Notes about the linear complexity of the cyclotomic sequences order three and four over finite fields

Vladimir Edemskiy, Nikita Sokolovskiy

Abstract—We investigate the linear complexity and the minimal polynomial over the finite fields of the characteristic sequences of cubic and biquadratic residue classes. Also we find the linear complexity and the minimal polynomial of the balanced cyclotomic sequences of order three.

Keywords—linear complexity, finite field, cubic residue classes, biquadratic residue classes

I. Introduction

THE linear complexity LC of a sequence is an important parameter in its evaluation as a key stream cipher for cryptographic applications [1], [6]. A high linear complexity is necessary for a good cryptographic sequence. It may be defined as the length of the shortest linear feedback shift register that is capable of generating the sequence. The feedback function of this shift register can be deduced from the knowledge of just $2LC$ consecutive digits of the sequence. Thus, it is reasonable to suggest that "good" sequences have $LC > N/2$ (where N denotes the period of the sequence) [11].

Using classical cyclotomic classes to construct binary and other sequences, which are called cyclotomic sequences, is an important method for sequence design [1]. Cyclotomic sequences have good pseudo-random properties and have been widely used as keystreams in private-key cryptosystems. There are many works devoted to the study of the linear complexity of above-mentioned binary sequences over the finite field of order two. Also, the linear complexity of several cyclotomic sequences of length p was derived over the finite field $\mathbb{F}_p$. The linear complexity of Legendre sequences over the finite field of any order was studied in [14]. Investigating the cyclic codes, C.Ding studies the minimal polynomial of the series of cyclotomic sequences when $p \equiv 1(\mathrm{mod}\ q)$, where p is the length of a sequence and q is the order of a finite field [2]. Also, several results about the linear complexity of cyclotomic sequences of orders three and four over the finite field $\mathbb{F}_q$ where $q \neq 2$ and q is not equal to the period of the sequence were obtained in [4], [5], [9], [13](see, also reference here).

In this paper we investigate the linear complexity of cyclotomic sequences of order three and four without restrictions on the length of the sequences. We obtain known results shown in [9], [13] as well as some new results.

This work was supported by the Ministry of Education and Science of the Russian Federation as a part of state-sponsored project no 1.949.2014/K.

II. Preliminaries

First, we briefly repeat the basic definitions and general information.

A. Definitions

Let $p = dR + 1, d = 2, 3, 4,\ R \in \mathbb{Z}$ be an odd prime and let θ be a primitive root modulo p [10], and let $\mathbb{Z}_p$ be a ring of residue classes modulo p. Put, by definition

$$H_0^{(d)} = \{\theta^{di} \bmod\ p, i = 0, 1, \ldots, R-1\},$$

where $a \bmod\ p$ denotes the least nonnegative integer that is congruent to a modulo p. Let $H_k^{(d)} = \theta^k H_0^{(d)}$, $k = 0, \ldots, d-1$, where the arithmetic is that of $\mathbb{Z}_p$. Then $H_k^{(d)}, k = 0, \ldots, d-1$ are cyclotomic classes of order d with respect to p [1]. In this case we have the following partition

$$\mathbb{Z}_p = \cup_{k=0}^{d-1} H_k^{(d)} \cup \{0\}.$$

Let $\mathbb{F}_q$ be a finite field of order q, where q is an odd prime and $q \neq p$. The field $\mathbb{F}_q$ we identify with the set of integers $\{0, 1, \ldots, q-1\}$. Further, we will investigate the linear complexity over $\mathbb{F}_q$ of sequences constructed on the cyclotomic classes $H_k^{(d)}$.

It is well known that if $\{s_i\}$ is a sequence of period p, then the linear complexity $LC_q(s)$ over $\mathbb{F}_q$ and the minimal polynomial of this sequence are defined by

$$LC_q(s) = p - \deg \gcd\big(x^p - 1, S(x)\big), \quad m(x) = (x^p - 1)/\gcd\big(x^p - 1, S(x)\big) \quad (1)$$

where $S(x) = s_0 + s_1 x + \ldots + s_{p-1} x^{p-1}$ [1]. It is worth pointing out that the minimal polynomials of $m(x)$ defined here may be the reciprocals of the minimal polynomials defined in other references.

Let α be a primitive pth root of unity in the extension of $\mathbb{F}_q$. It is known to exist by Galois theory. Then by Blahut's theorem

$$LC_q(s) = p - |\{v \mid S(\alpha^v), v = 0, 1, \ldots, p-1\}|. \quad (2)$$

So, in order to find the linear complexity of $\{s_i\}$ it is sufficient to find the zeros of $S(x)$ in the set $\{\alpha^v, v = 0, 1, \ldots, p-1\}$.

Introduce the subsidiary polynomials

$$\varphi_k^{(d)}(x) = \prod_{j \in H_k^{(d)}} (x - \alpha^j),\ k = 0, \ldots, d-1.$$

Then, we have the factorization of the polynomial

$$x^p - 1 = (x-1)\varphi_0^{(d)}(x)\,\varphi_1^{(d)}(x) \ldots \varphi_{d-1}^{(d)}(x)$$

and $\varphi_k^{(d)}(x) \in \mathbb{F}_q[x]$ if $q \in H_0^{(d)}$.

B. A computational method

Introduce the subsidiary polynomial $S_d(x) = \sum_{i \in H_0^{(d)}} x^i$. The following lemma is well-known (see, for example [1] or [12]).

Lemma 1: (i) If $v \in H_k^{(d)}$, $k = 0, \ldots, d-1$ then $S_d(\alpha^v) = S_d(\alpha^{\theta^k})$;

(ii) $\sum_{i \in H_k^{(d)}} (\alpha^{iv}) = S_d(\alpha^{v\theta^k})$, $k = 0, \ldots, d-1$.

