About the Linear Complexity of Binary Sequences with Optimal Autocorrelation Value/Magnitude and Length $4p$

Vladimir Edemskiy

Abstract—We derive the linear complexity and the minimal polynomial over the finite fields of order two and p of series of binary sequences with a period $4p$ and optimal autocorrelation value/magnitude. These sequences are constructed by cyclotomic classes of order two, four and six by methods proposed by K.T. Arasu et al. and Y. Sun et al.

We define the parameters of sequences with optimal autocorrelation and high linear complexity.

Keywords—random sequences, autoregression model, uniform distribution

I. Introduction

THE autocorrelation is an important measure of pseudo-random sequences for their application in code-division multiple access systems, spread spectrum communication systems, radar systems and so on [9]. An important problem in sequence design is to find sequences with optimal autocorrelation. In the literature, a sequence is said to have optimal autocorrelation property if it satisfies one or two of the following conditions: P1. The maximal out-of-phase autocorrelation magnitude is as small as possible. P2. The number of occurrences of the maximal out-of-phase autocorrelation magnitude is as small as possible. If the sequence satisfies Condition P1, then it is referred to as a sequence with the optimal autocorrelation magnitude. Further, it is said to be a sequence with optimal autocorrelation value if it also satisfies Condition P2.

In their paper, Arasu et al.[1] investigated almost difference sets and constructed new classes of binary sequences of period $4n$ with optimal autocorrelation $\{0, -4\}$. These sequences have also been referred to as interleaved sequences. In particular, the cyclotomic classes may be used for the construction of this sequences. Sun et al. presented another construction method of binary sequences of period $4p$ with optimal autocorrelation magnitude as well [16]. The cyclotomic classes of order four were used in this case.

The linear complexity is another important characteristic of pseudo-random sequence significant for cryptographic applications [4]. 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 $2L$ consecutive digits of the sequence. Thus, it is reasonable to suggest that "good" sequences have $L > N/2$ (where N denotes the period of the sequence) [13]. The linear complexity of interleaved sequences over the finite field of order two was investigated in series of papers [14], [17], [18], [6] (see also references therein). Also, the linear complexity of Legendre sequences and other cyclotomic sequences of length p was derived in [2], [3] over the finite field $\mathbb{F}_p$.

In this paper we derive the linear complexity and the minimal polynomials of two families of binary sequences with the optimal autocorrelation value/magnitude and a period $4p$ obtained from the cyclotomic classes. The first family of sequences will be constructed from Legendre or Halls sextic residue sequences by the method presented in [1], i. e. these sequences will be constructed using the cyclotomic classes of order two or six. We investigate the linear complexity of these sequences over $\mathbb{F}_2$ and $\mathbb{F}_p$. In part, the study of linear complexity of sequences obtained from Legendre sequences was presented at the conference [7]. The second family of sequences is based on the cyclotomic classes of order four as in [16]. In this case, we only study the linear complexity of sequences over $\mathbb{F}_p$ because over $\mathbb{F}_2$ it was investigated earlier. A computation method for the linear complexity of generalized cyclotomic binary sequences of length $2^n p^k$ was derived in [8].

II. Preliminaries

First, we briefly repeat the basic definitions from [1] and some general information.

Let p be a prime of the form $p \equiv 1 (\bmod\ d)$, where d is an even integer, and let $R = (p-1)/d$, and g be a primitive root modulo p [11]. Here and hereafter $g \bmod p$ denotes the least nonnegative integer that is congruent to g modulo p. Then the integers $\bmod p$ can be partitioned into d cosets $H_i, 0 \le i \le d-1$, each containing R elements, such that H_0 contains the dth power residues $\bmod p$, and the remaining H_i are formed from $g^i H_0$. Cosets H_i are also called the cyclotomic classes of order d with respect to p [4].

