Using of Generalized Cyclotomy for Sequence Design over the Finite Field of Order Four with High Linear Complexity

Vladimir Edemskiy

Abstract—We consider the use of generalized Ding-Helleseth cyclotomy to design sequences over the finite field of order four. Using generalized cyclotomic classes of order four we obtain the family of balanced sequences of odd period with high linear complexity. Also we present a method of constructing sequences with high linear complexity and arbitrary even period over the finite field of order four. These sequences are obtained with generalized Ding-Helleseth cyclotomy of order two . We generalize design of the sequences over the finite field of order four proposed by P. Ke et al. and D. Li et al.

Keywords—Linear complexity, finite field, sequences

I. Introduction

FOR cryptographic applications, the linear complexity (L) of a sequence is an important merit factor [10], [2]. 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)[14].

Using classical cyclotomic classes and generalized cyclotomic classes to construct binary sequences which are called classical cyclotomic sequences and generalized cyclotomic sequences respectively, is an important method for sequence design [2]. A generalized cyclotomy with respect to pq was introduced by Whiteman [16]. However, his generalized cyclotomy is not consistent with classical cyclotomy. In their paper [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 includes classical cyclotomy as a special case and they show how to construct binary sequences based on this new generalized cyclotomy. A unified approach for the generalized cyclotomy over the residue classes ring was presented in [9]. There are many works devoted to use of Ding-Helleseth cyclotomy or Whiteman cyclotomy to construct binary sequences. While, there are scattered results of generalized cyclotomic quaternary sequences over the finite field of order four $\mathbb{F}_4$ with high linear complexity.

In particular, the sequences of periods $2p, 2p^n, pq, 2pq, 2p^{m+1}q^{n+1}$ with high linear complexity were studied in [4], [12], [8], [1], [15] (see also references therein). The generalized Whiteman cyclotomy or Ding-Helleseth cyclotomy are used in these papers for design sequences. Authors of the above-mentioned article refer to these sequences as quaternary. At the same time, the number of researches believe that this name can only be used for sequences with terms $0, 1, 2, 4$ $(\pm i, \pm 1)$. Also using the Gray map for these sequences we may easily obtain sequences over $\mathbb{F}_4$ and vice versa. For the application of sequences over the finite field, see [13], for instance.

In this paper, first we consider using Ding-Helleseth cyclotomy of order four to design sequences over $\mathbb{F}_4$ with odd periods and high linear complexity. Secondary, we propose a method of constructing sequences over $\mathbb{F}_4$ with high linear complexity and arbitrary even period. These sequences are obtained using generalized Ding-Helleseth cyclotomy of order two [3]. In particular, we generalize the result of [4], [12] and present other method of designing sequences with periods $pq, 2p^{m+1}q^{n+1}$. These results were partially presented at the conference [7].

The rest of the paper is structured as follows. In Section II, we consider the case when a period of sequence N is an odd number. In Section III, we consider the design of sequences over the finite fields of order four with an even period. Finally, we conclude the paper with some remarks.

II. Design sequences with odd periods

In this section we consider the case when a period of sequence N is an odd number and $N = p_1^{e_1} \cdots p_t^{e_t}$, $p_i \equiv 1 (\mathrm{mod}\ 4), i = 1, \dots, t$, where $p_1, ..., p_t$ are pairwise distinct odd primes. It is well known that there exists a primitive root g_i modulo $p_i^{e_t}$ [11]. In what follows we suppose $D_0^{(p_i^{e_i})} = \{{g_i}^{4j} | j \in Z\}$ be the subgroup of $Z^*_{p_i^{e_i}}$, generated by g_i^4, and $D_k^{(p_i^{e_i})} = g_i^k D_0^{(p_i^{e_i})}$; $k = 1, 2, 3$, where the arithmetic is that of $Z_{p_i^{e_i}}$, $i = 1, 2, ..., t$, i.e. we will use Ding-Helleseth generalized cyclotomic classes of order four.

Let $G_k^{(p_i^{e_i})} = \bigcup_{l=0}^{e_i-1} p_i^l D_k^{(p_i^{e_i})}$. Then as in [3] we have a partition

$$Z_{p_i^{e_i}} = \bigcup_{j=0}^{3} G_k^{(p_i^{e_i})} \cup \{0\}.$$

According to the Chinese Remainder Theorem

$$Z_n \cong Z_{p_1^{e_1}} \times ... \times Z_{p_t^{e_t}}$$

relatively to isomorphism $\phi(x) = (x \mod p_1^{e_1}, ..., x \mod p_t^{e_t})$ [11]. Here and hereafter $x \bmod n$ denotes the least

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.

nonnegative integer that is congruent to x modulo n. Below, we will use the denotation $\phi^{-1}(x)$ for all of values t.

