)$. But we have $1 \leq j-i \leq p-2$ and this contradict the fact that the order of q is $p-1$ modulo $2p$. Then necessary, $q^i \neq q^j$ for all $i, j \in \{1,2,...,p-2\}$ with $i \neq j$. Since, the integer 2 is not in the classes C_0 and C_1 then $C_2 := \{2,\ 2q,\ 2q^2,...,2q^{p-2}\}$. The same argument as above, shows that we have $2q^i \neq 2q^j$ for all $i, j \in \{1,2,...,p-2\}$ with $i \neq j$. Since the prime p is an odd prime then p is not in the classes C_0, C_1, C_2; then we have $C_p := \{p,\ pq,\ pq^2,\ ...,\ pq^{n_s-1}\}$ $= \{p\}$ modulo $2p$. Firstly, $p \equiv p (\mathrm{mod}\, 2p)$ because $p < 2p$ then $p \in C_p$. We have also, $pq \equiv p (\mathrm{mod}\, 2p)$ because q is an odd prime great or equal to 3, and in this case we can write $q = 2t+1$ and consequently, we have $pq = p(2t+1) = 2pt + p \equiv p (\mathrm{mod}\, 2p)$. The same argument holds for pq^i, i.e, $pq^i \equiv p (\mathrm{mod}\, 2p)$. Since $|C_0| = |C_p| = 1$ and $|C_1| = |C_2| = p-1$, then we have

$$|C_0 \cup C_1 \cup C_2 \cup C_p| = |C_0| + |C_1| + |C_2| + |C_p| = 1+1+(p-1)+(p-1) = 2p,$$

which is the cardinal of S. And this confirms that we have:

$$C_0 \cup C_1 \cup C_2 \cup C_p = S.$$

Theorem 5 : *The number of monic irreducible factors of* $x^{2p}-1$ *over* $\mathbb{F}_q$ *is equal to the number of cyclotomic cosets of q modulo* $2p$.

With Proof: Ref. [2].

In this section, we consider the complete factorization of $x^{2p}-1$ over $\mathbb{F}_q$, with p and q are distinct odd primes and $\phi(p)=p-1$ is the multiplicative order of q modulo $2p$.

The unique complete factorization of $x^{2p}-1$ over $\mathbb{F}_q$ into irreducible polynomials is $x^{2p}-1=\prod m_s(x)$, where s runs over the complete set of representatives from distinct q-cyclotomic cosets modulo $2p$.

Since $x^{2p}-1=(x^p-1)(x^p+1)$. And we have:

$$(x^p-1)=(x-1)(x^{p-1}+x^{p-2}+\ldots+x+1)(x+1)$$

and $(x^p+1)=(x+1)(x^{p-1}-x^{p-2}+\ldots-x+1)$. Then,

$$x^{2p}-1=(x-1)(x^{p-1}+x^{p-2}+\ldots+x+1)(x+1)(x^{p-1}-x^{p-2}+\ldots-x+1)$$

$$=(x-1)(x+1)(x^{p-1}-x^{p-2}+\ldots-x+1)(x^{p-1}+x^{p-2}+\ldots+x+1)$$

The polynomials $x^{p-1}+x^{p-2}+\ldots+x+1$, $x^{p-1}+x^{p-2}+\ldots+x+1$ are shown to be irreducible in $\mathbb{F}_q$, with q is an odd prime and $\phi(p)=p-1$ is the multiplicative order of i modulo $2p$, see [3], [5] or [7].

The minimal polynomials corresponding to each cyclotomic coset are obtained below:

$m_0(x)=x-1,$
$m_p(x)=x+1,$
$m_1(x)=x^{p-1}-x^{p-2}+\ldots-x+1,$
$m_2(x)=x^{p-1}+x^{p-2}+\ldots+x+1.$
And we have: $x^{2p}-1=\prod_{s\in\{0,1,2,p\}} m_s(x).$