Hence, in order to find the values $S(\alpha^v)$ for the cyclotomic sequence it is sufficient to find the $S_d(\alpha^{\theta^k})$.

Since $1 + \alpha + \ldots + \alpha^{p-1} = 0$ by Lemma 1 it follows that

$$S_d(\alpha) + S_d(\alpha^\theta) + \cdots + S_d(\alpha^{\theta^{d-1}}) = -1. \tag{3}$$

It is worth pointing out that sums $\sum_{i \in H_k^{(d)}} \alpha^i$ is also called the Gauss periods over $\mathbb{F}_q$ [2]. 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 the characteristic sequence $\{h_j\}$ of set $H_0^{(d)}$ then $A_k = S_d(\alpha^k)$ [6].

Denote by $(i,j)_d, i, j \in \mathbb{Z}$ cyclotomic numbers of order d [8]. Then $(m,n)_d = |(H_m^{(d)}+1) \cap H_n^{(d)}|, m, n = 0, \ldots, d-1$.

The following statements was discussed in [12] (see, also [2], [5]).

Lemma 2: Let $j, k = 0, \ldots, d-1$. Then

$$S_d(\alpha^{\theta^j}) S_d(\alpha^{\theta^k}) = \sum_{f=0}^{d-1} (k-j, f)_d S_d(\alpha^{\theta^f}) + \delta,$$

where

$$\delta = \begin{cases} (p-1)/d, & \text{if } j = k, \\ 0, & \text{otherwise.} \end{cases}$$

If $p \equiv 1 (\mathrm{mod}\ 3)$ then $4p$ can be expressed as $4p = L^2 + 27M^2; L \equiv 1 (\mathrm{mod}\ 3)$, here M is two-valued, depending on the choice of the primitive root modulo p [10].

Lemma 3: Let $4p = L^2 + 27M^2; L \equiv 1 (\mathrm{mod}\ 3)$. Then $S_3(\alpha), S_3(\alpha^\theta), S_3(\alpha^{\theta^2})$ are roots of the polynomial

$$z^3 + z^2 - \frac{p-1}{3} z - \frac{3p + Lp - 1}{27}.$$

In what follows, we denote the polynomial

$$z^3 + z^2 - (p-1)/3z - (3p + Lp - 1)/27$$

by $P(z)$.

Remark 4: In particular case when $LM \equiv 0 (\mathrm{mod}\ q)$ the values of $S_3(\alpha), S_3(\alpha^\theta), S_3(\alpha^{\theta^2})$ were calculated in [9] and for the special case in [3].

If $p \equiv 1 (\mathrm{mod}\ 4)$ then p can be expressed as $p = x^2 + 4y^2; x \equiv 1 (\mathrm{mod}\ 4)$, here y is two-valued, depending on the choice of the primitive root. The following statements follow from [2], [14](the formulae (6.14), (6.19), etc.).

Lemma 5: Let $p \equiv 1 (\mathrm{mod}\ 4)$. Then:

(i) $S_2(\alpha)$ and $S_2(\alpha^\theta)$ are roots of $z^2 + z - (p-1)/4$;

(ii) When $p \equiv 5 (\mathrm{mod}\ 8)$ we have $S_4(\alpha^{\theta^i})$ and $S_4(\alpha^{\theta^{i+2}})$ are the zeros of equation

$$w^2 - S_2(\alpha^{\theta^i}) w + S_2(\alpha^{\theta^i})(x-1)/4 + (3p - 1 + 2x)/16 = 0;$$

(iii) When $p \equiv 1 (\mathrm{mod}\ 8)$ we have $S_4(\alpha^{\theta^i})$ and $S_4(\alpha^{\theta^{i+2}})$ are the zeros of equation

$$w^2 - S_2(\alpha^{\theta^i}) w + S_2(\alpha^{\theta^i})(x-1)/4 - (p + 1 - 2x)/16 = 0;$$

Denote by $\left(\frac{p}{q}\right)$ a symbol Legendre. The discriminant of $z^2 + z - (p-1)/4$ equals p. From this we can establish the following assertion.

Corollary 6: $S_2(\alpha) \in \mathbb{F}_q$ if and only if $\left(\frac{p}{q}\right) = 1$.

Remark 7: In particular cases the values of $S_4(\alpha), S_4(\alpha^\theta), S_4(\alpha^{\theta^2}), S_4(\alpha^{\theta^3})$ were investigated in [2], [9], [13] (see Section V).

III. The linear complexity of the characteristic sequence of cubic residues

First of all, we find the linear complexity of the characteristic sequence of cubic residue class. Let $\{s_i\}$ be a sequence of period p defined as

$$s_i = \begin{cases} 1, & \text{if } i \bmod p \in H_0^{(3)}, \\ 0, & \text{otherwise} \end{cases}. \tag{4}$$

By definition of sequence we see that

$$S(\alpha^v) = S_3\left(\alpha^{\theta^k}\right) \text{ for } v \in H_k,\ k = 0, 1, 2.$$

So, by (2) we obtain that

$$LC_q(s) = p - |\{k |\ \ S_3(\alpha^{\theta^k}) = 0,\ \ k = 0, 1, 2\}|(p-1)/3 - \Delta, \tag{5}$$

where

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

Suppose that exists $j : j \neq 0$ and $S(\alpha^j) = 0$; then without loss of generality, we can choose α such that $S_3(\alpha) \neq 0$ and $S_3\left(\alpha^{\theta^2}\right) = 0$.

Here we consider only the case when $q > 3$.