By definition, put $N_1 = N, N_{j+1} = N/p_1^{e_1}\cdots p_j^{e_j}; j = 2,\dots,t$ (here $N_{t+1}=1$) and

$$C_k = \phi^{-1}\big(G_k^{(p_1^{e_1})} \times Z_{N_2} \cup \{0\} \times G_k^{(p_2^{e_2})} \times Z_{N_3} \cup \dots \cup \{0\}\times\cdots\times\{0\} \times G_k^{(p_{t-1}^{e_{t-1}})} \times Z_{N_t} \cup \{0\}\times\cdots\times\{0\}\times G_k^{(p_t^{e_t})}\big); k = 0,1,2,3.$$

By definition, sets C_k are dependent on the order of factors in the expansion N. From our definitions it follows that $Z_N = \cup_{i=0}^3 C_k \cup \{0\}$.

Let $\mathbb{F}_4 = \{0, 1, \mu, \mu+1\}$ be a finite field of order four. We consider a sequence $\{s_i\}$ defined by

$$s_i = \begin{cases} 0, & \text{if } i \in C_0 \cup \{0\},\\ 1, & \text{if } i \in C_1,\\ \mu, & \text{if } i \in C_2,\\ \mu+1, & \text{if } i \in C_3. \end{cases} \quad (1)$$

The sequence defined by (1) is balanced. Further, we derive the linear complexity of this sequence. Before we give the main result of this section, we establish the following lemmas.

A. Subsidiary lemmas

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

$$m(x) = (x^N-1)/\gcd\big(x^N-1, S(x)\big), \qquad L = N - \deg\gcd\big(x^N-1, S(x)\big), \quad (2)$$

where $S(x) = s_0 + s_1x + ... + s_{N-1}x^{N-1}$.

Let α be a primitive Nth root of unity in the extension of $\mathbb{F}_4$. Then, according to (2), in order to find the minimal polynomial and the linear complexity of $\{s_i\}$ it is sufficient to find the zeros of $S(x)$ in the set $\{\alpha^v, v = 0,1,\dots,N-1\}$.

In this subsection we investigated the values $S(\alpha^v)$. By (1), to compute these values it is sufficient to find $\sum_{i\in C_k}\alpha^{vi}$. Suppose $F_1 = \phi^{-1}\big(G_0^{(p_1^{e_1})}\times Z_{N_2}\big)$ and $F_j = \phi^{-1}\big(\{0\}\times\cdots\times\{0\}\times G_0^{(p_j^{e_j})}\times Z_{N_{j+1}}\big); j = 2,\dots,t$; then $C_0 = \cup_{j=1}^t F_j$. First of all, we derive $\sum_{i\in F_j}\alpha^{vi}$.

Let $\beta_k = \alpha^{N/N_k}, k = 1,\dots,t$. Then β_k is a primitive N_kth root of unity in the extension of $\mathbb{F}_4$.

Lemma 1: If $v \not\equiv 0 (\mathrm{mod}\ N_k)$ then $\sum_{i\in Z_{N_k}}\beta_k^{vi} = 0$ for $k = 1,2,\dots,t$.

Proof: By definition, $\beta_k^{vN_k} = 1$. Then $0 = \beta_k^{vN_k} - 1 = (\beta_k^v - 1)(1 + \beta_k^v + \cdots + \beta_k^{v(N_k-1)})$. To conclude the proof, it remains to note that $\beta_k^v - 1 \neq 0$. ∎

Lemma 2: If $v \not\equiv 0 (\mathrm{mod}\ N_{k+1})$ for $k = 1,\dots,t-1$ then $\sum_{i\in\phi^{-1}\left(G_0^{(p_k^{e_k})}\times Z_{N_{k+1}}\right)}\beta_k^{vi} = 0$.

