EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 7, No. 3, 2014, 256-266
ISSN 1307-5543 – www.ejpam.com

On the Linear Complexity of Ding-Helleseth Generalized Cyclotomic Binary Sequences of Order Four and Six

Vladimir Edemskiy *, Olga Antonova

Department of Applied Mathematics and Informatics, Novgorod State University, Veliky Novgorod, Russia

Abstract. We propose a new computation method for the linear complexity and the minimal polynomial of Ding-Helleseth-generalized cyclotomic sequences. We will find the linear complexity of Ding-Helleseth-generalized cyclotomic sequences of order four and six and make the results of Tongjiang Yan *et. al* [19] about the sequences of order four more specific.

2010 Mathematics Subject Classifications: 11B50, 94A55, 94A60

Key Words and Phrases: Stream ciphers, Sequences, Generalized cyclotomy, Linear complexity, Minimal polynomial

1. Introduction

Pseudo-random sequences are widely used in many fields, in particular in stream ciphers [3]. The linear complexity of a sequence s^∞ is an important characteristic of its quality. It is defined to be the length of the shortest linear feedback shift register that can generate the sequence [14]. Sequences with high linear complexity ($L(s^\infty) > N/2$, where N denotes the period of the sequence) are important for cryptographic applications.

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 [3]. As we all know, certain classical cyclotomic sequences, such as Legendre sequences and Hall sextic residue sequences, possess good linear complexity and autocorrelation properties (see [8, 11, 13, 16]). A generalized cyclotomy with respect to pq was introduced by Whiteman [17]. New generalized cyclotomic sequences (D-GCS$_{2k}$, where $2k$ is the order) including classical as particular, were defined by Ding and Helleseth in [7]. They predicted that they may be applied in cryptography and coding [5, 6]. Further it was shown that such sequences might have poor autocorrelation properties. It makes them difficult to use in Engineering [2, 15].

*Corresponding author.

Email address: Vladimir.Edemsky@novsu.ru (V. Edemskiy)

The D-GCS$_2$ with period pq (where p and q are distinct odd primes) have high linear complexity [1, 4]. Later, the linear complexity of the D-GCS$_4$ with period pq was calculated in [19]. However there are some technical errors in [19], (Lemma 4), which led to wrong results in some parts of the Theorem 2 in [19] and casting doubt on the method of this article (see appendix). Note that in [18] T. Yan mentions his previous work [19] has an error, but does not indicate exactly where it is and how to correct it.

The purpose of this paper is to propose a new computation method for the linear complexity and the minimal polynomial of Ding-Helleseth-generalized cyclotomic sequences. We show that computation of the linear complexity of generalized cyclotomic sequences with period pq reduces to exploration of the classical cyclotomic sequences polynomial and obtain the linear complexity of Ding-Helleseth-generalized sequences of order four and six.

We retain notation used in [19]. Let p and q be two odd primes with $\gcd(p-1,q-1)=d$. Define $N=pq$, $e=(p-1)(q-1)/d$. The Chinese Remainder Theorem guarantees that there exists a common primitive root, g, of both p and q, and the order of g modulo N is e. Let x be an integer satisfying $x\equiv g(\mathrm{mod}\ p)$, and $x\equiv 1(\mathrm{mod}\ q)$. Thus, we can get a subgroup of the residue ring, Z_N, with its multiplication [17], as the following:

$$Z_N^*=\{g^i x^j : i=0,1,\dots e-1; j=0,1,\dots,d-1\}.$$

Ding-Helleseth generalized cyclotomic classes of order d with respect to p and q are defined as

$$D_i=\{g^{i+dt}x^j : t=0,1,\dots e/d-1; j=0,1,\dots,d-1\},$$

where $i=0,1,\dots d-1$ [7]. Then $Z_N^*=\bigcup_{i=0}^{d-1}D_i$, $D_i\cap D_j=\varnothing$ for $i\neq j$, where $\varnothing$ denotes the empty set.

By definition, put

$$D_i^{(p)}=\{g^{dt+i} : t=0,1,\dots (p-1)/d-1\}, D_i^{(q)}=\{g^{dt+i} : t=0,1,\dots (q-1)/d-1\}$$

and $P_i=pD_i^{(q)}$, $Q_i=qD_i^{(p)}$, where $i=0,1,\dots d-1$.