The ring residue classes $\mathbb{Z}_{4n} \cong \mathbb{Z}_4 \times \mathbb{Z}_n$ relative to isomorphism $\phi(a) = (a \bmod 4, a \bmod n)$ [11]. In [1] a new family of binary sequences with optimal autocorrelation is defined as

$$s_i = \begin{cases} 1, & \text{if } i \bmod 4n \in C; \\ 0, & \text{if } i \bmod 4n \notin C, \end{cases} \tag{1}$$

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.

for

$$C = \phi^{-1}\big(\{0\} \times C_0 \cup \{1\} \times (C_0 - \delta)^* \cup \{2\} \times C_0^* \cup \{3\} \times (C_0 - \delta)^*\big)$$

where C_0 is the support of binary sequences of period n with optimal autocorrelation, C_0^* and $(C_0 - \delta)^*$ denote the complements of C_0 and $(C_0 - \delta)$ in $\mathbb{Z}_n$, respectively; $0 \le \delta \le n-1$.

In this paper we consider only the case when C_0 is a support of a Legendre sequence or Halls sextic residue sequence. In this case $n = p$ where p is an odd prime and $p \equiv 3(\mathrm{mod}4)$ [10]. For $p = 3$ we can suppose that $\delta = 0, 1, 2$.

It is well known [4] that if $\{s_i\}$ is a binary sequence with period N, then the minimal polynomial $m(x)$ and the linear complexity L of this sequence is defined by

$$m(x) = (x^N - 1)/\gcd\big(x^N - 1, S(x)\big), \qquad L = N - \deg\gcd\big(x^N - 1, S(x)\big),$$

where $S(x) = s_0 + s_1 x + ... + s_{N-1}x^{N-1}$.

In our case $N = 4p$, hence over $\mathbb{F}_2$ we have

$$L = 4p - \deg\gcd\left((x^p - 1)^4, S(x)\right). \tag{2}$$

So, by (2), to compute the minimal polynomial and the linear complexity of $\{s_i\}$ it is sufficient to know the greatest common divisor of two polynomials. But first we need to prove intermediate lemmas.

A. Auxiliary lemmas

Let G be a subset of the residue class ring $\mathbb{Z}_{4p}$, and b be an element of $\mathbb{Z}$. Define

$$bG = \{ba \mod 4p | a \in G\}, \qquad G + b = \{(a + b) \mod 4p | a \in G\}.$$

Let C_1 be a compliment of C_0 in $\mathbb{Z}_p^*$. Then Lemma 1 follows from our definitions.

Lemma 1: (i) $\phi^{-1}\big(\{0\} \times C_m\big) + kp = \phi^{-1}\big(\{kp \bmod 4\} \times C_m\big)$, $m = 0, 1; k = 0, \ldots, 3$;

(ii) $\phi^{-1}\big(\{1\} \times (C_0 - \delta)^*\big) = \big(\phi^{-1}\big(\{0\} \times C_1\big) + 3p - \delta(p+1)\big) \cup \{3p - \delta(p+1)\}$;

(iii) $\phi^{-1}\big(\{3\} \times (C_0 - \delta)^*\big) = \big(\phi^{-1}\big(\{0\} \times C_1\big) + p - \delta(p+1)\big) \cup \{p - \delta(p+1)\}$.

Proof: We will prove the statement (ii). Let a belong to $\big(\phi^{-1}\big(\{0\} \times C_1\big) + 3p - \delta(p+1)\big) \cup \{3p - \delta(p+1)\}$. Since $p \equiv 3(\mathrm{mod}4)$, it follows that $a \equiv 1(\mathrm{mod}\ 4)$. Further, $a \equiv (b - \delta)(\mathrm{mod}\ p)$ where $b \in C_1$ or $a \equiv -\delta(\mathrm{mod}\ p)$. Hence, $a \bmod p \in (C_0 - \delta)^*$ and

$$\big(\phi^{-1}\big(\{0\} \times C_1\big) + 3p - \delta(p+1)\big) \cup \{3p - \delta(p+1)\} \subset \phi^{-1}\big(\{1\} \times (C_0 - \delta)^*\big).$$

Since the orders of the sets on both sides of the above inclusion are equal, it follows that the proposition (ii) is now established.