Proof: We have that

$$\sum_{i\in\phi^{-1}\left(G_0^{(p_k^{e_k})}\times Z_{N_{k+1}}\right)}\beta_k^{vi} = \sum_{a\in G_0^{(p_k^{e_k})}}\ \sum_{i\in\phi^{-1}\left(\{a\}\times Z_{N_{k+1}}\right)}\beta_k^{vi}.$$

Let us show that $\sum_{i\in\phi^{-1}\left(\{a\}\times Z_{N_{k+1}}\right)}\beta_k^{vi} = 0$ for $1 \le a < p_k^{e_k}$. We have

$$\sum_{i\in\phi^{-1}\left(\{a\}\times Z_{N_{k+1}}\right)}\beta_k^{vi} = \beta_k^{va}\sum_{i\in\phi^{-1}\left(\{a\}\times Z_{N_{k+1}}\right)}\beta_k^{v(i-a)} \quad (3)$$

Since $i \in \phi^{-1}\big(\{a\}\times Z_{N_{k+1}}\big)$, we see that $i - a = p_k^{e_k}f$ and $\gcd(p_k^{e_k}, N_{k+1}) = 1$. From this we can establish that $\beta_k^{v(i-a)} = \beta_{k+1}^{vf}$ or

$$\sum_{i\in\phi^{-1}\left(\{a\}\times Z_{N_{k+1}}\right)}\beta_k^{v(i-a)} = \sum_{f\in Z_{N_{k+1}}}\beta_{k+1}^{vf}.$$

The conclusion of this lemma then follows from (3) and Lemma 1. ∎

It is worth pointing out that Lemma 2 is false for $k = t$.

Corollary 3: Under the conditions of Lemma 2 we have $\sum_{i\in\phi^{-1}\left(G_0^{(p_j^{e_j})}\times Z_{N_{j+1}}\right)}\beta_j^{vi} = 0$ for $j = 1,\dots,k$.

Lemma 4: If $v \not\equiv 0 (\mathrm{mod}\ N_{k+1})$ then $\sum_{i\in F_j}\alpha^{vi} = 0$ for $j = 1,\dots,k$.

Proof: If $j = 1$ then the assertion of Lemma 4 is equivalent to the statement of Lemma 2.

Let $j \ge 2$. For all i such that $i \in F_j$ we have $i \equiv 0 (\mathrm{mod}\ p_1^{e_1}\dots p_{j-1}^{e_{j-1}})$. Therefore, since $\alpha^{p_1^{e_1}\cdots p_{j-1}^{e_{j-1}}} = \beta_j$, $F_j \bmod N_{j+1} = Z_{N_{j+1}}$ and $F_j \bmod p_j^{e_j} = G_0^{(p^{e_j})}$, by Corollary 3 we obtain that $\sum_{i\in F_j}\alpha^{vi} = \sum_{i\in\phi^{-1}\left(G_0^{(p_j^{e_j})}\times Z_{N_{j+1}}\right)}\beta_j^{vi} = 0$. ∎

Lemma 4 defines the values $\sum_{i\in F_j}\alpha^{vi} = 0$ for $v \not\equiv 0 (\mathrm{mod}\ N_{k+1})$. Let as study the case when $v \equiv 0 (\mathrm{mod}\ N_{k+1})$. We can see from the proof of Lemma 4 that in this case the sums $\sum_{i\in G_0^{(p_j^{e_j})}}\alpha^{vi}$ need an investigation. In the special case when $N = p^e$ these sums were studied in [5].

Now, we briefly repeat the result from [5]. Let $\alpha_i = \alpha^{N/p_i^{e_i}}$. Then α_i is a primitive $p_i^{e_i}$th root of unity in the extension of $\mathbb{F}_4$. Introduce the subsidiary polynomials $T_j(x) = \sum_{i\in D_0^{(p_j^{e_j})} \bmod p} x^i$, and let $\gamma_j = \alpha_j^{p_j^{e_j-1}}, j = 1,\dots,t$.

Suppose $c \in p_j^f D_l^{(p_j^{e_j})}$; then by [5] we have

$$\sum_{i\in G_0^{(p_j^{e_j})}}\alpha_j^{ci} = T_j(\gamma_j^{g_j^l}) + f(p_j-1)/4. \quad (4)$$

Lemma 5: Let $v \equiv 0 (\mathrm{mod}\ N_{k+1})$, $v \not\equiv 0 (\mathrm{mod}\ N_k)$, and $v\big(N/p_k^{e_k}\big)^{-1} \bmod p_k^{e_k} \in p_k^f D_l^{(p_k^{e_k})}$ where $\big(N/p_k^{e_k}\big)^{-1}$ is an inverse element $N/p_k^{e_k}$ modulo $p_k^{e_k}$. Then

$$\sum_{i\in C_0}\alpha^{vi} = T_k(\gamma_k^{g_k^l}) + f(p_k-1)/4 + \sum_{j=k+1}^{t}(p_u^{e_u}-1)/4$$

for $k = 1,\dots,t$.

