The evaluation of the linear complexity and the autocorrelation of generalized cyclotomic binary sequences of length $2^n p^m$

Vladimir Edemskiy, Olga Antonova

***Abstract*—In this article, we discuss a computation method for the linear complexity of generalized cyclotomic binary sequences of length $2^n p^m$. This method allows to assess the linear complexity of above-mentioned sequences and to design the sequences with high linear complexity. Also we generalize known results about binary sequences of length $2p^m$. In conclusion we evaluate the autocorrelation of generalized cyclotomic binary sequences of length $2^n p^m$. In most cases these sequences have high linear complexity and poor autocorrelation performance.**

***Index Terms*—Autocorrelation, linear complexity, generalized cyclotomic binary sequences**

I. Introduction

THE linear complexity of a sequence is an important characteristic of its quality. The linear complexity may be defined as the length of the shortest linear feedback shift register that is capable of generating the sequence [16]. Knowledge of just $2L$ consecutive digits of the sequence is sufficient to enable the remainder of the sequence to be constructed (about nonlinear feedback shift register see [1], [2] and also references therein). Thus, it is reasonable to suggest that 'good' sequences have $L > N/2$ (where N denotes the period of the sequence) [3], [18]. The autocorrelation is also important for many practical applications [3], [11].

Classical cyclotomic classes and generalized cyclotomic classes can be used to construct binary sequences, which are called classical cyclotomic sequences and generalized cyclotomic sequences, respectively [3]. C. Ding and T. Helleseth first introduced a new generalized cyclotomy of order 2 with respect to $p_1^{e_1} \dots p_t^{e_t}$, which included classical cyclotomy as a special case, and subsequently showed how to design binary sequences based on this new construction. T. Yan et al. [19], Y. J. Kim et al. [15], and S. Y. Jin et al. [13] studied the linear complexity and autocorrelation properties of generalized cyclotomic binary sequences of length p^m (see, also the article [6]).

J. W. Zhang et al. [20] proposed two generalized cyclotomic sequences of length $2p^m$ with high linear complexity. The results of J. W. Zhang et al. were generalized in [7]. Later, P. Ke et al. [14] represented new generalized cyclotomic binary sequences with period $2p^m$, which included constructions proposed by J. W. Zhang [20] as a special case. P.Ke et al. [14] discussed sequences defined by vector.

In this paper we discuss a computation method for the linear complexity of generalized cyclotomic binary sequences of length $2^n p^m$ and evaluate the linear complexity and the autocorrelation of generalized cyclotomic binary sequences of length $2^n p^m$. In particular, we consider the sequences of length $2p^m$ defined by two vectors. We show that in this case the pattern noted by P. Ke et al [14] persists. In most examined cases new generalized cyclotomic binary sequences have high linear complexity, but do not have desirable autocorrelation properties. We generalize results presented in [7]–[9], [14], [20].

II. The definition of the generalized cyclotomic sequences

Let p be an odd prime, and let d be an even divisor $p-1$. Denote $H_k = \{\theta^{k+td} \mod p^m,\ t = 1, 2, \dots, (p-1)/d\}, k = 0, 1, \dots, d-1$. Here and hereafter θ denotes a primitive root modulo p^m, where m is a positive integer [12] and $a \bmod p$ denotes the least nonnegative integer that is congruent to a modulo p. Then $H_k, k = 0, 1, \dots, d-1$ are generalized cyclotomic classes of order d with respect to p^m [4].

If A is a subset of $\mathbb{Z}_{p^m}$, then let us put by definition $bA = \{ba \mod p^m | a \in A\}$ and $b + A = \{(b+a) \mod p^m | a \in A\}$, where $b \in \mathbb{Z}$.

Then, we have partitions

$$\mathbb{Z}_{p^m}^* = \bigcup_{i=0}^{d-1} H_i \text{ and } \mathbb{Z}_{p^m} = \bigcup_{k=0}^{m-1} \bigcup_{i=0}^{d-1} p^k H_i \cup \{0\}. \qquad (1)$$

Let $N = 2^n p^m$, where n is a positive integer. The ring residue classes $\mathbb{Z}_N \cong \mathbb{Z}_{2^n} \times \mathbb{Z}_{p^m}$ relative to isomorphism $\phi(a) = (a \mod 2^n, a \mod p^m)$ [12]. Let $L_j = (I_0^{(j)}, I_1^{(j)}, \dots, I_{m-1}^{(j)})$, $j = 0, 1, \dots, 2^n - 1$, where $I_i^{(j)}, i = 0, 1, \dots, m-1$ are subsets of set $\{0, 1, \dots, d-1\}$ and $|I_i^{(j)}| = d/2$. Denote $E_j = \bigcup_{k=0}^{m-1} \bigcup_{i \in I_i^{(j)}} p^k H_i$, $C_j = \phi^{-1}(\{j\} \times E_j)$.