The propositions (i) and (iii) we can prove similarly as (ii). ■

By definition, put $B_m = \phi^{-1}(\{0\} \times C_m), m = 0, 1$. Let us introduce the auxiliary polynomials $E_m(x) = \sum_{i \in B_m} x^i$. The following assertion follows immediately from Lemma 1.

Lemma 2: Let $\{s_i\}$ be defined by (1). Then

$$S(x) \equiv \big(E_0(x) + (E_1(x) + 1) \times \left(x^{3p - \delta(p+1)} + x^{2p} + x^{p - \delta(p+1)}\right)(\mathrm{mod}(x^{4p} - 1)). \tag{3}$$

III. The linear complexity of sequences obtained from Legendre sequences

In this section we consider sequences with optimal autocorrelation value obtained from Legendre sequences [1].

Let $d = 2, p \equiv 3(\mathrm{\ mod\ }4)$. The Legendre sequence $l = \{l_i\}$ of period p is defined by

$$l_i = \begin{cases} 1, & \text{if } i \in H_0, \\ 0, & \text{otherwise}. \end{cases}$$

It is well known that Legendre binary sequences have optimal autocorrelation value if $p \equiv 3(\mathrm{mod}4)$.

Theorem 3: Let C_0 be a support of the Legendre sequence, and let $\{s_i\}$ be defined by (1). Then the linear complexity over $\mathbb{F}_2$ of $\{s_i\}$ is equal to

$$L = \begin{cases} 2p + 2, & \text{if } p \equiv \pm 3(\mathrm{mod}\ 8) \text{ and } \delta \neq 0, \\ p + 3, & \text{if } p \equiv \pm 1(\mathrm{mod}\ 8) \text{ and } \delta \neq 0, \\ & \text{or } p \equiv \pm 3(\mathrm{mod}\ 8) \text{ and } \delta = 0, \\ (p+7)/2, & \text{if } p \equiv \pm 1(\mathrm{mod}\ 8) \text{ and } \delta = 0. \end{cases}$$

Proof: Using (3) we see over $\mathbb{F}_2$ that $S(x) = E_0(x) + (E_1(x)+1)(x^{3p-\delta(p+1)} + x^{2p} + x^{p-\delta(p+1)} + 1) + E_1(x) + 1$ or $S(x) = E_0(x) + E_1(x) + 1 + (x^{2p}+1)(x^{p-\delta(p+1)}+1)(E_1(x)+1)$.

From our definitions it follows that $E_0(1) + E_1(1) + 1 = 1$ and $E_0(x) + E_1(x) + 1 = ((x^p - 1)/(x-1))^4$. Hence

$$\gcd\left((x^p - 1)^4, S(x)\right) = ((x^p - 1)/(x-1))^2 \gcd\left((x^p - 1)^2, E_1(x) + 1\right) \tag{4}$$

for $\delta \neq 0$ and

$$\gcd\left((x^p - 1)^4, S(x)\right) = ((x^p - 1)/(x-1))^3 \gcd\left((x^p - 1), E_1(x) + 1\right) \tag{5}$$

for $\delta = 0$.

The linear complexity of Legendre sequences was investigated in [5]. Let α be a primitive p-th root of unity in the extension of the field $\mathbb{F}_2$. Since $E_1(x) = \sum_{i \in \phi^{-1}(\{0\} \times H_1)} x^i$, it follows that $E_1(\alpha^j) = \sum_{i \in H_1} \alpha^{ji}$. Therefore, by [5] we have

$$\deg\gcd\left(x^p - 1, E_1(x) + 1\right) = \begin{cases} 0, & \text{if } p \equiv \pm 3(\mathrm{mod}\ 8), \\ (p-1)/2, & \text{if } p \equiv \pm 1(\mathrm{mod}\ 8). \end{cases}$$