Let $C_0=\bigcup_{i=0}^{d/2-1}\left(D_i\cup P_i\cup Q_i\right)\cup\{0\}$, $C_1=\bigcup_{i=d/2}^{d-1}\left(D_i\cup P_i\cup Q_i\right)$ then $Z_{pq}=C_0\cup C_1$ and $C_0\cap C_1=\varnothing$.

Ding-Helleseth-generalized cyclotomic sequence of order d (D-GCS$_d$), with $s^\infty=\{s_0,s_1,\dots,s_i,\dots\}$ is defined as

$$s_i=\begin{cases}1, & \text{if } i \bmod N\in C_1,\\ 0, & \text{otherwise.}\end{cases}.$$

Then s^∞ possesses the minimum period pq, and the almost balance of the symbols 1s and 0s.

2. A Computation Method for Linear Complexity of Ding-Helleseth-Generalized Cyclotomic Sequences with Period pq

For a binary sequence, s^∞, with period N, if $S_N(x)=s_0+s_1x+\ldots+s_{N-1}x^{N-1}$, then its minimal polynomial and linear complexity can be calculated by the following equations [14]:

$$m(x)=(x^N-1)/[\gcd(x^N-1,S_N(x))]. \tag{1}$$

$$L(s^{\infty}) = N - \deg[\gcd(x^N - 1, S_N(x))]. \quad (2)$$

Let α be a primitive N-th root of unity over the field $GF(2^m)$ that is the splitting field of $x^N - 1$. Then, by (2), we have

$$L(s^{\infty}) = N - \left|\{j \ \left| S(\alpha^j) = 0, j = 0, 1, \ldots, N-1\}\right|\right. . \quad (3)$$

where $S(x)$ is defined by $S(x) = \sum_{i \in C_1} x^i$. So, the computation of the linear complexity and the minimal polynomial of the sequence s^{∞} turns into the computation of roots of its polynomial.

Let $\beta = \alpha^q$ and $\gamma = \alpha^p$, then β and γ are primitive p-th and q-th roots of unity in the extension of field $GF(2)$. There exist integers a, b [12], such that

$$aq + bp = 1. \quad (4)$$

Then

$$\alpha = \beta^a \gamma^b. \quad (5)$$

Let $ind_g^{(q)} c$ be discrete logarithm of c in the field $GF(q)$ relative to the basis g. By definition of the discrete logarithm $p \equiv g^{ind_g^{(q)} p} (\mathrm{mod} q)$, hence from (4) we have

$$b \equiv g^{-ind_g^{(q)} p} (\mathrm{mod} q). \quad (6)$$

To explore the properties of the polynomial $S(x)$, let us introduce auxiliary polynomials $S_d(x) = \sum_{u \in D_0^{(p)}} x^u$ and $T_d(x) = \sum_{v \in D_0^{(q)}} x^v$. Properties of polynomials $S_d(x)$ and $T_d(x)$ are obtained in [9, 10] (see also [8, 13]). In particular from [9] we have

$$\sum_{u \in D_j^{(p)}} \beta^u = S_d(\beta^{g^j}), \ \sum_{v \in D_i^{(q)}} \gamma^v = T_d(\gamma^{g^i}) \quad (7)$$

and

$$S_d(\beta) + S_d(\beta^g) + \ldots + S_d(\beta^{g^{d-1}}) = 1, T_d(\gamma) + T_d(\gamma^g) + \ldots + T_d(\gamma^{g^{d-1}}) = 1. \quad (8)$$

The following Lemmas 1 - 3 are needed to prove Theorem 1.

By definition, put $D_{j,i} = \{g^{i+td} x^{j-i} : t = 0, 1, \ldots e/d - 1\}$, where $j, i = 0, 1, \ldots, d-1$.

