ISSN: 2692-5079

# Notes about the linear complexity of cyclotomic binary sequences of order four over a finite field of odd characteristic

Vladimir Edemskiy
*Department of Applied Mathematics and Information Science*
*Novgorod State University*
Veliky Novgorod, Russia
Vladimir.Edemsky@novsu.ru

Nikita Sokolovskii
*Department of Applied Mathematics and Information Science*
*Novgorod State University*
Veliky Novgorod, Russia
sokolovskiy.nikita@gmail.com

***Abstract*—In this paper, we investigate the linear complexity and the minimal polynomial of cyclotomic binary sequences of order four over a finite field of odd characteristic. The sequences considered are determined on the basis of two cyclotomic classes of the fourth order. We show that they have a high linear complexity.**

***Index Terms*—binary sequences, linear complexity, cyclotomy**

## I. Introduction

Binary sequences are widely used in various fields, in particular, in cryptography [2]. The linear complexity is an important characteristic of pseudo-random sequence for cryptographic applications. Let $s$ be a sequence with period $n$ over a finite field $GF(q)$, where $q$ is a prime number. The linear complexity of $s$ over $GF(q)$ is defined to be the smallest positive integer $L$ such that there are constants $c_0 \neq 0, c_1, \dots, c_L \in GF(q)$ satisfying

$$-c_0 s_i = c_1 s_{i-1} + c_2 s_{i-2} + \dots + c_L s_{i-L} \text{ for all } i \geq L.$$

Polynomial $m(x) = c_0 + c_1 x + \dots + c_{L-1}x^{L-1} + c_L x^L$ is called the minimal polynomial of $s$ [2].

From the engineering point of view, $L$ is the length of the shortest linear feedback shift register generating the sequence. As the Berlekamp - Massey algorithm is capable of deducing the whole sequence from a knowledge of just $2L$ consecutive digits, a high linear complexity $L$ should be no less than one half of the length (or minimum period) of the sequence.

Using classical cyclotomic and generalized cyclotomic classes to construct binary and other sequences, which are called cyclotomic and generalized sequences, is an important method for sequence design [2]. There are many works devoted to the study of the linear complexity of above-mentioned binary sequences over the finite field of order two. In particular, the sequences determined by two cyclotomic classes of the fourth order in [3], [6]. Recently, a number of papers have been published on the analysis of the linear complexity of cyclotomic sequences over an arbitrary finite field. So the characteristic sequences of quadratic, cubic and biquadratic residue classes that belong to cyclotomic classes were investigated in [4], [7], [11]–[13], two classes of biquadratic residues in [5], but with constraints on the period of the sequence and the characteristic of the finite field. As noted in [5], further investigation of this topic is also of interest (Problem 7.1).

In this paper, the linear complexity and minimal polynomials of the characteristic sequence of two fourth-order cyclotomic classes are investigated over an arbitrary finite field without restrictions on the period and the characteristic of the field.

## II. Preliminaries

First, we briefly repeat the basic definitions from [5].

Let $n$ be a prime such that $n \equiv 1 (\text{mod } 4)$, and $g$ be a primitive root modulo $n$ [9]. Define $C_i^{(4,n)} = g^i \langle g^4 \rangle$ for $i = 0, 1, 2, 3$, where $\langle g^4 \rangle$ is the subgroup of $GF^*(n)$ generated by $g^4$. The cosets $C_i^{(4,n)}$ are called the cyclotomic classes of order $4$ in $GF(n)$ [2].

Consider the binary sequence $s$ of a period $n$ defined as follows:

$$s_i = \begin{cases} 1, & \text{if } i \pmod{n} \in C_0^{(4,n)} \cup C_1^{(4,n)}, \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

The linear complexity and the minimal polynomial of this sequence were studied in [3], [6] for $q = 2$, [1] for $q = n$ and [5] for finite fields of other orders. In the last work, the sequence study was performed under the condition that $(n-1)/4 \equiv 0 \pmod{q}$, where $q$ is a characteristic of a finite field. So, in this paper we will investigate the linear complexity and the minimal polynomial of the sequence $s$ over the finite field $GF(q)$ for $q > 2$ and $(n-1)/4 \not\equiv 0 \pmod{q}$. For $q > 2$ the congruence means that $n \not\equiv 1 \pmod{q}$.