Theorem 8: Let $\{s_i\}$ be defined by (4), $4p = L^2 + 27M^2$, $L \equiv 1 (\mathrm{mod}\ 3)$ and $q > 3$. Then:

1) $LC_q(s) = (p-1)/3$ and $m(x) = \varphi_0^{(3)}(x)$ if $p \equiv 1 (\bmod\ q)$ and $L \equiv -2 (\mathrm{mod}\ q)$.
2) $LC_q(s) = 2(p-1)/3 + 1$ and $m(x) = (x-1)\varphi_0^{(3)}(x)\,\varphi_1^{(3)}(x)$ if $p \not\equiv 1 (\mathrm{mod}\ q)$ and $Lp + 3p \equiv 1 (\mathrm{mod}\ q)$.
3) $LC_q(s) = p - 1$ and $m(x) = (x^p - 1)/(x-1)$ if $p \equiv 1 (\mathrm{mod}\ q)$ and $L \not\equiv -2 (\mathrm{mod}\ q)$.
4) $LC_q(s) = p$ and $m(x) = x^p - 1$ if $p \not\equiv 1 (\mathrm{mod}\ q)$ and $Lp + 3p \not\equiv 1 (\mathrm{mod}\ q)$.

Proof: For the proof we use (1) and (5). First of all note that $S(1) = (p-1)/3$. Hence

$$\Delta = \begin{cases} 1, & \text{if } \ p \equiv 1 (\mathrm{mod}\ q), \\ 0, & \text{if } \ p \not\equiv 1 (\mathrm{mod}\ q). \end{cases}$$

By Lemma 3 $S_3(\alpha)$, $S_3(\alpha^\theta)$, $S_3(\alpha^{\theta^2})$ are roots of $P(z)$.

We consider the first case. Assume that zero is a root of multiplicity 2 of the polynomial $P(z)$, then

$$(3p + Lp - 1)/27 = 0 \text{ and } (p-1)/3 = 0.$$

So, $p \equiv 1 (\mathrm{mod}\ q)$ and $L \equiv -2 (\mathrm{mod}\ q)$.

Let $p \equiv 1 (\mathrm{mod}\ q)$ and $L \equiv -2 (\mathrm{mod} q)$; then $S_3(\alpha)$, $S_3(\alpha^\theta)$, $S_3(\alpha^{\theta^2})$ are roots of the equation $z^3 + z^2 = 0$. Hence, two of three elements $S_3(\alpha)$, $S_3(\alpha^\theta)$, $S_3(\alpha^{\theta^2})$ are

equal to 0 and the third element equals -1. So, by (5) we obtain $LC_q(s) = (p-1)/3$.

Further, by the assumption $S_3(\alpha) \neq 0$, hence $\gcd(x^p - 1, S(x)) = (x-1)\varphi_1(x)\varphi_2(x)$. Then the result follows immediately from (1).

Other statements of this theorem may be proved similarly. ∎

In the particular case for $M \equiv 0 \pmod q$, the first statement of Theorem 8 was proved by another method in [9].

Remark 9: It is a familiar fact that $S^q(\alpha) = S(\alpha^q)$ in $\mathbb{F}_q$. From this we can establish that if there exists $j : j \neq 0$ and $S(a^j) = 0$ then $q \in H_0$. So, by Theorem 8 we obtain that if $Lp + 3p \equiv 1 \pmod q$ then $q \in H_0^{(3)}$.

Example 10: Let $p = 127$ and $q = 5$. Since $4 \cdot 127 = 20^2 + 27 \cdot 2^2$, it follows that $L = -20, M = \pm 2$ and $Lp + 3p \equiv 1 \pmod 5$. Hence, in this case the linear complexity over $\mathbb{F}_5$ of $\{s_i\}$ is equal to $LC_5(s) = 85$. Here $M \not\equiv 0 \pmod 5$.

The results of direct computing of the linear complexity by Berlekamp-Massey algorithm for $p = 127, 457, q = 5$; $p = 607, q = 7$; $p = 1789, 1933, q = 11$ and $p = 919, 1021, q = 13$ confirm the results of Remark 9.

IV. Balanced cubic sequences

Let $\{s_i\}$ be a balanced cubic sequence defined by

$$s_i = \begin{cases} 0, & \text{if } i \bmod p \in \{0\} \cup H_0^{(3)}, \\ 1, & \text{if } i \bmod p \in H_1^{(3)}, \\ 2, & \text{if } i \bmod p \in H_2^{(3)}. \end{cases} \tag{6}$$

For $q = 3$ such sequences were investigated in [7]. In what follows let $q > 3$.

From our definition it follows that

$$S(\alpha^v) = S_3\left(\alpha^{\theta^{k+1}}\right) + 2S_3\left(\alpha^{\theta^{k+2}}\right) \tag{7}$$

for $v \in H_k,\ k = 0, 1, 2$.

The values of cyclotomic numbers of order three depend on p, L, M. By [8] we have that $(m,n)_3 = (n,m)_3$ and

$$\begin{aligned} (0,0)_3 &= (p - 8 + L)/9, \\ (0,1)_3 &= (2,2)_3 = (2p - 4 - L + 9M)/18, \\ (0,2)_3 &= (1,1)_3 = (2p - 4 - L - 9M)/18, \\ (1,2)_3 &= (p + 1 + L)/9. \end{aligned} \tag{8}$$

Suppose $S(\alpha^j) = 0$ and $j \neq 0$; then without loss of generality, we can choose α such that $S(\alpha) = 0$. Before we give the main result of this section, we establish the following lemmas.

Lemma 11: Let $\{s_i\}$ be defined by (6), $4p = L^2 + 27M^2, L \equiv 1 \pmod 3$. Then $S(\alpha) = 0$ if and only if $Mp \equiv p - 1 \pmod q$.