Lemma 1. *Let the symbols be the same as before.*

For $i, j = 0, 1, \ldots, d-1$ and $k = 1, 2, \ldots, pq-1$ we have

$$\sum_{u \in D_{j,i}} \alpha^{ku} = S_d(\beta^{akg^j}) T_d(\gamma^{bkg^i}).$$

Proof. By (5), definitions of $D_{j,i}$ and x we have $\sum_{u \in D_{j,i}} \alpha^{ku} = \sum_{t=0}^{e/d-1} \beta^{akg^{j+dt}} \gamma^{bkg^{i+dt}}$. By definition $\gcd(p-1, q-1) = d$, then $Z_{e/d} \cong Z_{(p-1)/d} \times Z_{(q-1)/d}$ relatively to isomorphism $\varphi(a) = (a \bmod (p-1)/d), a \bmod (q-1)/d)$ [12]. Hence $\sum_{u \in D_{j,i}} \alpha^{ku} = \sum_{v \in D_j^{(p)}} \beta^{akv} \sum_{w \in D_i^{(q)}} \gamma^{bkw}$. Application of (7) concludes the proof of Lemma 1. □

Lemma 2. *Let the symbols be the same as before.*
For $i = 0, 1, \dots, d-1$ and $k = 1, 2, \dots, pq-1$ we have

$$\sum_{u \in P_i} \alpha^{ku} = T_d(\gamma^{kg^i}).$$

Proof. By definition of P_i we have $\sum\limits_{u \in P_i} \alpha^{ku} = \sum\limits_{v \in D_i^{(q)}} \alpha^{kpv}$. Using (7) and definition $\gamma = \alpha^p$, we obtain $\sum\limits_{v \in D_i^{(q)}} \alpha^{kpv} = T_d(\gamma^{kg^i})$. Lemma 2 is proved. □

Lemma 3 can be shown in a similar way.

Lemma 3. *Let the symbols be the same as before.*
For $j = 0, 1, \dots, d-1$ and $k = 1, 2, \dots, pq-1$ we have

$$\sum_{u \in Q_j} \alpha^{ku} = S_d(\beta^{kg^j}).$$

Now we can prove the basic theorem about the linkage of the linear complexity of Ding-Helleseth-generalized cyclotomic sequences with the values of the polynomials of the classical sequences.

Theorem 1. *Let the symbols be the same as before.*
If $k = 1, 2, \dots, pq-1$, then

$$S(\alpha^k) = \sum_{i=d/2}^{d-1} \left(T_d\left(\gamma^{kg^{i-ind_g^{(q)}p}}\right)\delta + T_d(\gamma^{kg^i}) + S_d(\beta^{kg^i}) \right),$$

where

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

Proof. By definition of the sequence s^∞ we have

$$S(\alpha^k) = \sum_{i=d/2}^{d-1} \left(\sum_{u \in D_i} \alpha^{ku} + \sum_{u \in P_i} \alpha^{ku} + \sum_{u \in Q_i} \alpha^{ku} \right). \tag{9}$$

We consider the first item of this sum. By definition $D_i = \bigcup_{j=0}^{d-1} D_{j,i}$, hence $\sum\limits_{u \in D_i} \alpha^{ku} = \sum\limits_{j=0}^{d-1} \left(\sum\limits_{t \in D_{j,i}} \alpha^{kt} \right)$, then by Lemma 1 we have $\sum\limits_{u \in D_i} \alpha^{ku} = \sum\limits_{j=0}^{d-1} S_d(\beta^{kag^j}) T_d(\gamma^{kbg^i})$.

If $k \not\equiv 0(\mathrm{mod}p)$, then from (8) we obtain $\sum_{f=0}^{d-1} S_d(\beta^{kag^f}) = 1$. Yet, if $k \equiv 0(\mathrm{mod}p)$, then $\sum\limits_{f=0}^{d-1} S_d(\beta^{kag^f}) = p-1$ and $p-1 \equiv 0(\mathrm{mod}2)$. Thus, the first item of (9) is equal to $\delta \sum\limits_{i=d/2}^{d-1} T_d(\gamma^{kbg^i})$.

The sum of the second and the third items is $\sum\limits_{i=d/2}^{d-1} \left(T_d(\gamma^{kg^i}) + S_d(\beta^{kg^i}\right)$ by Lemmas 2 and 3. Application of (6) concludes the proof of Theorem 1 □.

To sum up, we can note, that by Theorem 1, the computation of the values of the sequence polynomial $S(x)$ and, therefore, the computation of the linear complexity of the sequence s^∞ turns into the computation of the values $S_d(x)$ and $T_d(x)$ for cyclotomic classes members.