The conclusion of this theorem then follows from (4), (5) and (2). ■

Without loss of generality, we can assume that $\sum_{i \in H_0} \alpha^i \neq 0$. From the proof of Theorem 3 we can establish that $m(x) =$

$(x^p-1)^2(x-1)^2$ if $p \equiv \pm 3 (\mathrm{mod}\ 8)$ and $\delta \neq 0$; $m(x) = (x^p-1)(x-1)^3$ if $p \equiv \pm 3 (\mathrm{mod}\ 8)$ and $\delta = 0$; $m(x) = (x-1)^4 \prod_{i \in H_0}(x-\alpha^i)^2$ if $p \equiv \pm 1 (\mathrm{mod}\ 8)$ and $\delta \neq 0$; $m(x) = (x-1)^4 \prod_{i \in H_0}(x-\alpha^i)$ if $p \equiv \pm 1 (\mathrm{mod}\ 8)$ and $\delta = 0$.

By Theorem 3 sequence s have high linear complexity only for $p \equiv \pm 3 (\mathrm{mod}\ 8)$ and $\delta \neq 0$.

Now, we derive the linear complexity of these sequences over $\mathbb{F}_p$. We use Günther-Blahut theorem to calculate the linear complexity over $\mathbb{F}_p$ of $\{s_i\}$ with a period $4p$ (see, for example [15]).

Theorem 4: Let C_0 be a support of the Legendre sequence, and let $\{s_i\}$ be defined by (1). Then the linear complexity over $\mathbb{F}_p$ of $\{s_i\}$ is equal to $4p$ and $m(x) = x^{4p} - 1$.

Proof: Let β be a primitive root 4th power of unity in an extension of $\mathbb{F}_p$. Since $E_0(\beta) = E_1(\beta) = (p-1)/2$, it follows from (3) that $S(\beta) = (p-1)/2 + (p+1)/2(\beta^3+\beta^2+\beta) = -1$. Similarly, we obtain that $S(1) \neq 0$, $S(-1) \neq 0$, $S(-\beta) \neq 0$. So, the statement of Theorem 4 follows from Günther-Blahut theorem. ∎

The results of computing the linear complexity by Berlekamp-Massey algorithm when $p = 3, 7, 11, 19, 23, 31, 43, 47, \ldots$ confirm Theorems 3 and 4.

Remark 5: If C_0 is a support of the m-sequence of length $2^n - 1 = p$ and $\{s_i\}$ is defined by (1) then by (4) and (5) we obtain that $\{s_i\}$ does not have high linear complexity.

IV. The linear complexity of sequences obtained from Hall's sextic residue sequences

Here we study sequences with optimal autocorrelation value obtained from Hall's sextic residue sequences [1].

Let $d = 6$, $p = A^2 + 27, A \equiv 1 (\mathrm{mod}\ 3)$ and let $H = H_0 \cup H_1 \cup H_3$ be a Hall's difference set [10]. Denote by h a Hall's sextic residue sequence, i.e.

$$h_i = \begin{cases} 1, & \text{if } i \bmod p \in H, \\ 0, & \text{else.} \end{cases}$$

It is well known that Hall's sextic residue sequences have optimal autocorrelation value.

The linear complexity of Hall's sextic residue sequences over $\mathbb{F}_2$ was investigated in [12]. By [12] we can choose α (as before, α is a primitive p-th root of unity in the extension of the field $\mathbb{F}_2$) such that

$$\gcd(x^p - 1, E_1(x) + 1) = \gcd(x^p - 1, E_0(x)) \begin{cases} 1, & \text{if } p \equiv \pm 3 (\mathrm{mod}\ 8), \\ \prod_{i \notin H_0 \cup \{0\}}(x - \alpha^i), & \text{if } p \equiv \pm 1 (\mathrm{mod}\ 8). \end{cases}$$

The linear complexity of Hall's sextic residue sequences over $\mathbb{F}_p$ was investigated in [3].