V. Edemskiy and N. Sokolovskii were supported by RFBR-NSFC according to the research project No. 19-55-53003.

It is well known that the linear complexity $L$ of a sequence $s$ and its minimal polynomial $m\left(x\right)$ can be calculated by the following formulas [2]:

$$L = n - \deg\left[\,(x^n - 1, S(x))\right],$$
$$m(x) = (x^n - 1)/\left(x^n - 1, S\left(x\right)\right), \quad (2)$$

where $S\left(x\right) = s_0 + s_1 x + \ldots + s_{n-1}x^{n-1}$.

Denote by $\mathrm{ord}_n(q)$ the multiplicative order $q$ modulo $n$, and by $\eta$ a primitive root of the $n$th degree of unity in the field $GF(q^{\mathrm{ord}_n(q)})$ [10]. Then, according to (2), we obtain that

$$L = n - \left|\left\{j \mid S\left(\eta^j\right) = 0,\ j = 0, 1, \ldots, n-1\right\}\right|. \quad (3)$$

Let $\eta_i = \sum_{j \in C_i^{(4,n)}} \eta^j, \quad i = 0, 1, 2, 3$ and $\theta_i = \eta_i + \eta_{i+2}, i = 0, 1$, i.e., $\theta_i = \sum_{j \in C_i^{(2,n)}} \eta^j$. The values $\eta_i$ depend on choice $g, \eta$. Here and hereafter the subscript of $\eta$ is performed modulo 4. Notice that

$$\eta_0 + \eta_1 + \eta_2 + \eta_3 = -1. \quad (4)$$

Further, by definition of the sequence we have $S\left(\eta^v\right) = \sum_{j \in C_0^{(4,n)} \cup\ C_1^{(4,n)}} \eta^{vj}$. Using the properties of $S(x)$ and the definition of $\eta_i$ from [5], we obtain that $S(\eta^j) = S(\eta^{g^i})$ for $j \in C_i^{(4,n)}$ and

$$S\left(\eta^j\right) = \eta_i + \eta_{i+1} \quad (5)$$

Thus, by the formula (3) we have that

$$L = n - |\{i \mid \ \ \eta_i + \eta_{i+1} = 0, \ \ i = 0, 1, 2, 3\}|(n-1)/4 - \Delta, \quad (6)$$

where

$$\Delta = \begin{cases} 1, & \text{if} \quad S(1) = 0, \\ 0, & \text{if} \quad S(1) \neq 0. \end{cases}$$

We introduce auxiliary polynomials $\Omega_i^{(4,n)}\left(x\right) = \prod_{j \in C_i^{(4,n)}} \left(x - \eta^j\right)$ for $i\ :\ 0 \leq i \leq 3$. By definition of cyclotomic classes and the choice of $\eta$ we have the decomposition:

$$x^n - 1 = (x-1)\prod_{i=0}^{3} \Omega_i^{(4,n)}(x).$$

Then by (2) the minimal polynomial of the sequence $s$ is

$$m(x) = (x-1)^{1-\Delta} \prod_{i\,:\ \ \eta_i + \eta_{i+1} \neq 0} \Omega_i^{(4,n)}(x). \quad (7)$$

It is easy to check that $\Omega_i^{(4,n)}(x) \in GF(q)[x]$, if $\eta_i \in GF(q)$ for $i = 0, 1, 2, 3$.

Thus, according to formulas (6) and (7), to calculate the linear complexity and the minimal polynomial of the sequence, it is sufficient to determine when $S\left(\eta^{g^i}\right) = \eta_i + \eta_{i+1} = 0$ for $i : 0 \leq i \leq 3$.

## III. Auxiliary lemmas.

In this section we prove several auxiliary statements necessary for what follows.

Since $n \equiv 1 (\mathrm{mod}\ 4)$, $n$ can be expressed as $n = u^2 + 4v^2$; $u \equiv 1(\bmod\ 4)$, here $v$ is two-valued, depending on the choice of the primitive root.