By Theorem 1, for fixed j and i, the values of $S(\alpha^k)$ are the same for all $k \in D_{j,i}$; for fixed i, the values of $S(\alpha^k)$ are same for all $k \in P_i$; for fixed i, the values of $S(\alpha^k)$ are same for all $k \in Q_i$. Then the matrix $\mathbf{S} = (s_{ij})$ of order $d+1$ is well defined, where $s_{ji} = S(\alpha^k)$, if $k \in D_{j,i}$ and $s_{dj} = S(\alpha^k)$, if $k \in P_j$; $s_{id} = S(\alpha^k)$, if $k \in Q_i$; $i, j = 0, 1, \ldots, d-1$, $s_{dd} = S(1)$. Let us note that in order to compute the linear complexity of sequences s^∞ and $m(x)$ it suffices to define the zero elements of the matrix $\mathbf{S}$.

Additionally we note that Theorem 1 also allows to evaluate the linear complexity of the sequence s^∞ as it was done in [18].

Later on, for the convenience of computations of the matrix $\mathbf{S}$ we introduce the following notations:

$$\mathbf{S}_d(x) = \left(S_d(x), S_d(x^g), \ldots, S_d(x^{g^{d-1}}), S_d(1)\right),$$
$$\mathbf{T}_d(x) = \left(T_d(x), T_d(x^g), \ldots, T_d(x^{g^{d-1}}), T_d(1)\right).$$

Let $\mathbf{A}_d(x) = \sum\limits_{i=d/2}^{d-1} \mathbf{S}_d(x^{g^i})$ and $\mathbf{B}_d(x) = \sum\limits_{i=d/2}^{d-1} \mathbf{T}_d(x^{g^i})$.

Then immediately from Theorem 1 we obtain the following:

Lemma 4. *Let the symbols be the same as before. Then we have*

$$\mathbf{S} = \begin{pmatrix}1 & \ldots & 1 & 0\end{pmatrix}^T \boldsymbol{B}_d\left(\gamma^{g^{-ind_g^{(q)}p}}\right) + \begin{pmatrix}1 & 1 & \ldots & 1\end{pmatrix}^T \boldsymbol{B}_d(\gamma) + \boldsymbol{A}_d^T(\beta)\begin{pmatrix}1 & \ldots & 1\end{pmatrix}, \quad (10)$$

where $\mathbf{A}^T$ *is a transposed matrix* $\mathbf{A}$.

The method of computation $\mathbf{S}_d(\beta)$ and $\mathbf{T}_d(\gamma)$ by using explicit formulas for computation of cyclotomic numbers was proposed in [9, 10]. Using Theorem 1 in the next sections we will obtain new results of the linear complexity of Ding-Helleseth-generalized sequences of order four and six.

3. The Linear Complexity and the Minimal Polynomial of D-GCS$_4$

For $d=4$ there is an expansion $p=x^2+4y^2$, where x,y are integers and $x\equiv 1(\mathrm{mod}4)$ [12]. In [9] the values of the polynomial $S_4(\beta)\big(T_4(\gamma)\big)$ are computed depending on x,y.

Let $\left(\frac{2}{p}\right)_4$ and $\left(\frac{2}{p}\right)_2$ denote the symbols of the 4th residues and 2th residues of p respectively. The following Lemma 5 is needed to prove Theorem 2.

Lemma 5. *Let the symbols be the same as before.*

(i) If $\left(\frac{2}{p}\right)_4=1$, *then* $\mathbf{A}_4(\beta)=(0,0,1,1,0)$ *or* $\mathbf{A}_4(\beta)=(1,1,0,0,0)$.

(ii) If $\left(\frac{2}{p}\right)_2=1$ *and* $\left(\frac{2}{p}\right)_4\neq 1$, *then* $\mathbf{A}_4(\beta)=(\mu,\mu+1,\mu+1,\mu,0)$, *where* μ *meets the rule* $\mu^2+\mu+1=0$.

(iii) If $\left(\frac{2}{p}\right)_2\neq 1$, *then* $\mathbf{A}_4(\beta)=(\eta,\eta^2,\eta^4,\eta^8,0)$ *or* $\mathbf{A}_4(\beta)=(\eta,\eta^8,\eta^4,\eta^2,0)$, *where* η *meets the condition* $\eta^4+\eta+1=0$.