By definition, put

$$C = \bigcup_{j=0}^{2^n-1} C_j \cup \{0, 2p^m, \dots, (2^n-2)p^m\} \text{ and } \widetilde{C} = \mathbb{Z}_N \setminus C.$$

V. Edemskiy is with the Department of Applied Mathematics and Information Science, Novgorod State University, Veliky Novgorod, Russia, 173003 e-mail: Vladimir.Edemsky@novsu.ru.

O. Antonova is with Novgorod State University. e-mail: antonova2906@yandex.ru

This work was supported by the Ministry of Education and Science of Russia as a part of state-sponsored project.

The generalized cyclotomic binary sequence $S = \{s_i\}$ of length $2^n p^m$ is then defined by

$$s_i = \begin{cases} 1, & \text{if } i \mod N \in C; \\ 0, & \text{if } i \mod N \in \widetilde{C}. \end{cases} \tag{2}$$

The sequence S is balanced by (1) and the definition.

In the particular case, when $d = 2$ we can consider $\{L_j, j = 0, 1, \dots, 2^n - 1\}$ as a set of any fixed binary vectors in $\mathbb{Z}_2^m$, i.e. $L_j = (i_0^{(j)}, i_1^{(j)}, \dots, i_{m-1}^{(j)})$, $j = 0, 1, \dots, 2^n - 1$.

If g is an odd from integers θ and $\theta + p^m$, then g is a primitive root modulo $2p^m$ [12]. Let $D_j = \{g^{j+2t} \mod 2p^m; t = 0, \dots, p^{m-1}(p-1)/2 - 1\}$, $j = 0, 1$ be cyclotomic classes modulo $2p^m$, and let $\text{ind}_\theta 2$ be a discrete logarithm of 2 base θ in the field $GF(p)$. It is easy to see that $D_j = \phi^{-1}(\{1\} \times H_j)$ and $2D_j = \phi^{-1}\big(\{0\} \times H_{(j+\text{ind}_\theta 2) \mod 2}\big)$. Hence, binary sequences proposed by J.W. Zhang [20] and P. Ke [14] are special cases of S. They were obtained for $L_1 = (1, \dots, 1)$ and $L_0 = (1, \dots, 1)$ or $L_0 = (0, \dots, 0)$ [20], also for $L_0 = L_1 = \mathcal{L}$ [14].

In the next sections we consider a computation method for the linear complexity of S. Also we evaluate the linear complexity and the autocorrelation function of S.

III. A computation method for the linear complexity of generalized cyclotomic sequences of length $2^n p^m$

It is well known ([3], [16]) 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

$$m(x) = (x^N - 1)/\big(\gcd(x^N - 1, S(x))\big),$$
$$L = N - \deg\big(\gcd(x^N - 1, S(x))\big), \tag{3}$$

where $S(x) = s_0 + s_1 x + ... + s_{N-1} x^{N-1}$, $S(x) \in GF(2)[x]$.

In our case $N = 2^n p^m$, hence we have $x^{2^n p^m} - 1 = (x^{p^m} - 1)^{2^n}$ in the ring $GF(2)[x]$ and

$$L = N - \deg\Big(\gcd\Big((x^{p^m} - 1)^{2^n}, S(x)\Big)\Big). \tag{4}$$

Let α be a primitive root of order p^m of unity in the extension of the field $GF(2)$. Then, according to (3) and (4), in order to find the minimal polynomial and the linear complexity of S it is sufficient to find the zeros of $S(x)$ in the set $\{\alpha^v, v = 0, 1, \dots, p^m - 1\}$ and determine their multiplicity.

Let us introduce auxiliary polynomials $S_k(x) = \sum_{i \in p^k H_0} x^i$, $k = 0, 1, \dots, m - 1$.

Lemma 1: If $v \in \mathbb{Z}$, then

$$\sum_{u \in \phi^{-1}(\{l\} \times p^k H_f)} \alpha^{vu} = S_k(\alpha^{v\theta^f})$$

for all $l = 0, 1, ..., 2^n - 1$ and $k = 0, 1, ..., m - 1$.

Proof: By definition of α we have $\alpha^u = \alpha^{u \mod p^m}$. Since $\big\{u \mod p^m \mid u \in \phi^{-1}\big(\{l\} \times p^k H_f\big)\big\} = p^k H_f$ and $H_f = \theta^f H_0$, then Lemma 1 is proved. ■

By Lemma 1 and the definition of the sequence S we obtain that

$$S(\alpha^v) = \sum_{j=0}^{2^n-1} \sum_{k=0}^{m-1} \sum_{i \in I_k^{(j)}} S_k(\alpha^{v\theta^i}) + 2^{n-1}. \tag{5}$$

The method of computing the values $S_k(\alpha^v)$ by using explicit formulas for the cyclotomic numbers was proposed in [6] ($d = 3, 4, 6, 8$). So, by formulas (5) and (2) we can derive the linear complexity and the minimal polynomial of S for any set of subsets $I_k^{(j)}, k = 0, 1, \dots, m - 1, \quad j = 0, 1, \dots, 2^n - 1$.