Proof: By definition $\sum_{i\in C_0}\alpha^{vi} = \sum_{j=1}^t\sum_{i\in F_j}\alpha^{vi}$. Since $v \not\equiv 0 (\mathrm{mod}\ N_k)$, by Lemma 4 it follows that $\sum_{i\in F_j}\alpha^{vi} = 0$ for $j = 1,\dots,k-1$.

Further, if $i \in F_j$ and $j > k$ then $i \equiv 0(\mathrm{mod}\ p_1^{e_1} \dots p_k^{e_k})$ and $vi \equiv 0(\mathrm{mod}\ N)$. So, in this case $\alpha^{vi} = 1$ and $\sum_{i \in F_j} \alpha^{vi} \equiv (p^{e_j} - 1)/4(\mathrm{mod}\ 2)$.

Now, we study the latest sum $\sum_{i \in F_k} \alpha^{vi}$. Under the conditions that $i \equiv 0(\mathrm{mod}\ p_1^{e_1} \dots p_{k-1}^{e_{k-1}})$ and $v \equiv 0(\mathrm{mod}\ N_{k+1})$, we obtain $vi \equiv 0(\mathrm{mod}\ N/p_k^{e_k})$. From this we can establish that $\alpha^{vi} = \alpha_k^{vi\left(N/p_k^{e_k}\right)^{-1} \bmod\ p_k^{e_k}}$. Since $F_k \bmod\ p_k^{e_k} = G_0^{(p_k^{e_k})}$, it follows that $\sum_{i \in F_k} \alpha^{vi} = |Z_{k+1}| \sum_{j \in G_0^{(p_k^{e_k})}} \alpha_k^{vi\left(N/p_k^{e_k}\right)^{-1}}$. Combining this with (4), we get the assertion of Lemma 5. ∎

Corollary 6: Under the conditions of Lemma 5 the following relation holds $\sum_{i \in C_m} \alpha^{vi} = T_k(\gamma_k^{g_k^{l+m}}) + f(p_k - 1)/4 + \sum_{u=k+1}^{t} (p_u^{e_u} - 1)/4$.

B. The linear complexity of sequence

In this subsection we derive the linear complexity and the minimal polynomial of $\{s_i\}$. The values $T_k(\gamma_k^{g_k^l})$ were studied in [6]. We write these values omitting index k.

If $p \equiv 1(\mathrm{mod}\ 4)$ then p has a quadratic partition of the form $p = x^2 + 4y^2$. Here x, y are an integers and $x \equiv 1(\mathrm{mod}\ 4)$. In [6] the values of the polynomial $T(x)$ are computed depending on x, y. Without breaking the integrity we can presume that $T(\gamma) \neq 0$ and let $\mathbf{T}(x) = \left(T(x), T(x^g), T(x^{g^2}), T(x^{g^3})\right)$. Then, by [6] we have:

(i) $\mathbf{T}(\gamma) = \left(\zeta, \zeta^2, \zeta^4, \zeta^8\right)$ or $\mathbf{T}(\gamma) = \left(\zeta, \zeta^8, \zeta^4, \zeta^2\right)$, if $y \equiv 1(\bmod\ 2)$, where ζ satisfied a relation $\zeta^4+\zeta^3+\zeta^2+\zeta+1 = 0$ or $\zeta^4 + \zeta^3 + 1 = 0$;

(ii) $\mathbf{T}(\gamma) = (1, 0, 0, 0)$, if $x \equiv 1(\mathrm{mod}\ 8), y \equiv 0(\mathrm{mod}\ 4)$;

(iii) $\mathbf{T}(\gamma) = (1, 1, 0, 1)$, if $x \equiv 5(\mathrm{mod}\ 8), y \equiv 0(\mathrm{mod}\ 4)$;

(iv) $\mathbf{T}(\gamma) = (\mu, 1, \mu + 1, 1)$, if $x \equiv 1(\mathrm{mod}\ 8), y \equiv 2(\mathrm{mod}\ 4)$. Here μ satisfies $\mu^2 = 1 + \mu$;

(v) $\mathbf{T}(\gamma) = (\mu, 0, \mu + 1, 0)$, if $x \equiv 5(\mathrm{mod}\ 8), y \equiv 2(\mathrm{mod}\ 4)$.