Proof. By definition $\mathbf{A}_4(\beta)=\mathbf{S}_4(\beta^{g^2})+\mathbf{S}_4(\beta^{g^3})$. Consequently, to prove Lemma 5 it is sufficient to give the values of $\mathbf{S}_4(\beta)$ for each option.

(i) If $\left(\frac{2}{p}\right)_4=1$, then $y\equiv 0(\mathrm{mod}4)$ [12]. In this case, by [9] we have $\mathbf{S}_4(\beta)=(1,1,0,1,0)$ for $x\equiv 5(\mathrm{mod}8)$ or $\mathbf{S}_4(\beta)=(1,0,0,0,0)$ for $x\equiv 1(\mathrm{mod}8)$.

(ii) If $\left(\frac{2}{p}\right)_2=1$ and $\left(\frac{2}{p}\right)_4\neq 1$, then $\mathbf{S}_4(\beta)=(\mu,0,\mu+1,0,0)$ for $x\equiv 5(\mathrm{mod}8)$ or $\mathbf{S}_4(\beta)=(\mu,1,\mu+1,1,0)$ for $x\equiv 1(\mathrm{mod}8)$, where μ meets the rule $\mu^2+\mu+1=0$ [9].

(iii) If $\left(\frac{2}{p}\right)_2\neq 1$, then $\mathbf{S}_4(\beta)=(\zeta,\zeta^2,\zeta^4,\zeta^8,1)$ or $\mathbf{S}_4(\beta)=(\zeta,\zeta^8,\zeta^4,\zeta^2,1)$, where ζ meets the condition $\zeta^8+\zeta^4+\zeta^2+\zeta+1=0$. In this case $\eta=\zeta^4+\zeta^8$ or $\eta=\zeta^4+\zeta^2$ [9].

After summing of we obtain the statement of Lemma 5 for all cases. □

If $\left(\frac{2}{p}\right)_4=1$ or $\left(\frac{2}{q}\right)_4=1$, then by Lemmas 2, 3 $S(\alpha^q)\in\{0,1\}, S(\alpha^p)\in\{0,1\}$ [9]. We can change α and without loss of generality assume that $S(\alpha^q)=S(\alpha^{qg})=0$, if $\left(\frac{2}{p}\right)_4=1$ and $S(\alpha^p)=S(\alpha^{pg})=0$, if $\left(\frac{2}{q}\right)_4=1$.

Let $D_i(x)=\prod_{i\in D_i}(x-\alpha^i)$, $P_i(x)=\prod_{i\in P_i}(x-\alpha^i)$ and $Q_i(x)=\prod_{i\in Q_i}(x-\alpha^i); i=0,1,2,3$.

Theorem 2. *Let the symbols be the same as before.*

(i) If $\left(\frac{p}{q}\right)_2=1$ *and* $\left(\frac{2}{p}\right)_4=1$, *then* $L(s^\infty)=q(p+1)/2-1$, $m(x)=(x^{pq}-1)/\big((x-1)D_0(x)D_1(x)Q_0(x)Q_1(x)\big)$.

(ii) If $\left(\frac{p}{q}\right)_2\neq 1$ *and* $\left(\frac{2}{p}\right)_4=1$, *then* $L(s^\infty)=pq-(p+1)/2$, $m(x)=(x^{pq}-1)/\big((x-1)Q_0(x)Q_1(x)\big)$.

(iii) *If* $\left(\frac{2}{q}\right)_4 = 1$, *then* $L(s^\infty) = pq-(q+1)/2$, $m(x) = (x^{pq}-1)\big((x-1)P_0(x)P_1(x)\big)$.

(iv) *If* $\left(\frac{2}{p}\right)_4 \neq 1$ *and* $\left(\frac{2}{q}\right)_4 \neq 1$, *then* $L(s^\infty) = pq-1$, $m(x) = (x^{pq}-1)/(x-1)$.

Proof. We will employ Theorem 2 to determine the values of the matrix **S**.