Now we consider an example of using formula (5). Ding et al. [10] examined binary sequences with period $2p, p \equiv 1(\text{mod}4)$ and optimal three-level autocorrelation function. If $p \equiv 1(\text{mod}4)$ then $p = x^2 + 4y^2, \ x \equiv 1(\text{mod}4)$ [16] where x, y are integers.

Lemma 2: If the binary sequence S defined by (2) for $m = n = 1$, $d = 4$, and $L_0 = \{i, j\}, L_1 = \{l, j\}$, i, j, l are various indices from zero to three, then the linear complexity of S is $L = 2p$, if $y \equiv 1(\text{mod } 2)$ or $y \equiv 2(\text{mod } 4), |i - l| \neq 2$, and $L = (3p + 1)/2$ otherwise.

Proof: By (5),

$$S(\alpha^v) = S_4(\alpha^{vg^i}) + S_4(\alpha^{vg^j}) + S_4(\alpha^{v\theta^l}) + S_4(\alpha^{vg^j}) + 1 =$$
$$S_4(\alpha^{vg^i}) + S_4(\alpha^{vg^l}) + 1.$$

The values of $S_4(\alpha)$ were shown in [6], after summing up we get that the order of set $|v : \{S(\alpha^v, v = 1, ..., p - 1\}|$ equals zero, if $y \equiv 1(\text{mod } 2)$ or $y \equiv 2(\text{mod } 4), |i - l| \neq 2$ and equals $(p - 1)/2$ otherwise.

Its easy to prove that $S(1) \neq 0$. From this and by (4) we get the statement of Lemma 2. ■

In particular, from Lemma 2 it follows that binary sequences of period $2p$ found in [10], which have optimal periodic autocorrelation function ($y = 1$ or $x = 1, |i - l| \neq 2$, have also high linear complexity $L = 2p$ (in other case from [10] which we do not consider here, $L = 2p - 2$).

Also we can design the sequences with high linear complexity by formula (5) without using the values of auxiliary polynomial. The following lemma allow to evaluate the linear complexity of S.

Lemma 3: If $v \in p^h \mathbb{Z}_{p^m}^*$, $h = 0, 1, \dots, m - 1$, then

$$\sum_{j=0}^{d-1} S_k(\alpha^{v\theta^j}) = \begin{cases} 1, & \text{if } h = m - k - 1; \\ 0, & \text{else.} \end{cases}$$

for $k = 0, 1, \dots, m - 1$.

Proof: By (1) and the definition of the auxiliary polynomial we have $\sum_{j=0}^{d-1} S_k(\alpha^{v\theta^j}) = \sum_{i \in p^k \mathbb{Z}_{p^m}^*} \alpha^{vi}$. Then

$$\sum_{j=0}^{d-1} S_k(\alpha^{v\theta^j}) = \begin{cases} 0, & \text{if } k + h \geq m; \\ \sum_{j \in \mathbb{Z}_{p^{m-k-h}}^*} \alpha^{p^{k+h} j}, & \text{if } k + h < m. \end{cases}$$

By the condition, $\alpha^{p^m} - 1 = 0$ and the order of α equals p^m, hence we obtain $\sum_{j \in \mathbb{Z}_{p^{m-t}}} \alpha^{jp^t} = 1$. Then

$$\sum_{j \in \mathbb{Z}_{p^{m-t}}^*} \alpha^{jp^t} = \begin{cases} 1, & \text{if } t = m - 1; \\ 0, & \text{else.} \end{cases}$$

Lemma 3 follows from the last formula. ■

Hence, by Lemmas 3 we can easily select the subset $I_k^{(j)}, j = 0, 1, \dots, 2^n - 1$ so that $S(\alpha^v) \neq 0, v = 1, 2, \dots, p^m - 1$. Then $L = 2p^m$ for $n = 1$ and $L \geq 2^n p^m - 2^n$ for $n > 1$.

Example Let $I_k^{(0)} = \{0,1\}, I_k^{(1)} = \{2,3\}, I_k^{(2)} = \{0,3\}, I_k^{(3)} = \{0,3\}, k = 0,1,\dots,m-1$ for $d = 4$ and $n = 2$. Then by Lemma 3 and (5) we have $S(\alpha^v) = 1, v = 1,2,\dots,p^m - 1$. Hence, $L = 4p^m - 4$ and $m(x) = (x^{4p^m} - 1)/(x-1)^4$ by (3). Note that in this case we can take any other subset $I_k^{(2)} = \{0,3\}$ and $I_k^{(3)} = I_k^{(2)}, k = 0,1,\dots,m-1$.