The following theorems may be proved similarly as Theorems 3 and 4.

Theorem 6: Let C_0 be a support of Hall's sextic residue sequence, and let $\{s_i\}$ be defined by (1). Then the linear complexity over $\mathbb{F}_2$ of $\{s_i\}$ is equal to

$$L = \begin{cases} 2p+2, & \text{if } p \equiv 3 (\mathrm{mod}\ 8) \text{ and } \delta \neq 0, \\ p+3, & \text{if } p \equiv 3 (\mathrm{mod}\ 8) \text{ and } \delta = 0, \\ (p+11)/3 & \text{if } p \equiv 7 (\mathrm{mod}\ 8) \text{ and } \delta \neq 0, \\ (p+23)/6, & \text{if } p \equiv 7 (\mathrm{mod}\ 8) \text{ and } \delta = 0. \end{cases}$$

In this case $m(x) = (x^p-1)^2(x-1)^2$ if $p \equiv 3 (\mathrm{mod}\ 8)$ and $\delta \neq 0$; $m(x) = (x^p-1)(x-1)^3$ if $p \equiv 3 (\mathrm{mod}\ 8)$ and $\delta = 0$; $m(x) = (x-1)^4 \prod_{i \in H_0}(x-\alpha^i)^2$ if $p \equiv 1 (\mathrm{mod}\ 8)$ and $\delta \neq 0$; $m(x) = (x-1)^4 \prod_{i \in H_0}(x-\alpha^i)$ if $p \equiv 1 (\mathrm{mod}\ 8)$ and $\delta = 0$.

Theorem 7: Let C_0 be a support of Hall's sextic residue sequence, and let $\{s_i\}$ be defined by (1). Then the linear complexity over $\mathbb{F}_p$ of $\{s_i\}$ is equal to $4p$ and $m(x) = x^{4p} - 1$.

The results of computing the linear complexity by Berlekamp-Massey algorithm when $p = 43, 283; p = 31, 127, 223, \ldots$ confirm Theorems 6 and 7.

In conclusion section we note that if $\{s_i\}$ equals the product of the binary sequence of length 4 with ideal autocorrelation and the Legendre sequence or Hall's sextic residue sequence, i.e., $C = \phi^{-1}(\{0,1,2\} \times C_0 \cup \{3\} \times (C_1 \cup \{0\}))$ then $S(x) \equiv (1 + x^p + x^{2p})E_0(x) + x^{3p}E_1(x) + x^{3p} (\mathrm{mod}\ (x^{4p} - 1))$. In this case $S(\beta^i) \neq 0, i = 0, 1, 2, 4$ and $L = 4p$ over $\mathbb{F}_p$. But over $\mathbb{F}_2$ we have $S(x) \equiv (x^p - 1)^3 E_0(x) + x^{3p} \left((x^p-1)/(x-1)\right)^4 (\mathrm{mod}\,(x^{4p}-1))$. Hence, here $L \leq p + 3$.

V. The linear complexity of sequences obtained from biquadratic residues

One more approach to design of binary sequences of period $4p$ with optimal autocorrelation magnitude was suggested in [16].

Let $d = 4$, $p \equiv 5 (\mathrm{mod}\ 8)$, and p has a quadratic partition of the form $p = x^2 + 4$. Here x is an integer and $x \equiv 1 (\mathrm{mod}\ 4)$.

Let the sequence $\{s_i\}$ be defined by

$$s_i = \begin{cases} 1, & \text{if } i \mod 4p \in C, \\ 0, & \text{if } i \mod 4p \notin C, \end{cases}$$

for

$$C = \phi^{-1}\big(\{0\} \times (H_{j_1} \cup H_{j_2}) \cup \{1\} \times (H_{j_1} \cup H_{j_2}) \cup \{2\} \times (H_{j_1} \cup H_{j_3}) \cup \{3\} \times (H_{j_2} \cup H_{j_4}) \cup \{0,2\}\big)$$

where j_1, j_2, j_3 and j_4 are pairwise distinct integers between 0 and 3. In their paper [16], Y. Sun et al. derive the values (j, m, n, k) for which $\{s_i\}$ have the optimal autocorrelation magnitude.