Since the classes C_0, C_p, C_1, C_2 are all the distinct q-cyclotomic cosets modulo $2p$, then $M_0=\langle m_0(x)\rangle$, $M_p=\langle m_p(x)\rangle$, $M_1=\langle m_1(x)\rangle$, $M_2=\langle m_2(x)\rangle$ are precisely all the distinct maximal cyclic codes of length $2p$ over $\mathbb{F}_q$. And we have $\widehat{m_0}=\langle\frac{(x^{2p}-1)}{m_0(x)}\rangle$, $\widehat{m_p}=\langle\frac{(x^{2p}-1)}{m_p(x)}\rangle$, $\widehat{m_1}=\langle\frac{(x^{2p}-1)}{m_1(x)}\rangle$, $\widehat{m_2}=\langle\frac{(x^{2p}-1)}{m_2(x)}\rangle$, are precisely all the distinct minimal cyclic codes of length $2p$ over $\mathbb{F}_q$. See [6], for the definitions of minimal and maximal cyclic

codes. The following tables 1 & 2 give the generating polynomial and the corresponding dimension of the above maximal and minimal codes.

Table 1
The maximal codes of length $2p$ over $\mathbb{F}_q$

Codes	Generating polynomial	Dimension
M_0	$m_0(x)$	$2p-1$
M_p	$m_p(x)$	$2p-1$
M_1	$m_1(x)$	$p+1$
M_2	$m_2(x)$	$p+1$

Table 2
The minimal codes of length $2p$ over $\mathbb{F}_q$

Codes	Generating polynomial	Dimension
$\widehat{m_0} = \langle \frac{(x^n-1)}{m_0(x)} \rangle$	$m_p(x) \times m_1(x) \times m_2(x)$	1
$\widehat{m_p} = \langle \frac{(x^n-1)}{m_p(x)} \rangle$	$m_0(x) \times m_1(x) \times m_2(x)$	1
$\widehat{m_1} = \langle \frac{(x^n-1)}{m_1(x)} \rangle$	$m_0(x) \times m_p(x) \times m_2(x)$	$p-1$
$\widehat{m_2} = \langle \frac{(x^n-1)}{m_2(x)} \rangle$	$m_0(x) \times m_p(x) \times m_1(x)$	$p-1$

3.1 *The relationship between the maximal cyclic codes and the minimal cyclic codes*

In this section, we show that every maximal cyclic code of length $2p$ over $\mathbb{F}_q$, with p and q are distinct odd primes and $\phi(p) = p-1$ is the multiplicative order of q modulo $2p$, can be written as an unique direct sum of three minimal cyclic codes. Finally, we show that each cyclic code of length $2p$ generated by the product of two distinct minimal polynomials, is the direct sum of two minimal cyclic codes.

Proposition 6 : As any cyclic code of length n over the finite field $\mathbb{F}_q$ is simply a subspace of the vector space $\mathbb{F}_q^n$, we have : if C_1 and C_2 are cyclic codes of length n over $\mathbb{F}_q$, then sum $C_1 + C_2 = \{c_1 + c_2 \mid c_2 \in C_1 \text{ and } c_2 \in C_2\}$ and the intersection $C_1 \cap C_2$ are also a cyclic codes.

Proposition 7 : Let C_i be a cyclic code of length n over $\mathbb{F}_q$ for $i = 1$ and 2. Then the sum $C_1 + C_2$ is direct, if and only if $C_1 \cap C_2 = \{0\}$.

The dimension of the cyclic code C is the dimension of C as a vector space over $\mathbb{F}_q$.

Proposition 8 : Let C_i be a cyclic code of length n over $\mathbb{F}_q$ for $i \in \{1, 2, 3\}$. Then $C_1 + C_2 + C_3$ is a direct sum if and only if

$$\dim(C_1 + C_2 + C_3) = \dim(C_1) + \dim(C_2) + \dim(C_3).$$

Theorem 9 : *Let C_i be a cyclic code of length n over $\mathbb{F}_q$ with generator polynomial $g_i(x)$ for $i = 1$ and 2. Then*

(i) *The cyclic code $C_1 \cap C_2$ has generator polynomial $lcm(g_1(x), g_2(x))$, and*

(ii) *The cyclic code $C_1 + C_2$ has generator polynomial $\gcd(g_1(x), g_2(x))$.*

Proof: For the proof see [4]. □

Now we prove our main results.

Proposition 10 : Every maximal cyclic code of length $2p$ over $\mathbb{F}_q$, is a direct sum of three minimal cyclic codes with p and q are distinct odd primes and $\phi(p) = p - 1$ is the multiplicative order of q modulo $2p$.