In the following section we investigate an evaluation of the linear complexity in detail for $d = 2$.

IV. The evaluation of the linear complexity of generalized cyclotomic sequences of length $2^n p^m$

Let

$$I = \{k | \sum_{l=0}^{2^n-1} i_k^{(l)} \equiv 1 \pmod 2 \text{ and } k = 0,1,\dots,m-1\},$$

i.e., the number of zeros and unities in the set $\{i_k^{(l)}, l = 0,\dots,2^n-1\}$ for $k \in I$ is odd. By I^* denote the complement of the set I in the set $\{0,1,\dots,m-1\}$.

Theorem 4: Let generalized cyclotomic sequence S be defined by (2). Then $S(\alpha^v) = 0$ for $v = 1,...,p^m - 1$ if and only if $v \in \bigcup_{k\in I} p^{m-k-1}\mathbb{Z}_{p^m}^*$ for $n = 1$ and $v \in \bigcup_{k\in I^*} p^{m-k-1}\mathbb{Z}_{p^m}^*$ for $n > 1$.

Proof: By Lemma 1 and the definition of S we have

$$S(\alpha^v) = 2^{n-1} + \sum_{l=0}^{2^n-1}\sum_{k=0}^{m-1} S_k\left(\alpha^{v\theta^{i_k^{(l)}}}\right)$$

or

$$S(\alpha^v) = 2^{n-1} + \sum_{k\in I}\left(S_k(\alpha^v) + S_k(\alpha^{v\theta})\right)$$

by the choice of I.

Therefore, $S(\alpha^v) = 0$ if and only if $\sum_{k\in I} S_k(\alpha^v) + S_k(\alpha^{v\theta}) = 1$ for $n = 1$ and $\sum_{k\in I} S_k(\alpha^v) + S_k(\alpha^{v\theta}) = 0$ for $n > 1$. In the first case, by Lemma 3, $v \in p^{m-k-1}\mathbb{Z}_{p^m}^*$ for $k \in I$, and in the second case $v \in p^{m-k-1}\mathbb{Z}_{p^m}^*$ for $k \notin I$. Theorem 4 is proved. ■

Corollary 5:

$$|\{v|S(\alpha^v) = 0, v = 0,1,\dots,p^m-1\}| = \begin{cases}\sum_{k\in I} p^k(p-1), & \text{if } n = 1;\\ \sum_{k\in I^*} p^k(p-1) + 1, & \text{if } n > 1.\end{cases}$$

Corollary 6: Let generalized cyclotomic sequence S be defined by (2). If $I = \varnothing$ and $n = 1$, then $L = 2p^m$. Also, if $I = \{0,1,\dots,m-1\}$ and $n > 1$, then $L \geq 2^n p^m - 2^n$.

All sequences satisfying the conditions of Corollary 6 have high linear complexity. Moreover, if the set of vectors $\{L_j\}$ defining the sequence is such that $m - 1 \notin I$ for $n = 1$ and $m - 1 \in I$ for $n > 1$, then $\sum_{k\in I(I^*)} p^k(p-1) \leq p^{m-1} - 1$. By Corollary 5 and (4) we see that $L \geq 2^n p^m - 2^n p^{m-1}$, i.e., $L > N/2$.

In order to refine the estimate of the linear complexity, we investigate the multiplicity of the zeros α^v of $S(x)$. For this purpose let us examine the derivative of $S(x)$. Since $\left(\sum_{i\in\phi^{-1}(\{l\}\times H_{i_k^{(l)}})} x^i\right)^{'} = 0$ when l is even, then

$$S^{'}(\alpha^v) = \alpha^{-v}\sum_{t=0}^{2^{n-1}-1}\sum_{k=0}^{m-1}\sum_{i\in\phi^{-1}(\{2t+1\}\times H_{i_k^{(2t+1)}})}\alpha^{v\theta^{i_k^{(2t+1)}}}. \tag{6}$$

It is obvious from (6) that the analysis of $S^{'}(\alpha^v)$ substantially differs in cases $n = 1$ and $n > 1$.

First, let $n > 1$. Define the set

$$J = \{k| \sum_{t=0}^{2^{n-1}-1} i_k^{(2t+1)} \equiv 1 \ (\bmod\ 2) \text{ and } k = 0,1,\dots,n-1\},$$

that is the number of zeros and unities in the set $\{i_k^{(2t+1)}, t = 0,\dots,2^{n-1}-1\}$ is odd for $k \in J$. By J^* denote the complement of J in $\{0,1,\dots,m-1\}$.

Lemma 7: If $n > 1$ and α^v is a zero of $S(x)$, then α^v is a multiple zero if and only if $v \in \bigcup_{k\in I^*\cap J^*} p^{m-k-1}\mathbb{Z}_{p^m}$.