Here we only derive the linear complexity of sequence defined by

$$s_i = \begin{cases} 1, & \text{if } i \mod 4p \in C; \\ 0, & \text{if } i \mod 4p \notin C, \end{cases} \tag{6}$$

for

$$C = \phi^{-1}\big(\{0,1\} \times (H_0 \cup H_1) \cup \{2\} \times (H_0 \cup H_3) \cup \{3\} \times (H_1 \cup H_2) \cup \{0,2\}\big).$$

The other cases are similar.

Put, by definition $D_m = \phi^{-1}(\{0\} \times H_m)$. Let us introduce the auxiliary polynomials $F_m(x) = \sum_{i \in D_m} x^i, m = 0, 1, 2, 3$. Hence, in this case by Lemma 1 for $S(x) = \sum_{i \in C} x^i$ we obtain that

$$S(x) \equiv T(x) (\mathrm{mod}(x^{4p} - 1)) \tag{7}$$

where

$$T(x) = (1 + x^p + x^{2p})F_0(x) + (1 + x^p + x^{3p})F_1(x) + x^{2p}F_3(x) + x^{3p}F_2(x) + 1 + x^{2p}.$$

In the following subsection we prove a few propositions about $F_m(x)$ and $F_m^{(n)}(x)$, where $F_m^{(n)}(x)$ is a formal derivative of order n of the polynomial $F_m(x)$.

A. Auxiliary lemmas

Let us introduce the auxiliary polynomials $T_{m,0}(x) = F_m(x)$, $T_{m,1}(x) = xF_m^{'}(x)$ and $T_{m,n}(x) = xT_{n-1}^{'}(x), m = 0, 1, 2, 3; n = 2, 3. \ldots$. Then $T_{m,n}(x) = \sum_{i \in D_m} i^n x^i$ and

$$x^n F_m^{(n)}(x) = T_{m,n}(x) - \sum_{j=1}^{n-1} a_{j,n}(x) F_m^{(j)}(x), \tag{8}$$

where $a_{j,n}(x)$ are polynomials.

Lemma 8: Let β be a primitive root of 4th power of unity in $\mathbb{F}_p$, $1 \le n \le p-1$ and $0 \le m \le 3$. Then

$$T_{m,n}(\beta^j) = \begin{cases} 0, & \text{if } n \not\equiv 0 (\mathrm{mod}(p-1)/4), \\ g^{mn}(p-1)/4, & \text{if } n \equiv 0 (\mathrm{mod}(p-1)/4). \end{cases}$$

Proof: Since $D_m = \phi^{-1}(\{0\} \times H_m)$ and $\beta^4 = 1$ in $\mathbb{F}_p$, it follows that $T_{m,n}(\beta^j) = \sum_{i \in D_m} i^n \beta^{ji} = \sum_{i \in D_m} i^n = \sum_{i \in H_m} i^n, n = 1, 2, \ldots$. By definitions of H_m we obtain that

$$T_{m,n}(\beta^j) = \sum_{t=0}^{R-1} g^{(m+4t)n}, n = 1, 2, \ldots.$$

If $n \equiv 0 (\mathrm{mod}(p-1)/4)$ then $T_{m,n}(\beta^j) = g^{mn}(p-1)/4$. Suppose $n \not\equiv 0 (\mathrm{mod}(p-1)/4)$; denote $\sum_{i \in H_0} i^n$ by B. Since $g \bmod p$ is a primitive root modulo p, it follows that

$$0 = \sum_{j=1}^{p-1} j^n = \sum_{t=0}^{3} \sum_{i \in H_t} i^n = B + g^n B + g^{2n} B + g^{3n} B = B(g^{4n} - 1)/(g^n - 1).$$

Hence, $B = 0$ and $\sum_{i \in H_m} i^n = 0$. ∎

Corollary 9: If $1 \le n < (p-1)/4$ then $F_m^{(n)}(\beta^j) = 0$ and $\beta^{j(p-1)/4} F_m^{(n)}(\beta^j) = g^{m(p-1)/4}(p-1)/4, j = 0, 1, 2, 3$.