Proof: First, we find the necessary conditions for the existence of the roots of $S(x)$ in the set $\{\alpha^v, v = 1, \ldots, p-1\}$. Let $S(\alpha) = 0$, i.e.,

$$S_3\left(\alpha^{\theta}\right) + 2S_3\left(\alpha^{\theta^2}\right) = 0.$$

Denote $S_3\left(\alpha^{\theta^2}\right)$ by a; then $S_3\left(\alpha^{\theta}\right) = -2a$ and $a,\ -2a$ are zeros of the polynomial $P(z)$. Hence,

$$\begin{cases} a^3 + a^2 - \frac{p-1}{3}a - \frac{3p+Lp-1}{27} = 0, \\ -8a^3 + 4a^2 + 2\frac{p-1}{3}a - \frac{3p+Lp-1}{27} = 0. \end{cases}$$

or

$$\begin{cases} 12a^2 + 2(1-p)a - (3p + Lp - 1)/3 = 0, \\ -a(-9a^2 + 3a + p - 1) = 0, \end{cases} \tag{9}$$

Besides, by Lemma 2 we have that

$$(a-1)\,a = (0,2)_3(a-1) + (1,2)_3(-2a) + (0,1)_3 a.$$

Using the above-mentioned formulas for the cyclotomic numbers (8), we obtain the following equation

$$a^2 - a = -\frac{L+2}{3}a - \frac{2p - 4 - L - 9M}{18}. \tag{10}$$

Suppose $a = 0$; then by the proof of Theorem 8 we have $p \equiv 1 \pmod q$, $L \equiv -2 \pmod q$ and $M \equiv 0 \pmod q$ by (10).

Let $a \neq 0$. From (9) and (10) we obtain that

$$(18 - 6p)a = -p + Lp + 3$$

and

$$6La = -4p + 6 - L - 9M.$$

We consider two cases.

(i) Let $p \equiv 3 \pmod q$. Then $L \equiv 0 \pmod q$ and $3M \equiv 2 \pmod q$. The assertion of this lemma is true.

(ii) Let $p \not\equiv 3 \pmod q$. In this case

$$a = (-p + Lp + 3)/(18 - 6p)$$

and by (9) we have that $L^2p^2 = 4p^3 - 27p^2 + 54p - 27$ or $L^2p^2 = (p-3)^2(4p-3)$.

Further, since $6La = -4p + 6 - L - 9M$ it follows that

$$(-4p + 6 - L - 9M)(3 - p) = -pL + L^2p + 3L.$$

Hence $Mp = p - 1$ in $\mathbb{F}_q$.

Now, we prove that $Mp \equiv p - 1 \pmod q$ is the sufficient condition for the existence of roots of $S(x)$ in the set $\{\alpha^v, v = 1, \ldots, p-1\}$. Since $Mp \equiv p - 1 \pmod q$ and $4p = L^2 + 27M^2$ it follows that $L^2p^2 = (p-3)^2(4p-3)$.

Further, we note that if $L^2p^2 = (p-3)^2(4p-3) = 4p^3 - 27p^2 + 54p - 27$ then

$$\left\{S_3\left(\alpha^{\theta^k}\right),\ k = 0, 1, 2\right\} = \{-2a, a-1,\ a\}$$

where

$$a = \begin{cases} 1/6\,(1 - Lp/(p-3)), & \text{if } p \not\equiv 3 \pmod q, \\ 2/3, & \text{if } p \equiv 3 \pmod q. \end{cases}$$

A proof of this fact can be easily carried out by computating the values of the polynomial $P(z)$ for $z = a, -2a, a-1$, which is omitted here.

Without loss of generality, we can choose $S_3\left(\alpha^{\theta^2}\right) = a$. There exist two cases

$$S_3(\alpha) = a - 1, \quad S_3\left(\alpha^{\theta}\right) = -2a$$

or

$$S_3(\alpha) = -2a, \quad S_3\left(\alpha^{\theta}\right) = a - 1.$$

In the first case $S(\alpha) = 0$ by (7). Now, we study the second case. By Lemma 2 we obtain

$$(a-1)\,a = (0,1)_3(a-1) + (0,2)_3 a + (0,1)_3(-2a)$$

or

$$6La = -4p + 6 - L - 9M. \tag{11}$$

If $p \equiv 3 (\mathrm{mod}\ q)$ then $L \equiv 0 (\mathrm{mod}\ q)$ and $3M \equiv 2 (\mathrm{mod}\ q)$. And we have a contradiction with (11).

Suppose $p \not\equiv 3 (\mathrm{mod}\ q)$; then $a = 1/6 - Lp/(6(p-3))$. Since $L^2p^2 \equiv (p-3)^2(4p-3) (\mathrm{mod}\ q)$ it follows from (11) that $Mp \equiv 1 - p (\mathrm{mod}\ q)$. By the condition $Mp \equiv p - 1 (\mathrm{mod}\ q)$, hence we see $M \equiv 0 (\mathrm{mod}\ q)$ and $p \equiv 1 (\mathrm{mod}\ q)$. From this we can establish by Lemma 3 that $\{-2a, a-1,\ a\} = \{0, 0,\ -1\}$ or $\{-2a, a-1,\ a\} = \{-2/3, -2/3, 1/3\}$. To conclude the proof, it remains to note that by (7) in both cases there exists $k : S(\alpha^{\theta^k}) = 0$. ∎

Lemma 12: Let $\{s_i\}$ be defined by (6), $4p = L^2 + 27M^2, L \equiv 1 (\mathrm{mod}\ 3)$. The polynomial $S(x)$ has two roots in the set $\{\alpha, \alpha^{\theta}, \alpha^{\theta^2}\}$ if and only if $p \equiv 3 (\mathrm{mod}\ q)$ and $3M \equiv 2 (\mathrm{mod}\ q)$.