Proof: Using the theorem 9 and properties of gcd of polynomials, we find:

$$\widehat{m_0} + \widehat{m_p} + \widehat{m_1} =$$

$$\left\langle \gcd \begin{pmatrix} m_p(x) \times m_1(x) \times m_2(x), m_0(x) \times m_1(x) \times m_2(x), \\ m_0(x) \times m_p(x) \times m_2(x) \end{pmatrix} \right\rangle$$

$$= \left\langle \gcd \begin{pmatrix} \gcd\left(m_p(x) \times m_1(x) \times m_2(x), m_0(x) \times m_1(x) \times m_2(x)\right), \\ m_0(x) \times m_p(x) \times m_2(x) \end{pmatrix} \right\rangle$$

$$= \langle \gcd(m_1(x) \times m_2(x), m_0(x) \times m_p(x) \times m_2(x)) \rangle$$

$$= \langle m_2(x) \times \gcd(m_1(x), m_0(x) \times m_p(x)) \rangle$$

$$= \langle m_2(x) \rangle$$

Also, using proposition 8 we find:

$$\dim(\widehat{m_0}+\widehat{m_p}+\widehat{m_1})=\dim(\langle m_2(x)\rangle)=p+1=\dim(\widehat{m_0})+\dim(\widehat{m_p})+\dim(\widehat{m_1}).$$

then $M_2=\widehat{m_0}\oplus\widehat{m_p}\oplus\widehat{m_1}$.

In a similar way, we find:

$$\widehat{m_0}+\widehat{m_p}+\widehat{m_2}=$$

$$\left\langle \gcd\begin{pmatrix} m_p(x)\times m_1(x)\times m_2(x), m_0(x)\times m_1(x)\times m_2(x), \\ m_0(x)\times m_p(x)\times m_1(x)\end{pmatrix}\right\rangle$$

$$=\left\langle \gcd\begin{pmatrix} \gcd\left(m_p(x)\times m_1(x)\times m_2(x), m_0(x)\times m_1(x)\times m_2(x)\right), \\ m_0(x)\times m_p(x)\times m_1(x)\end{pmatrix}\right\rangle$$

$$=\langle \gcd(m_1(x)\times m_2(x), m_0(x)\times m_p(x)\times m_1(x))\rangle$$

$$=\langle m_1(x)\times \gcd(m_2(x), m_0(x)\times m_p(x))\rangle\ \rangle$$

$$=\langle m_1(x)\rangle.$$

$$\dim(\widehat{m_0}+\widehat{m_p}+\widehat{m_2})=\dim(\langle m_1(x)\rangle)=p+1=\dim(\widehat{m_0})+\dim(\widehat{m_p})+\dim(\widehat{m_2}).$$

$$M_1=\widehat{m_0}\oplus\widehat{m_p}\oplus\widehat{m_2}.$$

$$\widehat{m_0}+\widehat{m_1}+\widehat{m_2}=\left\langle \gcd\begin{pmatrix} m_p(x)\times m_1(x)\times m_2(x), m_0(x)\times m_p(x)\times m_2(x), \\ m_0(x)\times m_p(x)\times m_1(x)\end{pmatrix}\right\rangle$$

$$=\left\langle \gcd\begin{pmatrix} \gcd(m_p(x)\times m_1(x)\times m_2(x), m_0(x)\times m_p(x)\times m_2(x)), \\ m_0(x)\times m_p(x)\times m_1(x)\end{pmatrix}\right\rangle$$

$$=\langle \gcd(m_p(x)\times m_2(x), m_0(x)\times m_p(x)\times m_1(x))\rangle$$

$$=\langle m_p(x)\times\ \gcd(m_2(x), m_0(x)\times m_1(x))\rangle$$

$= \langle m_p(x) \rangle.$

$$\dim(\widehat{m_0} + \widehat{m_1} + \widehat{m_2}) = \dim(\langle m_p(x) \rangle) = 2p-1 = \dim(\widehat{m_0}) + \dim(\widehat{m_1}) + \dim(\widehat{m_2})).$$