Theorem 10: Let the balanced binary sequences $\{s_i\}$ be defined by (6). Then $L = (11p + 5)/4$ over $\mathbb{F}_p$.

Proof: If $p \equiv 1 (\mathrm{mod}\ 4)$ then β belongs to $\mathbb{F}_p$. Hence, without loss of generality, we can assume that $\beta = g^{(p-1)/4}$. By Günther-Blahut theorem, to prove the assertion it suffices to find for $S(x)$ the multiplicity of roots $\pm 1, \pm\beta$. By definition and (7) we have $S(1) = S(\beta) = S(-\beta) = 0, S(-1) = 2$.

Further, since over $\mathbb{F}_p$

$$T^{(n)}(x) = (1 + x^p + x^{2p})F_0^{(n)}(x) + (1 + x^p + x^{3p})F_1^{(n)}(x) + x^{3p}F_2^{(n)}(x) + x^{2p}F_3^{(n)}(x).$$

or

$$x^n T^{(n)}(x) = (1 + x^p + x^{2p})x^n F_0^{(n)}(x) + (1 + x^p + x^{3p})x^n F_1^{(n)}(x) + x^{3p}x^n F_2^{(n)}(x) + x^{2p}x^n F_3^{(n)}(x), \tag{9}$$

by Corollary 9, (8), and Lemma 8 it follows that:

(i) $T^{(n)}(1) = 0$ for $1 \le n \le (p-5)/4$ and $T^{((p-1)/4)}(1) = (1 + \beta)(p-1)/2 \ne 0$;

(ii) $T^{(n)}(\beta) = 0$ for $1 \le n \le (p-5)/4$ and $\beta^{((p-1)/4)} T^{((p-1)/4)}(\beta) = \beta(p-1)$;

(iii) $T^{(n)}(-\beta) = 0$ for $1 \le n \le (p-5)/4$ and $T^{((p-1)/4)}(-\beta) = 0$.

So, the multiplicity of roots 1 and β is equal to $(p-1)/4$. The root $-\beta$ requires the additional study.

Using (8) we obtain from (9) that

$$x^n T^{(n)}(x) = (1 + x^p + x^{2p})T_{m,1}(x) + (1 + x^p + x^{3p})T_{m,2}(x) + x^{3p}T_{m,2}(x) + x^{2p}T_{m,3}(x) - x^n \sum_{j=1}^{n-1} a_{j,n}(x) T^{(j)}(x).$$

Hence, if $T^{((p-1)/4)}(-\beta) = 0$ then $T^{(j)}(-\beta) = 0$ for $(p-1)/4 < j < (p-1)/2$ by Lemma 2.

Further, by (9) and Lemma 8 $T^{((p-1)/2)}(-\beta) = 0$ and $\beta^{(3(p-1)/4)} T^{(3(p-1)/4)}(-\beta) = -\beta(p-1)$.

From this we can establish that the multiplicity of root $-\beta$ is equal to $3(p-1)/4$. This completes the proof of Theorem 10. ∎

Using the proof of Theorem 10 we can write that

$$m(x) = (x+1)^p \big((x-1)(x-\beta)\big)^{(3p+1)/4} (x+\beta)^{(p+3)/4} = (x+1)^p (x^2+1)^{(p+3)/4} \left(x - g^{(p-1)/2}\right)^{(p-1)/2}.$$

The minimal polynomial of sequence depends on the choice of g because the definition of sequence depends on the choice of g.

The results of computing the linear complexity by Berlekamp-Massey algorithm when $p = 5, 13, 29, 53, 173, 229, 293, \ldots$ confirm Theorem 10.