Proof: First, we find the necessary conditions for 2 roots of $S(x)$ to exist. Without loss of generality, we can choose α such that $S(\alpha) = S(\alpha^{\theta}) = 0$. Then by (4) we have

$$\begin{cases} S_3\left(\alpha^{\theta}\right) + 2S_3\left(\alpha^{\theta^2}\right) = 0, \\ S_3\left(\alpha^{\theta^2}\right) + 2S_3(\alpha) = 0. \end{cases}$$

So, by (3) $S_3(\alpha) = -1/3, S_3\left(\alpha^{\theta}\right) = 4/3, S_3\left(\alpha^{\theta^2}\right) = 2/3$. Using Lemmas 3 and 11 we obtain that $p \equiv 3 (\mathrm{mod}\ q)$ and $3M \equiv 2 (\mathrm{mod}\ q)$.

Let $p \equiv 3 (\mathrm{mod}\ q)$ and $3M \equiv 2 (\mathrm{mod}\ q)$. Then by Lemma 3 we obtain that $\{S_3(\alpha), S_3\left(\alpha^{\theta}\right), S_3\left(\alpha^{\theta^2}\right)\} = \{-1/3, -4/3, 2/3\}$. The conclusion of this lemma then follows from (7). ∎

Suppose that there exists $j : j \neq 0$ and $S(\alpha^j) = 0$; then without loss of generality, we can choose α such that $S(\alpha) = 0$ and $S\left(\alpha^{\theta^2}\right) \neq 0$.

Theorem 13: Let $\{s_i\}$ be defined by (6), $4p = L^2 + 27M^2$, $L \equiv 1 (\mathrm{mod}\ 3)$ and $q > 3$. Then:

1) $LC_q(s) = (p-1)/3$ and $m(x) = \varphi_2(x)$ if $p \equiv 3 (\mathrm{mod}\ q)$ and $3M \equiv 2 (\mathrm{mod}\ q)$.
2) $LC_q(s) = 2(p-1)/3$ and $m(x) = \varphi_1^{(3)}(x)\,\varphi_2^{(3)}(x)$ if $p \equiv 1 (\mathrm{mod}\ q)$ and $M \equiv 0 (\mathrm{mod}\ q)$.
3) $LC_q(s) = 2(p-1)/3 + 1$ and $m(x) = (x-1)\varphi_1^{(3)}(x)\,\varphi_2^{(3)}(x)$ if $pM \equiv p - 1 (\mathrm{mod}\ q)$ and $p \not\equiv 1, 3 (\mathrm{mod}\ q)$.
4) $LC_q(s) = p - 1$ and $m(x) = (x^p - 1)/(x-1)$ if $p \equiv 1 (\mathrm{mod}\ q)$ and $M \not\equiv 0 (\mathrm{mod}\ q)$.
5) $LC_q(s) = p$ and $m(x) = x^p - 1$ if $p \not\equiv 1 (\mathrm{mod}\ q)$ and $pM \not\equiv p - 1 (\mathrm{mod}\ q)$.

Theorem 13 follows immediately from Lemmas 11, 12.

The results of direct computing of the linear complexity by Berlekamp-Massey algorithm for $3 \leq q \leq 11, 5 \leq p \leq 6000$ confirm the results of Theorems 8, 13.

V. The linear complexity of the characteristic sequence of biquadratic residues

First of all, we consider a sequence defined by

$$s_i = \begin{cases} 1, & \text{if } i \bmod p \in H_0^{(4)}, \\ 0, & \text{if } i \bmod p \notin H_0^{(4)}. \end{cases} \tag{12}$$

The linear complexity of s was studied for $y \equiv 0 (\mathrm{mod}\ q)$ in [9].

The linear complexity and minimal polynomial of sequences defined as

$$u_i = \begin{cases} 1, & \text{if } i \bmod p \in H_1^{(4)} \cup H_2^{(4)} \cup H_3^{(4)}, \\ 0, & \text{if } i \bmod p \in H_0^{(4)}, \\ \varrho, & \text{if } i \bmod p = 0. \end{cases}$$

where $\varrho \in \{0, 1\}$ were investigated for $p \equiv 1 (\mathrm{mod}\ q)$ in [2], [4] and for $3p + 1 \equiv 0 (\mathrm{mod}\ q), \varrho = 1$ or $p = 9 + 4y^2, \varrho = 0$ in [13]. By our definitions $s_i = 1 - u_i$ for $i \bmod p$, thus this is sufficient to consider only the case when $p \not\equiv 1 (\mathrm{mod}\ q)$.

By Lemma 1 and (2) for the linear complexity of sequence constructed on the cyclotomic classes of order four we have the following formula

$$LC_q = p - |\{k|\ \ S_4(\alpha^{\theta^k}) = 0,\ k = 1, 1, 2, 3\}|(p-1)/4 - \Delta, \tag{13}$$

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

Lemma 14: Let $\{s_i\}$ be defined by (12). Then there exists i such that $S_4(\alpha^{\theta^i}) = 0$ iff there exist $a \in \mathbb{Z}$ such that $p \equiv a^2 (\mathrm{mod}\ q)$ and

$$x \equiv \begin{cases} (3a^2 + 2a + 1)/2a (\mathrm{mod}\ q), & \text{if } p \equiv 5 (\mathrm{mod}\ 8), \\ (a^2 + 2a - 1)/2a (\mathrm{mod}\ q), & \text{if } p \equiv 1 (\mathrm{mod}\ 8). \end{cases}$$

Proof: We prove this statement only for $p \equiv 5 (\mathrm{mod}\ 8)$. Without loss of generality, we can assume that $S_4(\alpha) = 0$. Then by Lemma 5 we have that $S_2(\alpha)(x-1)/4 + (3p - 1 + 2x)/16 = 0$, i.e., $S_2(\alpha) \in \mathbb{F}_q$. Hence, if $S_4(\alpha) = 0$ then there exists a such that $p \equiv a^2 (\mathrm{mod}\ q)$.