Let

$$\Delta_k = \begin{cases} 0, & \text{if } p_k \equiv 5(\mathrm{mod}\ 8), \\ (p_k^{e_k} - 1)/4, & \text{if } p_k \equiv 1(\mathrm{mod}\ 8). \end{cases}$$

For $p_k \equiv 1(\mathrm{mod}\ 8)$ we take $n_k = \delta_k + \mathrm{ind}_{g_k} N/p_k^{e_k}$ where

$$\delta_k = \begin{cases} 0, & \text{if } x_k \equiv 1(\mathrm{mod}\ 8), y_k \equiv 0(\mathrm{mod}\ 4), \\ 1, & \text{if } x_k \equiv 1(\mathrm{mod}\ 8), y_k \equiv 2(\mathrm{mod}\ 4), \\ 2, & \text{if } x_k \equiv 5(\mathrm{mod}\ 8), y_k \equiv 0(\mathrm{mod}\ 4), \\ 3, & \text{if } x_k \equiv 5(\mathrm{mod}\ 8), y_k \equiv 2(\mathrm{mod}\ 4). \end{cases}$$

Put, by definition $m_k(x) = 1$ if $p_k \equiv 5(\mathrm{mod}\ 8)$ and $m_k(x) = \prod_{i \in C_{n_k}} (x - \alpha_k^i)^{N/N_k}$ if $p_k \equiv 1(\mathrm{mod}\ 8)$.

Our main statement in this section is the following.

Theorem 7: Let $\{s_i\}$ be defined by (1). Then $L = N - 1 - \sum_{k=1}^{t} \Delta_k N/N_k$ and $m(x) = (x^N - 1)/\left((x-1)\prod_{k=1}^{t} m_k(x)\right)$.

Proof: By (1) $S(1) = (N-1)/4 + \mu(N-1)/4 + (\mu+1)(N-1)/4 = 0$. Suppose $1 \leq v \leq N-1$, $v \equiv 0(\mathrm{mod}\ N_{k+1})$, and $v \not\equiv 0(\mathrm{mod}\ N_k), k = 1, \dots, t$. ($k = t, N_{t+1} = 1$).

By definition $S(\alpha^v) = \sum_{i \in C_1} \alpha^{vi} + \mu \sum_{i \in C_2} \alpha^{vi} + (\mu + 1) \sum_{i \in C_3} \alpha^{vi}$. Using Lemma 5 and Corollary 6 we obtain that

$$S(\alpha^v) = T_k(\gamma_k^{g_k^{l+1}}) + \mu T_k(\gamma_k^{g_k^{l+2}}) + (\mu+1) T_k(\gamma_k^{g_k^{l+3}}) \quad (5)$$

where $l: \ v\left(N/p_k^{e_k}\right)^{-1} \bmod\ p_k^{e_k} \in p_k^f D_l^{(p_k^{e_k})}$.

By (5) from above-mentioned formulas for $T(\gamma)$ we obtain that $S(\alpha^v) \neq 0$ if $p \equiv 5(\mathrm{mod}\ 8)$; $S(\alpha^v) = 0$ if $p \equiv 1(\mathrm{mod}\ 8)$ and $v\left(N/p_k^{e_k}\right)^{-1} \bmod\ p_k^{e_k} \in G_{\delta_k}^{(p_k^{e_k})}$. In the latest case $v \bmod\ p_k^{e_k} \in G_{n_k}^{(p_k^{e_k})}$. To conclude the proof it remains to note that $|\{v : \ v \bmod\ p_k^{e_k} \in G_{n_k}^{(p_k^{e_k})}, v \equiv 0(\mathrm{mod}\ N_{k+1}), \text{ and } v \not\equiv 0(\mathrm{mod}\ N_k)\}| = N/N_k(p_k^{e_k} - 1)/4$. ∎

Corollary 8: Let $\{s_i\}$ be defined by (1) for $N = p^e$. Then $L = \begin{cases} N-1, & \text{if } p \equiv 5(\mathrm{mod}\ 8), \\ 3(N-1)/4, & \text{if } p \equiv 1(\mathrm{mod}\ 8). \end{cases}$.

Corollary 9: Under the conditions of Theorem 7 we have $L \geq 3(N-1)/4$.

The results of computing the linear complexity by Berlekamp-Massey algorithm when $N = p_1 p_2$, $N = p_1^2 p_2$ or $N = p_1 p_2^2$ for $p_1 = 5, 13, \dots, 29, p_2 = 13, 17, \dots, 37$ and for other values of N confirm the results of this section.

So, sequences defined by (1) have high linear complexity for all values of the period. Since by the definition the sequence depends on the order of factors in the expansion of the period, it follows that for one N we can construct a few sequences with various values of the linear complexity if exists i such that $p_i \equiv 1(\mathrm{mod}\ 8)$. For example, let $N = 1105$. Then:

$L = 844$ if $p_1 = 5, p_2 = 13, p_3 = 17$;

$L = 1084$ if $p_1 = 5, p_2 = 17, p_3 = 13$;

$L = 1100$ if $p_1 = 17, p_2 = 5, p_3 = 13$;

$L = 1052$ if $p_1 = 13, p_2 = 17, p_3 = 5$.