VI. Conclusion

In this paper we examine the linear complexity of binary sequences with optimal autocorrelation value/magnitude and a period $4p$ constructed on cyclotomic classes. First, we derive the linear complexity of binary sequences obtained from Legendre or Hall's sextic sequences. These sequences of length $4p$ with optimal autocorrelation were constructed by method proposed by Arasu et al.[1]. Second, we investigate the linear complexity of binary sequences of length $4p$ with optimal autocorrelation magnitude obtained from the cyclotomic classes of order four [16].

We determine the parameters of sequences with optimal autocorrelation and high linear complexity.

REFERENCES

[1] K.T. Arasu, C. Ding, T. Hellesenh, P. V. Kumar, H.M. Martinsen. "Almost difference sets and their sequences with optimal autocorrelation". *IEEE transactions on information theory.* vol. 47, 7, pp. 2934-2943, 2001.

[2] H. Aly, A. Winterhof. "On the k-error linear complexity over F_p of Legendre and Sidelnikov sequences". *Des Codes Crypt.,* vol.40, pp. 369-374, 2006.

[3] H. Aly, W. Meidl,A. Winterhof. "On the k-Error Linear Complexity of Cyclotomic sequences". *J. Math. Crypt.*, vol.1, pp.1-14, 2007.

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

[5] C. Ding, T. Helleseth, W. Shan. "On the Linear Complexity of Legendre Sequences", *IEEE Trans. Info Theory,* vol. IT-44, pp. 1276 - 1278, 1998.

[6] V. Edemskiy. "On the linear complexity of interleaved binary sequences of period 4p obtained from Hall sequences or Legendre and Hall sequences". *Electronics Letters.*, vol.50. Issue 8, p. 604-605, 2014.

[7] V. Edemskiy. "The Linear Complexity over F_2 and F_p of Binary Sequences of Length $4p$ with Optimal Autocorrelation". *Proc. of the 2015 International Conference on Pure Mathematics, Applied Mathematics and Computational Methods (PMAMCM 2015)*, Zakynthos Island, Greece, July 16-20, 2015, pp. 42-44.

[8] V. Edemskiy, O. Antonova. The linear complexity and the autocorrelation of generalized cyclotomic binary sequences of length $2^n p^m$. *In proc. of the 1-st International Conference on Mathematical Methods & Computational Techniques in Science & Engineering (MMCSTSE 2014)*, Athens, Greece, November 28-30, 2014, pp. 29-33.

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

[10] M. Hall.*Combinatorial Theory*, Wiley, New York (1975)

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

[12] J.H. Kim, H.Y. Song. "On the linear complexity of Hall's sextic residue sequences". *IEEE Trans. Inf. Theory*, vol. 47 (5), p. 2094-2096, 2001.

[13] R. Lidl, H. Niederreiter. *Finite Fields.* Addison-Wesley (1983).

[14] N. Li, X. Tang."On the linear complexity of binary sequences of period $4N$ with optimal autocorrelation value/magnitude", *IEEE Trans. Inf. Theory*, vol.57, pp. 7597-7604.

[15] J.L. Massey, S. Serconek. "Linear complexity of periodic Sequences: A General Theory". *Journal of Complexity* . Lecture Notes in Computer Science. pp. 358–371, 1996.

[16] Y. Sun, H. Shen. "New Binary Sequences of Length 4p with Optimal Autocorrelation Magnitude". *Ars Combinatoria (A Canadian Journal of Combinatorics)*, Vol. LXXXIX (89), pp. 255-262, 2008.

[17] Q. Wang, X. N. Du. "The linear complexity of binary sequences with optimal autocorrelation", *IEEE Trans. Inf. Theory*, vol. 56, pp. 6388-6397, 2010.

[18] H. Xiong, L. Qu, C. Li, S. Fu. "Linear complexity of binary sequences with interleaved structure", *IET Communications*, vol. 7(15), pp. 1688-1696, 2013.