By Lemma 5 we obtain that $S_2(\alpha)(x-1)/4$ is a zero of $z^2 + (x-1)z/4 - (x-1)^2(p-1)/64 = 0$. The discriminant of this equation equals $(x-1)^2 p/16$. Further, since $S_2(\alpha)(x-1)/4 = -(3p - 1 + 2x)/16$ it follows that $-(3p - 1 + 2x)/2 = -(x-1)(1 \pm a)$.

Suppose $3p - 1 + 2x = 2(x-1)(1+a)$; then we have $2xa = 1 + 2a + 3a^2$ or $x \equiv (3a^2 + 2a + 1)/2a (\mathrm{mod}\ q)$. Similarly, if $3p - 1 + 2x = 2(x-1)(1-a)$ then $2ax = -3a^2 + 2a - 1$ and changing a by $-a$ we again obtain $x \equiv (3a^2 + 2a + 1)/2a (\mathrm{mod}\ q)$.

Let $x \equiv (3a^2 + 2a + 1)/2a (\mathrm{mod}\ q)$ and $p \equiv a^2 (\mathrm{mod}\ q)$. Then by Lemma 5 we have $S_2(\alpha) = (-1-a)/2$ and $S_2(\alpha) = (-1+a)/2$ or vice versa. Since $\frac{x-1}{4}\frac{-1-a}{2} + \frac{3p-1+2x}{16} = 0$ for $x \equiv (3a^2 + 2a + 1)/2a (\mathrm{mod}\ q)$ and $p \equiv a^2 (\mathrm{mod}\ q)$, by Lemma 5 it follows that $S_4(\alpha)S_4(\alpha^{\theta^2}) = 0$ or $S_4(\alpha^{\theta})S_4(\alpha^{\theta^3}) = 0$. This completes the proof of Lemma 14 for $p \equiv 5 (\mathrm{mod}\ 8)$.

The statement of this lemma for $p \equiv 1 (\mathrm{mod}\ 8)$ may be proved similarly. ∎

If $\left(\frac{p}{q}\right) = -1$ then $LC_q(s) = p$ and $m(x) = x^p - 1$.

Now we consider the case when $\left(\frac{p}{q}\right) = 1$. Since $p \not\equiv 1(\mathrm{mod}\ q)$, it follows that $S(1) \neq 0$.

Suppose that there exists $j : j \neq 0$ and $S(a^j) = 0$; then without loss of generality, we can choose α such that $S_4(\alpha) \neq 0$ and $S_4\left(\alpha^{\theta^3}\right) = 0$.

Lemma 15: Let $\{s_i\}$ be defined by (12) and $p \not\equiv 1(\mathrm{mod}\ q)$. Then $LC_q(s) \geq (p+1)/2$.

Proof: Suppose $LC_q(s) < (p+1)/2$; then by (13) three numbers from $S_4(\alpha^{\theta^i}) = 0, i = 0, 1, 2, 3$ are equal to zero. So, $S_2(\alpha) = 0$ or $S_2(\alpha^\theta) = 0$. Hence, by Lemma 5 we obtain that $p \equiv 1(\mathrm{mod}\ q)$, thus we have the contradiction. ■

Lemma 16: Let $\{s_i\}$ be defined by (12), $p = x^2 + 4y^2, x \equiv 1(\mathrm{mod}\ 4)$. Then $LC_q(s) = (p+1)/2$ iff $p \equiv 5(\mathrm{mod}\ 8)$, $3p + 1 \equiv 0(\mathrm{mod}\ q)$ and $x \equiv 1(\mathrm{mod}\ q)$.

Proof: Let $LC_q(s) = (p+1)/2$. By (13) and the proof of Lemma 15 in this case $S_4(\alpha)S_4(\alpha^{\theta^2}) = 0$ and $S_4(\alpha^\theta)S_4(\alpha^{\theta^3}) = 0$. We consider two cases.

(i) Suppose $p \equiv 5(\mathrm{mod}\ 8)$; then by Lemma 5 $S_2(\alpha)(x-1)/4 + (3p - 1 + 2x)/16 = 0$ and $S_2(\alpha^\theta)(x-1)/4 + (3p - 1 + 2x)/16 = 0$. Summing we obtain that $3p + 1 = 0$. Then $S_2(\alpha)(x-1)/4 + (x-1)/8 = 0$ and $x \equiv 1(\mathrm{mod}\ q)$ or $S_2(\alpha) = -1/2$. By Lemma 5 the latest equality is impossible. The converse assertion follows from [13].

(ii) Suppose $p \equiv 1(\mathrm{mod}\ 8)$; then by Lemma 5 $S_2(\alpha)(x-1)/4 - (p+1-2x)/16 = 0$ and $S_2(\alpha^\theta)(x-1)/4 + (p+1-2x)/16 = 0$. Summing we obtain that $-(x-1)/4 - (p+1-2x)/8 = 0$, hence $p \equiv 1(\mathrm{mod}\ q)$. ■

Thus, we have established the following statements.