(i) By assumption $\gcd(p-1,q-1)=4$, consequently $\left(\frac{2}{q}\right)_2 \neq 1$ for $\left(\frac{2}{p}\right)_4 = 1$ [12]. In this case by Lemma 6 we have $\mathbf{A}_4(\beta)=(0,0,1,1,0)$ or $\mathbf{A}_4(\beta)=(1,1,0,0,0)$ and $\mathbf{B}_4(\gamma)=(\eta,\eta^2,\eta^4,\eta^8,0)$ or $\mathbf{B}_4(\gamma)=(\eta,\eta^8,\eta^4,\eta^2,0)$.
Now, if $\left(\frac{p}{q}\right)_2 = 1$, then $ind_g^{(q)}p \equiv 0(\mathrm{mod}4)$ or $ind_g^{(q)}p \equiv 2(\mathrm{mod}4)$. In the first case $\mathbf{B}_d\left(\gamma^{g^{-ind_g^{(q)}p}}\right)+\mathbf{B}_d(\gamma)=(0,0,0,0,0,0)$ and in the second case $\mathbf{B}_d\left(\gamma^{g^{-ind_g^{(q)}p}}\right)+\mathbf{B}_d(\gamma)=(1,1,1,1,0)$. Thus, by Lemma 5 we can deduce that the first two rows of the matrix **S** consist of zeros, also $s_{44}=0$, and all other entries are non-zero. Hence,

$$\left|\{j \ \left|S(\alpha^j)=0, j=0,1,\ldots,N-1\}\right.\right| = 2\left|D_i\right| + 2\left|Q_i\right| + 1 = q(p-1)/2+1$$

and by (3) $L(s^\infty)=q(p+1)/2-1$. From (1) we have

$$m(x)=(x^{pq}-1)/\big((x-1)D_0(x)D_1(x)Q_0(x)Q_1(x)\big)$$

by the choice of α.

(ii) In this case the expressions for $\mathbf{A}_4(\beta)$ and $\mathbf{B}_4(\gamma)$ are the same as in (1), but when $\left(\frac{p}{q}\right)_2 \neq 1$ we have $ind_g^{(q)}p \equiv 1(\mathrm{mod}4)$ or $ind_g^{(q)}p \equiv 3(\mathrm{mod}4)$. Hence $\mathbf{B}_d\left(\gamma^{g^{-ind_g^{(q)}p}}\right)+\mathbf{B}_d(\gamma)=(b_0,b_1,b_2,b_3,0)$ and $b_j\neq 0$, $b_j\neq 1$ for $j=1,2,3,4$. Then by Lemma 4 we have $s_{04}=s_{14}=s_{44}=0$, and all other entries of **S** are non-zero. Therefore, $\left|\{j \ \left|S(\alpha^j)=0, j=0,1,\ldots,N-1\}\right.\right| = 2\left|Q_i\right|+1=(p+1)/2$. From (1) and (3), it follows that $L(s^\infty)=pq-(p+1)/2$ and $m(x)=(x^{pq}-1)/\big((x-1)Q_0(x)Q_1(x)\big)$.

Statements of (iii) and (iv) can be proved in the same way. □

From Theorem 2 we can obtain that if $\left(\frac{2}{p}\right)_4 = 1$, then the linear complexity of D-GCS$_4$ depends on value $\left(\frac{p}{q}\right)_2$. For example, if $p=73, q=5$ or $p=73, q=101$, then $\left(\frac{73}{5}\right)_2 \neq 1$ and $\left(\frac{73}{101}\right)_2 \neq 1$, hence $L(s^\infty)=pq-(p+1)/2=328$ or $L(s^\infty)=7336$, respectively. Yet, if $p=89, q=5$ or $p=73, q=173$, then $\left(\frac{89}{5}\right)_2=1$ and $\left(\frac{73}{173}\right)_2=1$ hence $L(s^\infty)=q(p+1)/2-1=224$ or $L(s^\infty)=6400$ respectively. These facts can be easily obtained by means of calculation of the linear complexity of D-GCS$_4$ using, for example, the Berlekamp-Massey algorithm [14]. Thus, Theorem 2 from [19] is not true.

4. The Linear Complexity of D-GCS$_6$

Let $d=6$, the values of the polynomial $S_6(\beta)\big(T_6(\gamma)\big)$ are computed in [9]. Similar to the proof of Theorem 2, we can prove the following Theorem 3.