$$M_p = \widehat{m_0} \oplus \widehat{m_1} \oplus \widehat{m_2}.$$

$$\widehat{m_p} + \widehat{m_1} + \widehat{m_2} = \left\langle \gcd \begin{pmatrix} m_0(x) \times m_1(x) \times m_2(x), m_0(x) \times m_p(x) \times m_2(x), \\ m_0(x) \times m_p(x) \times m_1(x) \end{pmatrix} \right\rangle$$

$$= \left\langle \gcd \begin{pmatrix} \gcd(m_0(x) \times m_1(x) \times m_2(x), m_0(x) \times m_p(x) \times m_2(x)), \\ m_0(x) \times m_p(x) \times m_1(x) \end{pmatrix} \right\rangle$$

$$= \langle \gcd(m_0(x) \times m_2(x), m_0(x) \times m_p(x) \times m_1(x))$$

$$= \langle m_0(x) \times \gcd(m_2(x), m_p(x) \times m_1(x)) \rangle$$

$$= \langle m_0(x) \rangle.$$

$$\dim(\widehat{m_p} + \widehat{m_1} + \widehat{m_2}) = \dim(\langle m_0(x) \rangle) = 2p-1 = \dim(\widehat{m_p}) + \dim(\widehat{m_1}) + \dim(\widehat{m_2})).$$

$$M_0 = \widehat{m_p} \oplus \widehat{m_1} \oplus \widehat{m_2}.$$

□

Proposition 11 : Every cyclic code of length $2p$ over $\mathbb{F}_q$ generated by product of two minimal polynomials is a direct sum of two minimal cyclic codes with p and q are distinct odd primes and $\phi(p) = p-1$ is the multiplicative order of q modulo $2p$.

Proof: Using the theorem 9 and properties of $\gcd$ we find:

$$\widehat{m_0} + \widehat{m_p} = \langle \gcd(m_p(x) \times m_1(x) \times m_2(x), m_0(x) \times m_1(x) \times m_2(x)) \rangle$$

$$= \langle m_1(x) \times m_2(x) \gcd(m_p(x), m_0(x)) \rangle$$

$$= \langle m_1(x) \times m_2(x) \rangle.$$

Also, using proposition 7 and properties of of lcm we find:

$$\widehat{m_0} \cap \widehat{m_p} = \langle lcm(m_p(x) \times m_1(x) \times m_2(x), m_0(x) \times m_1(x) \times m_2(x)) \rangle$$

$$= \langle m_0(x) \times m_p(x) \times m_1(x) \times m_2(x) \rangle$$

$$= \langle x^{2p} - 1 \rangle = \{0\}.$$

so $\langle m_1(x) \times m_2(x) \rangle = \widehat{m_0} \oplus \widehat{m_p}$.

In a similar way, we find: $\langle m_p(x) \times m_2(x) \rangle = \widehat{m_0} \oplus \widehat{m_{1,}}$

$$\langle m_p(x) \times m_1(x) \rangle = \widehat{m_0} \oplus \widehat{m_2},$$

$$\langle m_0(x) \times m_2(x) \rangle = \widehat{m_p} \oplus \widehat{m_1},$$

$$\langle m_0(x) \times m_1(x) \rangle = \widehat{m_p} \oplus \widehat{m_2},$$

$$\langle m_0(x) \times m_p(x) \rangle = \widehat{m_1} \oplus \widehat{m_2}.$$ □

Example 12 : Take $q = 3$, $p = 17$ and $n = 1$. The maximal ternary cyclic codes M_0, M_p, M_1, M_2 of length 34 and The minimal ternary cyclic codes

$\widehat{m_0}$, $\widehat{m_p}$, $\widehat{m_1}$, $\widehat{m_2}$ of length 34 have the following parameters: (a) The minimal polynomial corresponding to each cyclotomic coset is obtained below:

$$m_0(x) = x - 1, \; m_{17}(x) = x + 1,$$

$$m_1(x) = x^{17} - x^{16} + x^{15} - x^{14} + x^{13} - x^{12} + x^{11} - x^{10} + x^9 - x^8 + x^7$$
$$-x^6 + x^5 - x^4 + x^3 - x^2 + x + 1,$$
$$m_2(x) = x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8$$
$$+x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