The following statements follow from [5], [12] (the formulae (6.14), (6.19), etc.).

*Lemma 1:*

Let $n = u^2 + 4v^2$. Then:

(i) $\theta_0$ and $\theta_1$ are the roots of the polynomial

$$x^2 + x - (n-1)/4.$$

(ii) When $n \equiv 5 \pmod 8$ we have $\eta_i$ and $\eta_{i+2}$ are the roots of the polynomial

$$x^2 - \theta_i x + \theta_i(u-1)/4 + (3n - 1 + 2u)/16.$$

(iii) When $n \equiv 1 \pmod 8$ we have $\eta_i$ and $\eta_{i+2}$ are the roots of the polynomial

$$x^2 - \theta_i x + \theta_i(u-1)/4 - (n + 1 - 2u)/16.$$

The following lemma defines the necessary and sufficient conditions for the existence of the root of $S(x)$ in the set $\{\eta^j, \ \ j = 1, 2, \ldots, n-1\}$.

*Lemma 2:* Let $n = u^2 + 4v^2$. Then there exists $j \neq 0$ such that $S(\eta^j) = 0$ if and only if

$$u^2 n + 2n + 1 \equiv \begin{cases} 0, & \text{if } n \equiv 5 \pmod 8, \\ 4n, & \text{if } n \equiv 1 \pmod 8. \end{cases} \pmod q.$$

*Proof:* Let $n \equiv 5 \pmod 8$ and $S(\eta^j) = 0, 0 < j < n$. Without loss of generality, we can assume that $S(\eta) = 0$. Then by (5) we see $\eta_0 = -\eta_1$ and by Lemma 1 we get

$$\begin{cases} \eta_0^2 - \theta_0\eta_0 + \theta_0(u-1)/4 + (3n - 1 + 2u)/16 = 0, \\ \eta_0^2 + \theta_1\eta_0 + \theta_1(u-1)/4 + (3n - 1 + 2u)/16 = 0. \end{cases}$$

Hence $\eta_0 = -(u-1)/4 - \theta_0(u-1)/2$. Denote $(u-1)/4$ by $t$. Then $\eta_0 = -t - 2\theta_0 t$ and

$$(4t^2 + 2t)\theta_0^2 + (4t^2 + 2t)\theta_0 + (3n + u^2)/16 = 0.$$

By Lemma 1 we see that

$$(4t^2 + 2t)\theta_0^2 + (4t^2 + 2t)\theta_0 - (4t^2 + 2t)(n-1)/4 = 0.$$

Therefore,

$$(3n{+}u^2)/4 = -(4t^2{+}2t)(n{-}1) \text{ or } 3n{+}u^2 = -(u^2{-}1)(n{-}1),$$

i.e., $u^2 n + 2n + 1 \equiv 0 \pmod q$.

Let $u^2 n + 2n + 1 \equiv 0 \pmod q$ and $y = -t - 2\theta_0 t$. It is straightforward to verify that $y$ is a root of $x^2 - \theta_0 x + \theta_0(u-1)/4 + (3n - 1 + 2u)/16$ and $-y$ is a root of $x^2 - \theta_1 x + \theta_1(u-1)/4 + (3n - 1 + 2u)/16$. The conclusion of this lemma then follows from Lemma 1 and (5).

The second statement of this lemma may be proved similarly as the first. ■

*Corollary 3:* Let $n \equiv 5 \pmod 8$ and $u^2n + 2n + 1 \equiv 0 \pmod q$ or $n \equiv 1 \pmod 8$ and $u^2n - 2n + 1 \equiv 0 \pmod q$. Then

$$\eta_0, \eta_2 \in \{-\frac{u-1}{4} - \frac{u-1}{2}\theta_0, \frac{u-1}{4} + \frac{u+1}{2}\theta_0\},$$

and

$$\eta_1, \eta_3 \in \{\frac{u-1}{4} + \frac{u-1}{2}\theta_0, -\frac{u+3}{4} - \frac{u+1}{2}\theta_0\}.$$

We note that in the proof of the Lemma 2 the condition $n \not\equiv 1 \pmod q$ for $q > 2$ was not used, that is, the statement of Lemma 2 is fair for $n \equiv 1 \pmod q$. In this case we get that $u^2 \equiv -3 \pmod q$ for $n \equiv 5 \pmod 8$ and $u^2 \equiv 1 \pmod q$ for $n \equiv 1 \pmod q$, that agrees with the Theorem 7.1 from [5].