Theorem 3. *Let the symbols be the same as before.*

(i) If $\left(\frac{2}{p}\right)_6 = 1$ *and* $\left(\frac{2}{q}\right)_6 = 1$*, then* $L(s^\infty) = (pq+1)/2 - \Delta$*;*

(ii) If $\left(\frac{2}{p}\right)_6 = 1$*;* $\left(\frac{2}{q}\right)_6 \neq 1$ *and* $\left(\frac{p}{q}\right)_3 = 1$ *or* $\left(\frac{2}{p}\right)_6 = 1$*;* $\left(\frac{2}{q}\right)_3 = 1$ *and* $\left(\frac{2}{q}\right)_2 \neq 1$*;* $\left(\frac{p}{q}\right)_3 \neq 1$*, then* $L(s^\infty) = (p+1)q/2 - \Delta$*, where* $\Delta = \begin{cases} 1, & \text{if } S(1) = 0, \\ 0, & \text{otherwise} \end{cases}$*;*

(iii) If $\left(\frac{2}{p}\right)_6 = 1$*;* $\left(\frac{2}{q}\right)_3 \neq 1$ *and* $\left(\frac{p}{q}\right)_3 \neq 1$ *then* $L(s^\infty) = pq - (p-1)/2 - \Delta$*;*

(iv) If $\left(\frac{2}{q}\right)_6 = 1$ *and* $\left(\frac{2}{p}\right)_6 \neq 1$ *then* $L(s^\infty) = pq - (q-1)/2 - \Delta$*;*

(v) If $\left(\frac{2}{p}\right)_2 = 1$*;* $\left(\frac{2}{p}\right)_3 \neq 1$*;* $\left(\frac{2}{q}\right)_3 \neq 1$ *and* $\left(\frac{p}{q}\right)_3 \neq 1$*, then* $L(s^\infty) = pq - (p-1)(q-1)/6 - \Delta$*;*

(vi) If conditions (i)-(v) are not true, then $L(s^\infty) = pq - \Delta$*.*

Also we can obtain the minimal polynomial of DCS_6. Additionally we can note that for the case of (ii) the linear complexity of D-GCS_6 does not depend on the value $\left(\frac{p}{q}\right)_3$, but for the minimal polynomial this is not the case.

Our examples $p = 31, q = 127$; $p = 31, q = 19$ or $p = 31, q = 43$; $p = 31, q = 7$; $p = 7, q = 31$; $p = 7, q = 79$; $p = 13, q = 7$ shows that all the cases of Theorem 3 are possible.

5. Conclusion

For additive stream ciphering, the linear span of the keystream sequence must be large enough. This paper shows that almost all Ding-Helleseth-generalized cyclotomic sequences of order four or six with period pq have high linear complexity and almost ideal balance property. Long periods can also be obtained easily.

References

[1] E. Bai, X. Liu, and G. Xiao. Linear complexity of new generalized cyclotomic sequences of order two of length pq. *IEEE Transactions on Information Theory*, 51:1849–1853, 2005.

[2] Z. Chen and S. Li. Some Notes on Generalized Cyclotomic Sequences of Length pq. *Journal of Computer Science and Technology*, 23(5):843–850, 2008.

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

[4] C. Ding. Linear complexity of generalized cyclotomic binary sequences of order 2. *Finite Fields and Their Applications*, 3(2):159–174, 1997.

[5] C. Ding. Autocorrelation values of generalized cyclotomic sequences of order two. *IEEE Transactions on Information Theory*, 44(5):1699–1702, 1998.

[6] C. Ding. New generalized cyclotomy and its applications. *Finite Fields and Their Applications*, 4(2):140–166, 1998.

[7] C. Ding and T. Helleseth. Generalized cyclotomic codes of length $p_1^{e_1} \dots p_t^{e_t}$. *IEEE Transactions on Information Theory*, 45(2):467–474, 1999.

[8] C. Ding, T. Helleseth, and W. Shan. On the linear complexity of Legendre sequences. *IEEE Transactions on Information Theory*, 44:1276–1278, 1998.

[9] V.A. Edemskii. On the linear complexity of binary sequences on the basis of biquadratic and sextic residue classes. *Discrete Mathematics and Applications*, 20(1):75–84, 2010.

[10] V.A. Edemskiy. Linear complexity of ternary sequences formed on the basis of power residue classes. *Problems of Information Transmission.*, 44(4):287–294, 2008.