Theorem 17: Let $\{s_i\}$ be defined by (12), $p \equiv 5(\mathrm{mod}\ 8)$, $p \not\equiv 1(\mathrm{mod}\ q)$, and $p = x^2 + 4y^2, x \equiv 1(\mathrm{mod}\ 4)$. Then:

(i) $LC_q(s) = (p+1)/2$ and $m(x) = (x-1)\varphi_1^{(4)}(x)\,\varphi_3^{(4)}(x)$ if $3p + 1 \equiv 0(\mathrm{mod}\ q)$ and $x \equiv 1(\mathrm{mod}\ q)$;

(ii) $LC_q(s) = 3(p-1)/4 + 1$ and $m(x) = (x-1)\varphi_1^{(4)}(x)\,\varphi_2^{(4)}(x)\,\varphi_3^{(4)}(x)$ if there exists $a \in \mathbb{Z}$ such that $p \equiv a^2(\mathrm{mod}\ q)$, $x \equiv (3a^2 + 2a + 1)/2a(\mathrm{mod}\ q)$, and $3p \not\equiv -1(\mathrm{mod}\ q)$;

(iii) $LC_q(s) = p$ and $m(x) = x^p - 1$ in other cases.

Our examples $q = 7, p = 37$, and $q = 5, p = 149; q = 11, p = 157$ and $q = 7, p = 53$ show that all the cases of Theorem 17 are possible.

Theorem 18: Let $\{s_i\}$ be defined by (12), $p \equiv 1(\mathrm{mod}\ 8)$, $p \not\equiv 1(\mathrm{mod}\ q)$, and $p = x^2 + 4y^2, x \equiv 1(\mathrm{mod}\ 4)$. Then:

(i) $LC_q(s) = 3(p-1)/4 + 1$ and $m(x) = (x-1)\varphi_1^{(4)}(x)\,\varphi_2^{(4)}(x)\,\varphi_3^{(4)}(x)$ if there exists $a \in \mathbb{Z}$ such that $p \equiv a^2(\mathrm{mod}\ q)$, $x \equiv (a^2 + 2a - 1)/2a(\mathrm{mod}\ q)$;

(ii) $LC_q(s) = p$ and $m(x) = x^p - 1$ in other cases.

Here, for example $q = 5, p = 149(i), q = 7, p = 53(ii)$.

Now, we consider a sequence defined by

$$v_i = \begin{cases} 1, & \text{if } i \bmod p \in \{0\} \cup H_0^{(4)}, \\ 0, & \text{otherwise.} \end{cases} \tag{14}$$

In this case we can obtain the following statements.

Lemma 19: Let $\{v_i\}$ be defined by (14). Then there exist i such that $S_v(\alpha^{\theta^i}) = 0$ iff there exists $a \in \mathbb{Z}$ such that $p \equiv a^2(\mathrm{mod}\ q)$ and

$$x \equiv \begin{cases} (3a^2 - 6a + 9)/2a(\mathrm{mod}\ q), & \text{if } p \equiv 5(\mathrm{mod}\ 8), \\ (a^2 - 6a - 9)/2a(\mathrm{mod}\ q), & \text{if } p \equiv 1(\mathrm{mod}\ 8). \end{cases}$$

Theorem 20: Let $\{v_i\}$ be defined by (14), $p \equiv 5(\mathrm{mod}\ 8)$, and $p = x^2 + 4y^2, x \equiv 1(\mathrm{mod}\ 4)$. Then:

(i) $LC_q(v) = (p-1)/2$ if $p \equiv -3(\mathrm{mod}\ q)$ and $x \equiv -3(\mathrm{mod}\ q)$;

(ii) $LC_q(v) = 3(p-1)/4 + 1$ if there exists $a \in \mathbb{Z}$ such that $p \equiv a^2(\mathrm{mod}\ q)$, $x \equiv (3a^2 - 6a + 9)/2a(\mathrm{mod}\ q)$, and $p \not\equiv -3(\mathrm{mod}\ q)$;

(iii) $LC_q(v) = p - 1$ if $p \equiv -3(\mathrm{mod}\ q)$ and $x \not\equiv -3(\mathrm{mod}\ q)$;

(iv) $LC_q(v) = p$ in other cases.

Our examples $q = 7, p = 109$; $q = 5, p = 101; q = 11, p = 173$, and $q = 13, p = 37$ show that all the cases of Theorem 20 are possible.

Theorem 21: Let $\{v_i\}$ be defined by (14), $p \equiv 1(\mathrm{mod}\ 8)$, and $p = x^2 + 4y^2, x \equiv 1(\mathrm{mod}\ 4)$. Then:

(i) $LC_q(v) = (p+3)/4$ if $p \equiv 9(\mathrm{mod}\ q)$ and $x \equiv -3(\mathrm{mod}\ q)$;

(ii) $LC_q(v) = 3(p-1)/4$ if there exists $a \in \mathbb{Z}$ such that $p \equiv a^2(\mathrm{mod}\ q)$, $x \equiv 2a - 3(\mathrm{mod}\ q)$, and $p \not\equiv -3(\mathrm{mod}\ q)$;

(iii) $LC_q(v) = 3(p-1)/4 + 1$ if there exists $a \in \mathbb{Z}$ such that $p \equiv a^2(\mathrm{mod}\ q)$, $x \equiv (a^2 - 6a - 9)/2a(\mathrm{mod}\ q)$, and $p \not\equiv -3(\mathrm{mod}\ q)$;

(iv) $LC_q(v) = p - 1$ if $p \equiv -3(\mathrm{mod}\ q)$ and $x \not\equiv -3(\mathrm{mod}\ q)$;

(v) $LC_q(v) = p$ in other cases.

Here we can confirm the results of Theorem 21 by the following examples: $q = 5, p = 409; q = 7, p = 193; q = 11, 193; q = 5, p = 17$, and $q = 13, p = 17$.