This method may also be used when $p_i \equiv 3(\bmod\ 4)$. Here we can take the generalized cyclotomic classes of order 2 for pairs of elements from $\mathbb{F}_4$ by turns. But, in this case the sequences will have very bad balanced properties. In order to eliminate this drawback, in the following section we consider sequences of an even period.

III. Design sequences of even periods

In this section we consider the design sequences over the finite fields of order four with an even period. First we build a partition of residue classes ring Z_N. Let N be an even integer and $N = 2^m n$, where $\gcd(n, 2) = 1$. Then $n = p_1^{e_1} \cdots p_t^{e_t}$, when $p_1, ..., p_t$ are pairwise distinct odd primes. In this case we can use Ding-Helleseth generalized cyclotomic classes.

Let $\{C_0, C_1\}$ be generalized cyclotomic classes of order two with respect Z_n, where Z_n is a ring of residue classes modulo n [3]. Then $\{C_0, C_1\}$ is a partition of $Z_n \setminus \{0\}$, i.e. $Z_n = C_0 \cup C_1 \cup \{0\}$ and $C_0 \cap C_1 = \varnothing$.

Using Ding-Helleseth cyclotomy, we obtain a partition of Z_N. The ring of residue classes $Z_{2^m n} \cong Z_{2^m} \times Z_n$ relative to isomorphism $\phi(x) = (x \bmod\ 2^m, x \bmod\ n)$. Put, by definition

$$H_{j,i} = \phi^{-1}\left(\{j\} \times C_i\right), j = 0, \dots, 2^m - 1; i = 0, 1.$$

Here we have a partition

$$Z_N = \{0, n, \ldots, (2^m-1)n\} \cup \bigcup_{j=0}^{2^m-1} H_{j,0} \cup H_{j,1},$$
$$H_{j,i} \cap H_{l,k} = \emptyset \text{ for all } j \neq l, i \neq k.$$

In the following subsection we construct sequences with high linear complexity using this partition. The number of classes in this partition is always divisible by four.

A. The design of sequences with high linear complexity

As earlier, let $\mathbb{F}_4 = \{0, 1, \mu, \mu+1\}$ be a finite field of order four. By assigning the elements of $\mathbb{F}_4$ to each of generalized cyclotomic classes with respect to Z_N, one obtains a quaternary sequence of length N naturally. However, in order to guarantee that the constructed sequences have high linear complexity, one should do it specially.

In our case $N = 2^m n$, hence over $\mathbb{F}_4$ we have

$$L = N - \deg \gcd\left((x^n-1)^{2^m}, S(x)\right). \quad (6)$$

Let β be a primitive nth root of unity in the extension of $\mathbb{F}_4$. Then, according to (6), in order to find the minimal polynomial and the linear complexity of $\{s_i\}$ it is sufficient to find the zeros of $S(x)$ in the set $\{\beta^v, v = 0, 1, \ldots, n-1\}$ and determine their multiplicity. In order to investigate the values of $S(\beta^v)$, let us introduce subsidiary polynomials. Let $S_A(x) = \sum_{i \in A} x^i$, where A is a subset of Z_n or Z_N.

Lemma 10: If $1 \leq v \leq n-1$ then $S_{C_0}(\alpha^v) + S_{C_1}(\alpha^v) = 1$.

Proof: From our definition it follows that $S_{C_0}(\alpha^v) + S_{C_1}(\alpha^v) = \sum_{i=1}^{n-1} \alpha^{vi}$. ∎

Lemma 11: If $0 \leq v \leq n-1$ then $S_{H_{j,i}}(\alpha^v) = S_{C_i}(\alpha^v)$.

Proof: By definitions $S_{H_{j,i}}(\alpha^v) = \sum_{i \in H_{j,i}} \alpha^{vi}$ and $H_{j,i} \bmod p = C_i$. This completes the proof of Lemma 11. ∎

1) The sequences with a period $2n$: Let a, b, c, d belong to $\mathbb{F}_4$ and a, b, c, d are pairwise distinct. We construct a sequence with the first $2n$ terms of sequence $\{s_i\}$ defined as

$$s_i = \begin{cases} 0, & \text{if } i = 0, \\ a, & \text{if } i \in H_{0,0}, \\ b, & \text{if } i \in H_{0,1}, \\ c, & \text{if } i \in H_{1,0}, \\ d, & \text{if } i \in H_{1,1}, \\ e, & \text{if } i = n. \end{cases} \quad (7)$$

for $e \neq c + d$. The sequence defined by (7) is balanced for $e \neq 0$.