## IV. The linear complexity of sequence

Let us prove the main result of the article.

*Theorem 4:* Let $s$ be defined by (V) and $(n-1)/4 \not\equiv 0 \pmod q$, $q > 2$, and let $n = u^2 + 4v^2$ with $u \equiv 1 \pmod 4$. Then the linear complexity and the minimal polynomial of $s$ are defined by the following relations:

(a) The case that $n \equiv 5 \pmod 8$:

1) When $u^2n + 2n + 1 \not\equiv 0 \pmod q$, we have $L = n$ and $m(x) = x^n - 1$.
2) When $u^2n+2n+1 \equiv 0 \pmod q$ and $n \not\equiv -1 \pmod q$, we have $L = (3n+1)/4$ and

$$m(x) = \begin{cases} (x^n-1)/\Omega_0^{(4,n)}(x), & \text{if} \quad \eta_0 = -\eta_1, \\ (x^n-1)/\Omega_1^{(4,n)}(x), & \text{if} \quad \eta_1 = -\eta_2, \\ (x^n-1)/\Omega_2^{(4,n)}(x), & \text{if} \quad \eta_2 = -\eta_3, \\ (x^n-1)/\Omega_3^{(4,n)}(x), & \text{if} \quad \eta_0 = -\eta_3. \end{cases}$$

3) When $n \equiv -1 \pmod q$ and $u^2 \equiv -1 \pmod q$ , we have $L = (n+1)/2$ and

$$m(x) = \begin{cases} (x-1)\Omega_0^{(4,n)}(x)\Omega_1^{(4,n)}(x), \\ \qquad \text{if} \quad \eta_0 = \eta_2 = -\eta_3, \\ (x-1)\Omega_2^{(4,n)}(x)\Omega_3^{(4,n)}(x), \\ \qquad \text{if} \quad \eta_0 = -\eta_1 = \eta_2, \\ (x-1)\Omega_0^{(4,n)}(x)\Omega_3^{(4,n)}(x), \\ \qquad \text{if} \quad \eta_1 = -\eta_2 = \eta_3, \\ (x-1)\Omega_1^{(4,n)}(x)\Omega_2^{(4,n)}(x), \\ \qquad \text{if} \quad -\eta_0 = \eta_1 = \eta_3. \end{cases}$$

(b) The case that $n \equiv 1 \pmod 8$:

1) When $u^2n - 2n + 1 \not\equiv 0 \pmod q$, we have $L = n$ and $m(x) = x^n - 1$.
2) When $u^2n - 2n + 1 \equiv 0 \pmod q$, we have $L = (3n+1)/4$ and

$$g(x) = \begin{cases} (x^n-1)/\Omega_0^{(4,n)}(x), & \text{if} \quad \eta_0 = -\eta_1, \\ (x^n-1)/\Omega_1^{(4,n)}(x), & \text{if} \quad \eta_1 = -\eta_2, \\ (x^n-1)/\Omega_2^{(4,n)}(x), & \text{if} \quad \eta_2 = -\eta_3, \\ (x^n-1)/\Omega_3^{(4,n)}(x), & \text{if} \quad \eta_0 = -\eta_3. \end{cases}$$

*Proof:* First, we consider the case when $n \equiv 5 \pmod q$.

Let $u^2n+2n+1 \not\equiv 0 \pmod q$. Since by definition $S(1) = (n-1)/2$, from the conditions of this theorem, Lemma 2 and (5) it follows that $L = n$ and $m(x) = x^n - 1$.