Proof: By (6) and the definition of J, we obtain

$$S^{'}(\alpha^v) = \alpha^{-v}\sum_{k\in J}\left(S_k(\alpha^v) + S_k(\alpha^{v\theta})\right),$$

similar as in Theorem 4. Then by Lemma 3, it follows that $S^{'}(\alpha^v) = 0$ if and only if $v \in p^{m-k-1}\mathbb{Z}_{p^m}$ for $k \in J^*$. So, the statement of Lemma 7 follows from Theorem 4. ■

From Theorem 4 and Lemma 7, we get the following estimate:

$$L \geq 2^n p^m - \sum_{k\in I^*\setminus J^*} p^k(p-1) - 2^n \sum_{k\in I^*\cap J^*} p^k(p-1) - 2^n.$$

Hence, if $n > 1$, then it is easy to find out for which defining vectors the sequence S has high linear complexity.

Let $n = 1$ and symbols be the same as before. Without loss of generality, we can assume that $S_{m-1}(\alpha) \neq 0$.

Theorem 8: If generalized cyclotomic sequence S is defined by (2), then

(i) $L = 2p^m - \sum_{k\in I} p^k(p-1)$ and $m(x) = \left(x^{2p^m} - 1\right)/G(x)$, if $p \equiv \pm 3(\bmod 8)$. Here $G(x) = \prod_{k\in I}\left(x^{p^{k+1}} - 1\right)/\left(x^{p^k} - 1\right)$.

(ii) $L = 2p^m - 1.5\sum_{k\in I} p^k(p-1)$ and $m(x) = \left(x^{2p^m} - 1\right)/\left(G(x)\prod_{k\in I}\prod_{u\in p^{m-k-1}H_{f_k}}(x - \alpha^v)\right)$, if $p \equiv \pm 1(\bmod 8)$.

Here

$$f_k = \begin{cases} i_k^{(1)}, & \text{if } (m-k) \text{ is even and } p \equiv -1(\bmod 8);\\ 1 - i_k^{(1)}, & \text{else.}\end{cases}$$

Proof: If $n = 1$ then $S^{'}(\alpha^v) = \alpha^{-v}\sum_{k=0}^{m-1} S_k(\alpha^{v\theta^{i_k^{(1)}}})$. By Lemma 2 [6] we have

$$S^{'}(\alpha^v) = \alpha^{-v}\left(S_{m-1}\left(\alpha^{\theta^{i_k^{(1)}+f}}\right) + (m-k-1)(p-1)/2\right),$$

if $v \in p^{m-k-1}H_f$ or

$$S^{'}(\alpha^v) = \alpha^{-v}\left(T\left(\beta^{\theta^{i_k^{(1)}+f}}\right) + (m-k-1)(p-1)/2\right),$$

where $\beta = \alpha^{p^{m-1}}$ and $T(x) = \sum_{j \in H_0 \bmod p} x^j$.

The values $T(\beta^v)$ were derived by C. Ding et al [5]. Specifically, if $p \equiv \pm 3 \pmod 8$, then $T(\beta^v) \notin \{0, 1\}$, that is $S^{'}(\alpha^v) \neq 0$, and the first statement follows from Theorem 4. In the case $p \equiv \pm 1 (\bmod 8)$, according to our assumption $T(\beta) = 1$ and $T(\beta^\theta) = 0$, therefore $S^{'}(\alpha^v) = 0$, if $v \in p^{m-k-1} H_f$ for

$$f = \begin{cases} i_k^{(1)}, & \text{if } (m-k) \text{ is even and } p \equiv -1 (\bmod 8); \\ 1 - i_k^{(1)}, & \text{else.} \end{cases}$$

Applying (3) and (4), we conclude the proof of Theorem 8. ■

Theorems 1 and 2 [20], Theorem 1 [14] are special cases of Theorem 8 ($I = \{0, 1, \ldots, m-1\}, I = \varnothing$, respectively).

In the second case of Theorem 8, if the set of vectors $\{L_k\}$ defining the sequence S is such that $m - 1 \in I$, then $L \leq p^m$, i.e., in this case sequences do not have high linear complexity. All results from the section IV have been verified by subjecting various sequences to Berlekamp-Massey algorithm for small values of p, m, and n.