Remark 12: If $n = p^k$ then this sequence equals the sequence from [12] for $p \equiv \pm 1 (\bmod 8)$ and when replacing $\{c, d\}$ with $\{d, c\}$ for $p \equiv \pm 3 (\bmod 8)$.

Theorem 13: Let $\{s_i\}$ be defined by (7) for $e \neq c + d \in \mathbb{F}_4, e \neq 0$. Then $L = N$ and $m(x) = x^N - 1$.

Proof: Let us show that $S(\beta^v) \neq 0$ for $v = 0, 1, \ldots, n-1$. By (7) we have

$$S(x) = ex^N + a\sum_{i \in H_{0,0}} x^i + b\sum_{i \in H_{0,1}} x^i + c\sum_{i \in H_{1,0}} x^i + d\sum_{i \in H_{1,1}} x^i.$$

Let $1 \leq v \leq n-1$. By Lemma 11 we obtain

$$S(\beta^v) = e + aS_{C_0}(\beta^v) + bS_{C_1}(\beta^v) + cS_{C_0}(\beta^v) + dS_{C_1}(\beta^v)$$

or by Lemma 10 $S(\beta^v) = e + (a+b+c+d)S_{C_0}(\beta^v) + b + d$. By definition $a + b + c + d = 0 + 1 + \mu + \mu^2 = 0$. Thus, the above expression is equivalent to following $S(\beta^v) = e + b + d$. So, $S(\beta^v) \neq 0, 1 \leq v \leq n-1$.

To conclude the proof, it remains to note that $S(1) = e + (a+b+c+d)(n-1)/2$. ∎

In conclusion of the subsection we say a couple of words about the case when $e = b + d$. Here $\beta^v S'(\beta^v) = b + (a+b)S_{C_0}(\beta^v)$. So, in general case when $n \neq p^k$ it is possible that $|S'(\beta^v) = 0, 1 \leq v \leq n-1| > (n-1)/2$, i.e., L can be less than $(n+3)/2$ ($L \geq (n+3)/2$ for $n = p^k$ [12]).

2) The sequences with a period $4n$: Let as earlier, a, b, c, d be a permutation of the elements of $\mathbb{F}_4$. We consider a sequence $\{s_i\}$ defined by

$$s_i = \begin{cases} a, & \text{if } i \in H_{0,0} \cup H_{1,0} \cup \{0\}, \\ b, & \text{if } i \in H_{2,0} \cup H_{0,1} \cup \{n\}, \\ c, & \text{if } i \in H_{3,0} \cup H_{1,1} \cup \{2n\}, \\ d, & \text{if } i \in H_{2,1} \cup H_{3,1} \cup \{3n\}. \end{cases} \quad (8)$$

The sequence defined by (4) is balanced.

Theorem 14: Let $\{s_i\}$ be defined by (8). Then $L = N - 1$ and $m(x) = (x^N - 1)/(x - 1)$.

Proof: Similarly as in Theorem 13, by Lemmas 10 and 11 we obtain $S(\beta^v) = b + c$. Hence, $S(\beta^v) \neq 0$ for $v = 0, 1, \ldots, n-1$. By definition $S(1) = (a+b+c+d)(n+1) = 0$.

Further, $xS'(x) = a\sum_{i \in H_{1,0}} x^i + bx^n + c\sum_{i \in H_{3,0}} x^i + c\sum_{i \in H_{1,1}} x^i + d\sum_{i \in H_{3,1}} x^i + dx^{3n}$. So, $S'(1) = (a+d)(n-1)/2 + b + d$, i.e. $S'(1) \neq 0$. ∎

3) The general construction: Let j_1, j_2, j_3, j_4 be pairwise distinct integers between 0 and $2^m - 1$. We consider a subsidiary subsequence $\{t_i\}$ defined as

$$t_i = \begin{cases} a, & \text{if } i \in H_{j_1,0} \cup H_{j_2,1} \cup \{j_1 n\}, \\ b, & \text{if } i \in H_{j_2,0} \cup H_{j_3,1} \cup \{j_2 n\}, \\ c, & \text{if } i \in H_{j_3,0} \cup H_{j_4,1} \cup \{j_3 n\}, \\ d, & \text{if } i \in H_{j_4,0} \cup H_{j_0,1} \cup \{j_4 n\}, \\ 0, & \text{otherwise.} \end{cases} \quad (9)$$

Put, by definition $F_t(x) = \sum_{l=0}^{N-1} t_l x^l$.