The statements of Theorems 20, 21 may be proved similarly to Theorem 17, 21.

VI. Note about the balanced biquadratic sequences

Let $q > 3$. We consider a sequence defined by

$$s_i = \begin{cases} 0, & \text{if } i \in H_0^{(4)} \cup \{0\}, \\ 1, & \text{if } i \bmod p \in H_1^{(4)}, \\ 2, & \text{if } i \bmod p \in H_2^{(4)}, \\ 3, & \text{if } i \bmod p \in H_3^{(4)}. \end{cases} \tag{15}$$

Theorem 22: Let $\{s_i\}$ be defined by (15) and $\left(\frac{p}{q}\right) = -1$. Then $LC_q(s) = p$.

Proof: Assume the converse that $LC_q(s) < p$. By definition, $S(1) = 3(p-1)/2$, so that there exist $v : S(\alpha^v) = 0, 1 \leq v < N$. We can assume without loss of generality that $v = 1$.

By the law of quadratic reciprocity we have

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

Since $p \equiv 1 (\mathrm{mod}\ 4)$, it follows that $\left(\frac{q}{p}\right) = -1$ and $q \notin H_0^{(4)} \cup H_2^{(4)}$. Thus, $q \in H_k^{(4)}, k = 1, 3$ and

$$0 = S^q(\alpha) = S(\alpha^q) = S_4(\alpha^{\theta^{k+1}}) + 2S_4(\alpha^{\theta^{k+2}}) + 3S_4(\alpha^{\theta^{k+3}}). \quad (16)$$

We consider two cases.

(i) Suppose $q \in H_1^{(4)}$; then $S_4^q(\alpha^j) = S_4(\alpha^{\theta j})$ and by (16) we have

$$\begin{cases} S_4(\alpha^\theta) + 2S_4(\alpha^{\theta^2}) + 3S_4(\alpha^{\theta^3}) = 0, \\ S_4(\alpha^{\theta^2}) + 2S_4(\alpha^{\theta^3}) + 3S_4(\alpha) = 0. \end{cases}$$

Subtracting we get $S_4(\alpha^\theta) + S_4(\alpha^{\theta^2}) + S_4(\alpha^{\theta^3}) - 3S_4(\alpha) = 0$ or $S_4(\alpha) = -1/4$ by (3). Therefore, since $S_4(\alpha)$ is a root of $w^2 - S_2(\alpha)w + S_2(\alpha)(x-1)/4 + (3p-1+2x)/16$ we obtain that $S_2(\alpha) \in \mathbb{F}_q$. And we have a contradiction with Corollary 6.

(ii) Let $q \in H_3^{(4)}$. In this case this theorem may be proved similarly as for $q \in H_1^{(4)}$.

■

The results of direct computing of the linear complexity by Berlekamp-Massey algorithm for $3 \le q \le 13, 5 \le p \le 6000$ confirm the results of Theorems 17- 22.

VII. Conclusion

We investigate the linear complexity and the minimal polynomial of the series of cyclotomic sequences of order three and four over the finite fields of different orders. In particular, we find the linear complexity and the minimal polynomial of the characteristic sequence of cubic residue class and biquadratic residue class and balanced cyclotomic sequences of order three.

Some analytical results giving the estimate of the designed distance of the cyclic codes based on the series of cyclotomic sequences of order four were proved in [2], [4], [9]. It may be interesting to study the cyclic codes based on sequences considered along the recent works.

References

[1] T.W. Cusick, C. Ding, A. Renvall. *Stream Ciphers and Number Theory*, North-Holland Publishing Co., Amsterdam 1998

[2] C. Ding, *Codes from Difference Sets*, World Scientific 2015

[3] C. Ding, H. Niederreiter, "Cyclotomic Linear Codes of Order 3", *IEEE Trans. on Inform. Theory*, vol. 53 (6), 2007, 2274- 2277.

[4] C. Ding, "Cyclic codes from cyclotomic sequences of order four", *Finite Fields Appl.*, vol. 23 (2013), 8-34

[5] V. A. Edemskii, "On the linear complexity of binary sequences on the basis of biquadratic and sextic residue classes", *Discret. Math. Appl.* vol. 20(1)(2010) 75-84; translation from Diskretn. Mat. vol. 22(4)(2010) 74-82.

[6] S.W. Golomb, G. Gong. *Signal Design for Good Correlation: For Wireless Communications, Cryptography and Radar Applications.* Cambridge University Press 2005

[7] D. H. Green, "Linear complexity of modulo-m power residue sequences", *IEE Proc., Comput. Digit. Tech.*, vol.151 (6), 2004, pp. 385-390.

[8] M. Hall. *Combinatorial Theory*, Wiley, New York 1975

[9] L. Hu, Q. Yue, X. Zhu, "Gauss periods and cyclic codes from cyclotomic sequences of small orders", *Journal of electronics (China)*, vol. 31 (6), 2014, 537-546.

[10] K. Ireland, M. Rosen. *A Classical Introduction to Modern Number Theory*, Springer, Berlin 1982

[11] R. Lidl, H. Niederreiter. *Finite Fields.* Addison-Wesley 1983

[12] G. Myerson, "Period polynomials and Gauss sums for finite fields", *Acta Arith.*, vol. 39, 1981, pp. 251-264.

[13] Q. Wang, "Some cyclic codes with prime length from cyclotomy of order 4", *Cryptogr. Commun.*, DOI 10.1007/s12095-016-0188-3

[14] Q. Wang, D. Lin, X. Guang, "On the Linear Complexity of Legendre Sequences Over F_q", I*EICE Trans. Fundamentals,* vol. E97-A (7)(2014) 1627- 1630.