[11] M. Hall. A survey of difference sets. *Proceedings of the American Mathematical Society*, 7:975–986, 1056.

[12] K. Ireland and M. Rosen. *A Classical introduction to modern number theory.* Springer-Verlag, North-Holland Publishing Co., Amsterdam, 1982.

[13] J.H. Kim and H.Y. Song. On the linear complexity of halls sextic residue sequences. *IEEE Transactions on Information Theory*, 47(5):2094–2096, 2001.

[14] R. Lidl and H. Niederreiter. *Finite Fields.* Addison-Wesley Press, Massachusetts, 1983.

[15] W. Meidl. Remarks on a cyclotomic sequence. *Designs, Codes, and Cryptography*, 51(1):33–44, 2009.

[16] W. Meidl and A. Winterhof. On the autocorrelation of cyclotomic generators. In *Lecture Notes in Computer Science.*, volume 2948. Springer, Berlin, 2004.

[17] A.L. Whiteman. A family of difference sets. *Illinois Journal of Mathematics*, 6:107–121, 1962.

[18] T Yan. Linear complexity of ding-helleseth generalized cyclotomic binary sequences of any order. eprint arXiv 1108.4450, 2011.

[19] T. Yan, L. Hong, and G. Xiao. The linear complexity of new generalized cyclotomic binary sequences of order four. *Information Sciences*, 178(3):2094–2096, 2008.

Appendix

Let as in [19] $S^Q_{j(j+1)} = \sum_{i \in Q_j \bigcup Q_{j+1}} \alpha^i$ and $S^{PD}_{j(j+1)} = \sum_{i \in P_j \bigcup P_{j+1} \bigcup D_j \bigcup D_{j+1}} \alpha^i$ Then $S(\alpha) = S^Q_{23} + S^{PD}_{23}$ and the values of $S(\alpha^k)$ are given in Table 1 [19]. In particular, authors argue that $S(\alpha^k) = S^Q_{23} + S^{PD}_{23} + 1$, if $k \in D_2$ and $k(\text{mod p}) \in D_0^{(p)}$. We argue that this is not true.

By definition we have

$$S(\alpha^k)=\left(\sum_{i\in Q_2}+\sum_{i\in Q_3}+\sum_{i\in P_2}+\sum_{i\in P_3}+\sum_{i\in D_2}+\sum_{i\in D_3}\right)\alpha^{ki}$$

or

$$S(\alpha^k)=\left(\sum_{j\in kQ_2}+\sum_{j\in kQ_3}+\sum_{j\in kP_2}+\sum_{j\in kP_3}+\sum_{j\in kD_2}+\sum_{j\in kD_3}\right)\alpha^{j}.$$

If $k\in D_2$ and $k(\mathrm{mod}\ p)\in D_0^{(p)}$, then by Lemma 2 [19] we have $kQ_2=Q_2$; $kQ_3=Q_3$; $kP_2=P_0$; $kP_3=P_1$; $kD_2=D_0$; $kD_3=D_1$, hence $S(\alpha^k)=S_{23}^{Q}+S_{01}^{PD}$.

By Lemma 3 [19] we note that $\sum\limits_{i\in P_0\bigcup P_1}\alpha^i=\sum\limits_{i\in P_2\bigcup P_3}\alpha^i+1$ and $\sum\limits_{i\in D_0\bigcup D_1}\alpha^i=\sum\limits_{i\in D_2\bigcup D_3}\alpha^i+1$, then $S(\alpha^k)=S_{23}^{Q}+S_{23}^{PD}$.

The other errors in the Table can be shown in the same way. It is easy to test for $p=5$, $q=13$.

The technical errors in Lemma 4 led to wrong results in Lemma 7. If $2\in D_1$ and $2(\mathrm{mod}p)\in D_0^{(p)}$, then $4\in D_2$, $4(\mathrm{mod}p)\in D_0^{(p)}$ and $S(\alpha^4)=S^4(\alpha)=S(\alpha)$. In [19] $S(\alpha^4)=S^4(\alpha)=S(\alpha)+1$ and authors draw a conclusion that $S(\alpha)\notin\{0,1\}$. This is not true. Thus, proof of the main theorems in [19] is not complete.