Let $u^2n + 2n + 1 \equiv 0 \pmod q$ and $n \not\equiv -1 \pmod q$. Then by Lemma 2 there exists $i : S(\eta^{g^i}) = 0, 0 \le i \le 3$. Suppose that there also exists $k : 0 \le k \le 3, k \ne i$ such that $S(\eta^{g^k}) = 0$. Then by (5) we have $\eta_k = -\eta_{k+1}$ and $\eta_i = -\eta_{i+1}$. Hence, $\eta_0 = \eta_2$ or $\eta_1 = \eta_3$. Without loss of generality, we can assume that we have the first option. Then by Lemma 1 we obtain that

$$\theta_0^2 - (u-1)\theta_0 - (3n-1+2u)/4 = 0.$$

Since $\theta_0$ is a root of $x^2+x-(n-1)/4$, it follows that $u\theta_0+(n+u)/2 = 0$ and $(n+u)^2/4 - u(n+u)/2 - u^2(n-1)/4 = 0$. So, $n \equiv u^2 \pmod q$. Therefore, since $u^2n+2n+1 \equiv 0 \pmod q$ and $n \not\equiv 1 \pmod q$ we obtain that $n \equiv -1 \pmod q$. We have a contradiction. The conclusion of this theorem in this case follows from Lemma 2 and (6)-(7) .

Let $n \equiv -1 \pmod q$ and $u^2 \equiv -1 \pmod q$. Then by Lemma 1 $\theta_0$ and $\theta_1$ are roots of the polynomial $x^2+x+1/2$. Since $n \equiv u^2 \pmod q$, it follows that $\theta_0 = (-1-u)/2$ and $\theta_1 = (-1+u)/2$ or vice versa. In this case by Lemma 1 we obtain that $\eta_0$ and $\eta_2$ are roots of

$$x^2 + (u+1)x/2 + (u+1)(u-1)/8 + (3u^2 - 1 + 2u)/16$$

or

$$x^2 + (u+1)x/2 + (u^2 + 2u + 1)/16.$$

Hence $\eta_0 = \eta_2 = -(u+1)/4$.

Similarly, we have that $\eta_1$ and $\eta_3$ are roots of $x^2 - (u-1)x/2 - (u+2)/8$. Thus, $\eta_1, \eta_3 \in \{-(u+1)/4, (3u-1)/4\}$. Since $u \not\equiv 0 \pmod q$, it follows by (4) that

$$|\{i : \eta_i + \eta_{i+1} = 0, i = 0, 1, 2, 3\}| = 2.$$

To conclude the proof for $n \equiv 5 \pmod 8$, it remains to use (6) and (7).

Let $n \equiv 1 \pmod 8$. If there exist $k, i : 0 \le k < i \le 3$, $k \ne i$ such that $S(\eta^{g^k}) = S(\eta^{g^i}) = 0$ then as earlier we can obtain that $n \equiv u^2 \pmod q$. Since $u^2n - 2n + 1 \equiv 0 \pmod q$, it follows that $u^2 \equiv 1(\bmod\ p)$ and $n \equiv 1 \pmod q$. This contradicts the conditions of Theorem 4. So, with similar arguments as above we obtain the statement of Theorem 4 for $n \not\equiv 1 \pmod q$. ■

*Corollary 5:* Let $n \equiv 5 \pmod 8$, $n \equiv -1 \pmod q$, and $u^2 \equiv -1 \pmod q$. Then

$$\{\eta_0, \eta_1, \eta_2, \eta_3\} = \\ \{-(u+1)/4, -(u+1)/4, -(u+1)/4, (3u-1)/4\}.$$

According to Theorem 4, the sequence $s$ has a high linear complexity over the field $GF(q)$ $\left(L > \frac{n}{2}\right)$.

Let's consider some examples.

1) Let $q = 3$. Then $u^2 \equiv 1 \pmod 3$ and congruence $u^2n \pm 2n + 1 \equiv 0 \pmod 3$ has no solution when $n \not\equiv 1 \pmod 3$. Consequently, by Theorem 4, the

linear complexity of the sequence for $n \not\equiv 1 \pmod 3$ ($n = 17, 29$) is equal to the period of the sequence (cases a.1, b.1 in the theorem).