Lemma 15: If $0 \leq v \leq n-1$ then $F_t(\alpha^v) = 0$.

Lemma 15 may be proved similarly as Theorem 13.

Now we will give a general definition of sequence with a period $N = 2^m n, m > 2$. If $m > 2$ then we can take the partition $\{4, \ldots, 2^m - 1\} = \cup_{k=1}^{2^{m-2}-1} I^{(k)}$, where $I^{(k)} = (j_1^{(k)}, j_2^{(k)}, j_3^{(k)}, j_4^{(k)})$ and $\{j_l^{(k)}\}, l = 1, 2, 3, 4; k =$

$1, \ldots, 2^{m-2}-1$ are pairwise distinct integers of the same parity between 4 and 2^m-1. Put, by definition

$$u = s + \sum_{k=1}^{2^{m-2}-1} t^{(k)} \tag{10}$$

where s is defined by (8) and $t^{(k)}$ is defined by (9) for $I^{(k)} = (j_1^{(k)}, j_2^{(k)}, j_3^{(k)}, j_4^{(k)})$. By Theorem 14 and Lemma 15 we obtain the following statement.

Theorem 16: Let $\{u_i\}$ be defined by (10). Then $L = N-1$ and $m(x) = (x^N-1)/(x-1)$.

IV. Conclusion

In this paper, we consider using Ding-Helleseth cyclotomy to design sequences over the finite field of order four with high linear complexity. We propose a method of constructing sequences with high linear complexity and arbitrary even period. These sequences are obtained by means of generalized Ding-Helleseth cyclotomy of order two. Also, using Ding-Helleseth cyclotomy of order four we construct balanced sequences over $\mathbb{F}_4$ with high linear complexity for series of odd periods. A problem of designing balanced sequences over the finite field of order four with high linear complexity and any odd period remains unsolved. The sequences with high linear complexity are significant for cryptographic applications.

We generalize design of the sequences over the finite field of order four proposed by Ke et al.[12]. Our method of designing sequences is different from the one proposed in the papers [4], [1], [15].

References

[1] Z. Chang, D. Li. "On the linear complexity of quaternary cyclotomic sequence of length 2pq". *IEICE Transactions on Fundamentals*, vol. E97-A(2), pp. 679–684, 2014.

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

[3] C. Ding, T. Helleseth. "New generalized cyclotomy and its applications". *Finite Fields and Their Applications*. vol.4(2), pp. 140–166, 1998.

[4] X. Du, Z. Chen. "Linear complexity of quaternary sequences generated using generalized cyclotomic classes modulo 2p". *IEICE Trans. Fundamentals*, vol. E94-A(5), pp. 1214–1217, 2011.

[5] 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.

[6] 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), pp. 75-84, 2010translation from Diskretn. Mat. 22(4)(2010) 74-82.

[7] V. Edemskiy. "Design Sequences over the Finite Field of Order Four with High Linear Complexity and Arbitrary Even Period", *Proc. of the 2015 International Conference on Applied Mathematics, Computational Science & Engineering (AMCSE 2015)*, Agios Nikolaos, Crete, Greece, October 17-19, 2015, pp. .

[8] V. Edemskiy, A. Ivanov. "Linear complexity of quaternary sequences of length pq with low autocorrelation". *Journal of Computational and Applied Mathematics*., vol. 259, pp. 555-560, 2014

[9] C. Fan, G. Ge. "A unified approach to Whiteman's and Ding-Helleseth's generalized cyclotmy over residue class rings". *IEEE Transactions Inform Theory* , vol. 60, pp. 1326– 1336, 2014.

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

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

[12] P. Ke, S. Zhang. "New classes of quaternary cyclotomic sequence of length $2p^m$ with high linear complexity". *Information Processing Letters*. vol. 112, pp. 646–650, 2012.

[13] J.J. Komo, L.L. Joiner. *QPSK sequences over* F_4, in: ISIT. Washington. DC, 2001

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

[15] D. Li, Z. Chang, Q. Wen and J. Zhang. "Linear Complexity of Generalized Cyclotomic Quaternary Sequences of Length $2p^{m+1}q^{n+1}$". *IET Information Security.*DOI: 10.1049/iet-ifs.2015.0006 , Online ISSN 1751-8717 Available online: 07 September 2015

[16] A. L. Whiteman, A family of difference sets,. *Illinois J. Math.*, 6, pp.107-121, 1962.