(b) If $g_s(x)$ is the generating polynomial of $\widehat{m_s}$ then we have

$$g_0(x)=\frac{(x^{34}-1)}{m_0(x)}=x^{33}+x^{32}+x^{31}+x^{30}+x^{29}+x^{28}+x^{27}+x^{26}+x^{25}+x^{24}$$
$$+x^{23}+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}$$
$$+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1,$$
$$g_{17}(x)=\frac{(x^{34}-1)}{m_{17}(x)}=x^{33}-x^{32}+x^{31}-x^{30}+x^{29}-x^{28}+x^{27}-x^{26}+x^{25}-x^{24}$$
$$+x^{23}-x^{22}+x^{21}-x^{20}+x^{19}-x^{18}+x^{17}-x^{16}+x^{15}-x^{14}+x^{13}-x^{12}+x^{11}$$
$$-x^{10}+x^9-x^8+x^7-x^6+x^5-x^4+x^3-x^2+x+1,$$
$$g_1(x)=\frac{(x^{34}-1)}{m_1(x)}=x^{18}+x^{17}-x-1,$$
$$g_2(x)=\frac{(x^{34}-1)}{m_2(x)}=x^{18}-x^{17}+x-1.$$

(c) The generating polynomial and dimension of the maximal ternary cyclic codes of length 34 are given by:

Table 3

Codes	M_0	M_{17}	M_1	M_2
Generating polynomial	$m_0(x)$	$m_{17}(x)$	$m_1(x)$	$m_2(x)$
Dimension	33	33	18	18

d) The generating polynomial and dimension of the minimal ternary cyclic codes of length 34 are given as:

Table 4

Codes	$\widehat{m_0}$	$\widehat{m_p}$	$\widehat{m_1}$	$\widehat{m_2}$
Generating polynomial	$g_0(x)$	$g_{17}(x)$	$g_1(x)$	$g_2(x)$
Dimension	1	1	16	16

References

[1] S. Batra, S.K. Arora, Some cyclic codes of length $2p^n$. *Des. Codes Cryptogr.* 61(1), 41–69 (2011).

[2] S.L, Chaoping.xing, Coding Theory, A First Course, Cambridge University Press,2004.

[3] K. Conrad, Cyclotomic extension, http://www.math.uconn.edu/ kconrad /math5211s13/handouts/ cyclotomic.pdf.

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

[5] N. Jacobson, Lectures in abstract algebra, vol. III, D. Van Nostrand Company, Inc. Princeton, 1964.

[6] R. Lidl, H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, 1997.

[7] C. Mihoubi, P. Solé, New class of isodual cyclic codes of rate $1/2$ over $\mathbb{F}_p$, *Romanian Journal of Mathematics and Computer Science.* 6(1), 1–5 (2016).

[8] M. Ali. Mohammed, A . J. munshid, M Alaeiyan (2021) Cyclic codes of length p^n over $(\mathbb{Z}p)^m$, *Journal of Discrete Mathematical Sciences and Cryptography,* 24:2, 579-588, DOI: 10.1080/09720529.2021.1891693..

[9] Pankaj, M. Pruthi, (2017) Cyclic codes from Whiteman's generalized cyclotomic sequences of order 2^r, $r \geq 2$, *Journal of Information and Optimization Sciences,* 38 : 3-4, 621-646, DOI: 10.1080/02522667.2017.1303948.

[10] Pankaj, M. Pruthi, (2018) Cyclic codes of prime power length from generalized cyclotomic classes of order 2^r, *Journal of Information and Optimization Sciences,* 39:4, 965-971, DOI: 10.1080/02522667. 2018.1460136.

[11] M. Pruthi, S Kumar (2019) Cyclic codes with generalized cyclotomic cubic classes, *Journal of Discrete Mathematical Sciences and Cryptography,* 22:6, 923-933, DOI: 10.1080/09720529.2019.1627706.

[12] V. Pless, Introduction to the Theory of Error Correcting Codes. Wiley, New York, 1998.

[13] M. Pruthi, S.K. Arora, Minimal cyclic codes of prime power length, Finite Fields Appl. 3 (1997) 99–113.

[14] M. Pruthi, S.K. Arora, Minimal cyclic codes of length $2p^n$; Finite Fields Appl. 5 (2) (1999) 177–187.

[15] J, H. van Lint, G. van der Geer, Introduction to Coding Theory and algebraic geometry., Birkhäuser Verlag, Basel, 1988.

Received July, 2021

Revised January, 2022