2) Let $q = 5$, $u^2 n \pm 2n + 1 \equiv 0 \pmod 5$ and $n \not\equiv 1 \pmod 5$. Then $n \equiv 5 \pmod 8$, $n \equiv -1 \pmod 5$ and $u^2 \equiv -1 \pmod 5$. Consequently, in this case, only one option with $L = (n+1)/2$ is possible. Here $v \equiv 0 \pmod 5$. It is a familiar fact that in this case $5 \in C_0^{(4,n)}$ [9]. For $n = 109$ we have $L = 55$ ( a.3).
3) Let $q = 7$, $n = 193$. Then $u \equiv -7 \pmod 7$, $n \equiv 4 \pmod 7$ and $L = 145$ (b.2). Let $q = 7$, $n = 37$. Here $u^2 \equiv 1 \pmod 7$ and $n \equiv 2 \pmod 7$, so $L = 28$ (a.2).

Thus, all cases of Theorem 4 are possible. Other results of calculations of the linear complexity of the sequence according to the Berlekamp-Massey algorithm are also consistent with the statements of Theorem 4.

*Remark 6:* The set $C_0^{(4,n)} \cup C_1^{(4,n)}$ will be an almost difference set with parameters $(n, (n-1)/2, (n-5)/4, (n-1)/2)$ in $(GF(n), +)$ when $v = \pm 1$ and $n = u^2 + 4$ [3]. Then congruence $u^2 n + 2n + 1 \equiv 0 \pmod q$ holds if and only if $u^2 \equiv -3 \pmod q$ and $n \equiv 1 \pmod q$. Hence, under the conditions of Theorem 4, the linear complexity of the characteristic sequence of this almost difference set is equal to the period of the sequence.

It is worth pointing out that $\eta_i, i = 0, 1, 2, 3$ are also called the Gauss periods over $GF(q)$ [5]. Thus, we find a series of the Gauss periods and generalize the results from [11]. Besides, if $A_k = \sum_{j=0}^{p-1} h_j \alpha^{kj}, k = 0, 1, \ldots, p-1$ is a (discrete) Fourier transform of a sequence $\{h_j\}$ with the support $C_0^{(4,n)}$ then $A_k = \eta_j$ if $k \in C_j^{(4,n)}$ [8]. So, Corollaries 3 and 5 define the discrete Fourier transform in the considering case.

It is a familiar fact that $(S(\eta))^q = S(\eta^q)$ in $GF(q)$. From this we can establish by (3) and (4) that if there exists $j : j \neq 0$ and $S(\eta^j) = 0$ then $q \in C_0^{(4,n)}$. So, from Lemma 2 we obtain an interesting corollary. If $u^2 n + 2n + 1 \equiv 0 \pmod q$ for $n \equiv 5 \pmod q$ or $u^2 n - 2n + 1 \equiv 0 \pmod q$ for $n \equiv 1 \pmod 8$ then $q \in C_0^{(4,n)}$ (here, $q > 2$).

## V. Notes on cyclic codes

Cyclic codes are used in many areas [10]. It is a well-known fact that for any cyclic code $C$ of length $n$ over $GF(q)$ there exists a unique unitary polynomial $g(x) \in GF(q)[x]$ of smallest degree such that $C = \langle g(x) \rangle$, where $\langle g(x) \rangle$ is the principal ideal of the ring $GF(q)[x]/(x^n - 1)$. A polynomial $g(x)$ divides $x^n - 1$ and is called a generating polynomial of cyclic code $C$ [5].

Let $D$ is a nonempty subset $\mathbb{Z}_n$ and $D(x) = \sum\limits_{i \in D} x^i$. Cyclic code in $GF(q)$ with generating polynomial $g(x) = \gcd(x^n - 1, D(x))$ is called the cyclic code of the set $D$ [5]. In [5] C. Ding investigated the parameters of the cyclic code over $GF(q)$, when $D$ is a difference set or an almost difference set. In particular, when $D$ is a union of two cyclotomic classes of the fourth order modulo $n$. In the latter case, under the restriction that the characteristic of the field $GF(q)$ divides $(n-1)/4$.