V. Autocorrelation of generalized cyclotomic sequences of length $2^n p^m$

The periodic autocorrelation function $C_S(\tau)$ of a binary sequence $\{s_i\}$ of period N is defined by

$$C_S(\tau) = \sum_{i=0}^{N-1} (-1)^{s_{i+\tau} + s_i}.$$

In this section we evaluate the autocorrelation function of generalized cyclotomic binary sequences defined by (2). We measure the autocorrelation function by using known methods [13], [17] and generalized cyclotomic numbers of order 2 with respect to p^h for $h \geq 1$ [4],

$$(u, v)^{(p^h)} = |(H_v^{(p^h)} + 1) \cap H_u^{(p^h)}|,$$

where $H_j^{(p^h)} = \{a \pmod{p^h} | a \in H_j\}$. C. Ding and T. Helleseth [4] showed that

1. If $p \equiv 1 \pmod 4$, then

$$(0,0)^{(p^h)} = p^{h-1}(p-5)/4,$$
$$(0,1)^{(p^h)} = (1,0)^{(p^h)} = (1,1)^{(p^h)} = p^{h-1}(p-1)/4;$$

2. If $p \equiv 3 \pmod 4$, then

$$(0,0)^{(p^h)} = (1,0)^{(p^h)} = (1,1)^{(p^h)} = p^{h-1}(p-3)/4,$$
$$(0,1)^{(p^h)} = p^{h-1}(p+1)/4.$$

As before, let $E_j = \bigcup_{k=0}^{m-1} p^k H_{i_k^{(j)}}$. First we define the difference function $d(j, l, \tau) = |E_j \cap (E_l + \tau)|$.

Lemma 9: If $\tau \in p^f H_a$, $f = 0, 1, \ldots, m-1; a = 0, 1$, then

$$d(j,l,\tau) = \sum_{k=0: i_k^{(j)} = j_k^{(l)}}^{f-1} p^{m-k-1}(p-1)/2 + \left(p^{m-f-1}(p \pm 1) + \delta\right)/4,$$

where

$$\delta = \begin{cases} -4, & \text{if } a = i_f^{(j)}, a \neq i_f^{(l)}, p \equiv 3 \pmod 4 \\ & \quad \text{or } a = i_f^{(j)} = i_f^{(l)}, p \equiv 1 \pmod 4; \\ -2, & \text{if } i_f^{(j)} = i_f^{(l)}, p \equiv 3 \pmod 4 \\ & \quad \text{or } i_f^{(j)} \neq i_f^{(l)}, p \equiv 1 \pmod 4; \\ 0, & \text{if } a = i_f^{(l)}, a \neq i_f^{(j)}, p \equiv 3 \pmod 4 \\ & \quad \text{or } a \neq i_f^{(j)}, i_f^{(j)} = i_f^{(l)}, p \equiv 1 \pmod 4. \end{cases}$$

Here we use the minus sign if $i_f^{(j)} = i_f^{(l)}$ and the plus sign otherwise.

Proof: To simplify the proof, we denote $i_k^{(j)}, i_k^{(l)}$ as h_k and g_k respectively. Then $d(j, l, \tau) = \sum_{k=0}^{m-1} |E_j \cap (p^k H_{g_k} + \tau)|$.

Let us break the last sum into three summands and examine each of them separately.

1) Let $k < f$, then $p^k H_{g_k} + \tau = p^k H_{g_k}$ [6] and

$$\sum_{k=0}^{f-1} |E_j \cap (p^k H_{g_k} + \tau)| = \sum_{k=0}^{f-1} |p^k H_{h_k} \cap p^k H_{g_k}| = \sum_{k=0: h_k = g_k}^{f-1} p^{m-k-1}(p-1)/2.$$

2) Let $k = f$, then

$$|E_j \cap (p^f H_{g_f} + \tau)| = |p^f H_{h_f} \cap (p^f H_{g_f} + \tau)| + \sum_{k=f+1}^{m-1} |p^k H_{h_k} \cap (p^f H_{g_f} + \tau)|.$$

The first summand from the last sum equals $(g_f + a, h_f + a)^{(p^{m-f})}$. By Lemma 2 [19]

$$|p^k H_{h_k} \cap (p^f H_{g_f} + \tau)| = \begin{cases} (p^{m-k} - p^{m-k-1})/2, & \text{if } a = g_f, p \equiv 1 \pmod 4 \\ & \quad \text{or } a \neq g_f, p \equiv 3 \pmod 4; \\ 0, & \text{else.} \end{cases}$$

Therefore,

$$|E_j \cap (p^f H_{g_f} + \tau)| = \begin{cases} (0, h_f + a)^{(p^{m-f})} + (p^{m-f-1} - 1)/2, \\ \qquad \text{if } a = g_f, p \equiv 1 \pmod 4; \\ (1, h_f + a)^{(p^{m-f})} + (p^{m-f-1} - 1)/2, \\ \qquad \text{if } a \neq g_f, p \equiv 3 \pmod 4; \\ (g_f + a, h_f + a)^{(p^{m-f})}, \qquad \text{else.} \end{cases}$$

3) Let $k > f$, then $p^k H_{g_k} + \tau \subset p^f H_a$ [14] and

$$\sum_{k=f+1}^{m-1} |E_j \cap (p^k H_{g_k} + \tau)| = \sum_{k=f+1}^{m-1} |p^f H_{h_f} \cap (p^k H_{g_k} + \tau)| = (p^{m-f-1} - 1)/2,$$

if $a = h_f$ and $\sum_{k=f+1}^{m-1} |E_j \cap (p^k H_{g_k} + \tau)| = 0$ if $a \neq h_f$.