Let $s(D)$ be the characteristic sequence of a set $D$, i.e. $s(D)$ is the binary sequence with period $n$, defined as

$$s(D)_i = \begin{cases} 1, & \text{if } i \pmod n \in D, \\ 0, & \text{otherwise.} \end{cases}$$

Then $m_{s(D)}(x) = (x^n - 1)/g(x)$ and $L_{s(D)} = \operatorname{rank}_q D$, where $\operatorname{rank}_q D$ is the code dimension $C_{GF(q)}(D)$ over $GF(q)$.

Consequently, Theorem 4 also determines the dimension and the generating polynomial of the above cyclic codes, when $D = C_0^{(4,n)} \cup C_1^{(4,n)}$. Thus, a partial solution of Problem 7.1 from [5] is proposed in this paper. The question of estimating the Hamming distance for these codes remains open. When $\operatorname{rank}_q D = L = (n+1)/2$ one can apply an estimate for dual codes.

*Example 7:* Let $(q, n) = (7, 37)$. Then $n = u^2 + 4v^2 = 1 + 4 \cdot 3^2$. Hence, $u^2 n + 2n + 1 \equiv 0(\bmod\ 7)$. Then $C_{GF(7)}(D)$ is a $[37, 28]$ cyclic code with generating polynomial $x^9 + 3x^6 + 4x^5 + 4x^4 + 2x^3 + 2x^2 + 5x + 6$.

## VI. Conclusion

We investigated the linear complexity of the class of periodic binary cyclotomic sequences and found their minimal polynomial. The sequences are formed on the basis of two cyclotomic classes of the fourth order. We have shown that these sequences have high linear complexity over the finite field of an odd characteristic different from the sequence period.

## References

[1] H. ALy, W. Meidl, A. Winterhof, “ On the k-error linear complexity of cyclotomic sequences,” J. Math. Crypt., vol. 1, pp. 1-14, 2007.
[2] T.M. Cusick, C. Ding, A. Renvall, Stream Ciphers and Number Theory, North-Holland Publishing Co., Amsterdam, 1998.
[3] C. Ding, T. Helleseth, H. Martinsen, “New families of binary sequences with optimal three-level autocorrelation,” IEEE Trans. Info. Theory, vol.47, pp. 428 - 433, 2001.
[4] C. Ding, “Cyclic codes from cyclotomic sequences of order four,” Finite Fields Appl, vol. 23, pp. 8-34, 2013.
[5] C. Ding, Codes from Difference Sets, World Scientific, 2015.
[6] V. Edemskii, “On the linear complexity of binary sequences on the basis of biquadratic and sextic residue classes,” Discret. Math. Appl., vol. 20(1), pp. 75-84, 2010; translation from Diskretn. Mat. vol. 22(4), pp. 74-82, 2010.
[7] V. Edemskiy, N. Sokolovskiy, “Linear Complexity Cubic Sequences over Finite Fields,” Proc. of the 3rd International Conference on Mathematics and Computers in Sciences and Industry ( MCSI 2016), Chania, Crete, Greece, August 27-29, pp. 57-60, 2016.
[8] S.W. Golomb, G. Gong, Signal Design for Good Correlation: For Wireless Communications, Cryptography and Radar Applications. Cambridge University Press, 2005.
[9] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, Springer, Berlin, 1982.
[10] R. Lidl, H. Niederreiter, Finite Fields, Addison-Wesley, MA, 1983.
[11] L. Hu, Q. Yue, X. Zhu, “Gauss periods and cyclic codes from cyclotomic sequences of small orders,” Journal of electronics (China),vol. 31 (6), pp. 537-546, 2014.
[12] Q. Wang, D. Lin, X. Guang, “On the Linear Complexity of Legendre Sequences Over $F_q$,” IEICE Trans. Fundamentals, vol. E97-A (7), pp. 1627-1630, 2014.
[13] Q. Wang, “Some cyclic codes with prime length from cyclotomy of order 4,” Cryptogr. Commun., vol. 9 (1), pp. 85-92, 2017.