Summing up the results, we obtain the statement of Lemma 9. ■

Like Y. Sun and H. Shen showed [17], it is simple to see that

$$|C\cap(C+\tau)| = \sum_{u=0}^{2^n-1}|C_u\cap(C_{(u-\tau)\mod 2^n}+\tau)|+$$
$$|C\cap\{0,\dots,(2^n-2)p^m\}|+|\{0,\dots,(2^n-2)p^m\}\cap(C+\tau)|,$$

and

$$|C_j\cap(C_{(j-\tau)\mod 2^n}| = |E_j\cap(E_{(j-\tau)\mod 2^n}+\tau)| = d\big(j,(j-\tau)\mod 2^n,\tau\big).$$

Since $C_S(\tau)=4|C\cap(C+\tau)|-N$, then Lemma 9 shows that for $m\geq 1$ the sequence S has poor autocorrelation properties. Applying Lemma 9, we can derive the autocorrelation function for the given set of defining vectors. In particular, from Lemma 9 we can simply obtain Theorem 2 [14].

Consider the autocorrelation function for $\tau\equiv 0(\mathrm{mod}\ 2^n)$.

Theorem 10: If the sequence S is defined by (2) and $\tau\in\phi^{-1}(\{0\}\times p^f H_a)$, $f=0,1,\dots,m-1; a=0,1$, then

$$C_S(\tau)=2^n(p^m-p^{m-f}-p^{m-f-1})+A,$$

where $A=0$, if $p\equiv\ 3(\mathrm{mod}\ 4)$ and

$$A=|\{t|i_f^{(2t)}=a,t=0,1,\dots,2^{m-1}-1\}|-$$
$$|\{t|i_f^{(2t+1)}=a,t=0,1,\dots,2^{m-1}-1\}|,$$

if $p\equiv\ 1(\mathrm{mod}\ 4)$.

Proof: Under the conditions of Theorem 10 we have

$$|C\cap(C+\tau)| = \sum_{u=0}^{2^n-1}|E_u\cap(E_u+\tau)|+$$
$$|C\cap(\{0,\dots,(2^n-2)p^m\}+\tau)\,|+$$
$$|\{0,\dots,(2^n-2)p^m\}\cap(C+\tau)|. \quad (7)$$

By definition, put

$$A_1=|\{t|i_f^{(2t+1)}=a,\quad t=0,1,\dots,2^{m-1}-\ 1\}|$$

and

$$A_2=|\{t|i_f^{(2t)}=a,\quad t=0,1,\dots,2^{m-1}-1\}|.$$

From Lemma 9 it follows that

$$\sum_{u=0}^{2^n-1}|E_u\cap(E_u+\tau)| =$$
$$\sum_{u=0}^{2^n-1}d(u,u,\tau)=2^{n-2}(2p^m-p^{m-f}-p^{m-f-1})-B, \quad (8)$$

where $B=\begin{cases}A_1+A_2, & \text{if } p\equiv 1\ (\mathrm{mod}\ 4);\\ -2^{n-1}, & \text{if } p\equiv 3\ (\mathrm{mod}\ 4).\end{cases}$.

If $\tau\in\phi^{-1}(\{0\}\times p^f H_a)$, then

$$|C\cap(\{0,2p^m,\dots,(2^n-2)p^m\}+\tau)\,| =$$
$$\sum_{j=0}^{2^{n-1}-1}|E_{2j}\cap(\{0,2p^m,\dots,(2^n-2)p^m\}+\tau)| =$$
$$\sum_{j=0}^{2^{n-1}-1}|E_{2j}\cap\{\tau\}|.$$

Similarly, $|\{0,2p^m,\dots,(2^n-2)p^m\}\cap(C+\tau)| = \sum_{j=0}^{2^{n-1}-1}|\{0\}\cap(E_{2j}+\tau)|$.

If $p\equiv 1\ (\mathrm{mod}\ 4)$, then $-1\in H_0$ and $-1\in H_1$ if $p\equiv 3\ (\mathrm{\ mod\ } 4)$ [14]. Hence, $|E_{2j}\cap\{\tau\}|$ is equal to 1, if $a=i_f^{(2j)}$ and zero if $a\neq i_f^{(2j)}$. Next,

$$|\{0\}\cap(E_{2j}+\tau)| = \begin{cases}1, \text{ if } a=i_f^{(2j)}, p\equiv 1\ (\mathrm{mod}\ 4)\\ \quad \text{or } a\neq i_f^{(2j)}, p\equiv 3\ (\mathrm{mod}\ 4);\\ 0, \text{ else.}\end{cases}$$

Therefore,

$$|C\cap(\{0,2p^m,\dots,(2^n-2)p^m\}+\tau)|+$$
$$|\{0,2p^m,\dots,(2^n-2)p^m\}\cap(C+\tau)| =$$
$$=\begin{cases}2A_2, & \text{if } p\equiv 1\ (\mathrm{mod}\ 4);\\ 2^{n-1}, & \text{if } p\equiv 3\ (\mathrm{mod}\ 4).\end{cases} \quad (9)$$

Since $C_S(\tau)=4|C\cap(C+\tau)|-N$, we obtain Theorem 10 by summing up (7), (8), and (9). ■

Theorem 10 shows that for $m>1$ the autocorrelation function of S is far from ideal (see [14]).

VI. Conclusion

We discuss a computation method for the linear complexity of generalized cyclotomic binary sequences of length 2^np^m. Also we generalize the results about binary sequences of length $2p^m$ and evaluate the linear complexity and autocorrelation properties of generalized cyclotomic binary sequences of length 2^np^m. Our method allows to design the sequences with high linear complexity.

References

[1] N.G.Bardis, A.Polymenopoulos, E.G.Bardis, A.P.Markovskyy, and D.V.Andrikou, "An approach to determine the complexity of random and pseudo random binary sequences", *WSEAS TRANSACTIONS on COMMUNICATIONS.,* iss. 1, vol.1, pp. 37–42, 2002.

[2] Bardis N.G, Markovskyy A.P., Andrikou D.V., "Method for Design of pseudorandom binary sequences generators on nonlinear feedback shift register (NFSR)"., *WSEAS TRANSACTIONS on COMMUNICATIONS*, iss. 2, vol.3, pp. 758-763, April 2004.

[3] T. Cusick, C. Ding, and A. Renvall, *Stream ciphers and number theory*. N.-Holl. Math. Libr. vol.55, 1998.

[4] C. Ding, T. Helleseth. "Generalized cyclotomy and its applications". *Finite Fields Appl.*, vol.4, pp. 467–474, 1999

[5] C. Ding, T. Helleseth, and W. Shan. "On the linear complexity of Legendre sequences". *IEEE Trans. Inform. Theory*, vol. 44, pp. 1276–1278, 1998

[6] V. Edemskiy. "About computation of the linear complexity of generalized cyclotomic sequences with period p^{n+1}". *Des. Codes Cryptogr.*, vol. 61, pp. 251–260, 2011.

[7] V. Edemskiy, O. Antonova. "The linear complexity of generalized cyclotomic sequences with period $2p^n$". *AAECC*, vol. 25, iss. 3, pp. 213–223, 2014.

[8] V. Edemskiy, O. Antonova. "The linear complexity and the autocorrelation of generalized cyclotomic binary sequences of length 2^np^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] V. Edemskiy, O. Antonova." Linear complexity of generalized cyclotomic sequences with period 2^mp^n". *Applied Discrete Mathematics*, vol. 3, pp. 5–12, 2012 (in Russian).

[10] C. Ding, T. Helleseth, and H. Martinsen. "New families of binary sequences with optimal three-level autocorrelation". *IEEE Trans. Info. Theory.*, vol. IT-47, pp. 428 – 433, 2001.

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

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

[13] S. Y. Jin, Y. J. Kim, and H. Y. Song. ”Autocorrelation of new generalized cyclotomic sequences of period p^n”. *IEICE Trans. Fundam.*, vol.E93-A, pp. 2345–2348, 2010.

[14] P. Ke, J. Zhang, and S. Zhang. ”On the linear complexity and the autocorrelation of generalized cyclotomic binary sequences of length $2p^m$”. *Des. Codes Cryptogr.,* vol.67, no. 3, pp.325–339, 2013

[15] Y. J. Kim, H. Y. Song. ”Linear complexity of prime n-square sequences”. *In: IEEE International Symposium on Information Theory*, Toronto, Canada, pp. 2405–408, 2008

[16] R. Lidl, H. Neid, *Finite Fields.* Addison-Wesley, 1983.

[17] Y. Sun, H. Shen. ”New Binary Sequences of Length $4p$ with Optimal Autocorrelation Magnitude”. *Ars Combinatoria (A Canadian Journal of Combinatorics).* vol.89, pp.255–262, 2008

[18] M. A. Mioc. ”Study of Using Shift Registers in Cryptosystems for Grade 8 Irreducible Polynomials”, *WSEAS Conference SMO*, 23-25 September 2008.

[19] T. Yan, S. Li, and G. Xiao. ”On the linear complexity of generalized cyclotomic sequences with the period p^m”. *Appl. Math. Lett.,* vol.21, pp. 187–193, 2008

[20] J. W. Zhang, C. A. Zhao, and X. Ma. ”Linear complexity of generalized cyclotomic binary sequences of length $2p^m$”. *AAECC.,* vol. 21, pp. 93–108, 2010.