Notes about the linear complexity of Ding-Helleseth generalized cyclotomic sequences of length pq over the finite field of order p or q

Vladimir Edemskiy[1,⋆] and *Nikita* Sokolovskiy[1]

[1] *Novgorod State University, Veliky Novgorod, Russia*

Abstract. We investigate three classes of Ding-Helleseth-generalized cyclotomic sequences of length pq. We derive the linear complexity and the minimal polynomial of above-mentioned sequences over the finite fields of orders p and q, where p and q are two odd distinct primes, and obtain series of sequences with high linear complexity.

1 Introduction

Pseudo-random sequences are widely used in many fields, in particular in stream ciphers [3]. The linear complexity is defined to be the length of the shortest linear feedback shift register that can generate the sequence [9]. The concept of the linear complexity of sequence is very useful in the study of the security of stream ciphers.

Cyclotomic sequences have good pseudo-random properties and have been widely used as keystreams in private-key cryptosystems. In [7], Ding and Helleseth introduced a generalized cyclotomy of order 2 with respect to odd modulo N, in particularly for $N = pq$, where p and q are two odd distinct primes. Further, this cyclotomy was generalized in series of papers. There are many works devoted to the study of the properties of Ding-Helleseth-generalized cyclotomic sequences and their use in cryptography and coding. So, the linear complexity of Ding-Helleseth-generalized cyclotomic sequences of length pq over the finite field of order two have been calculated in [4, 5, 10, 14, 15](see also references here). Further, Ding [6] investigated the linear complexity of the series of these sequences over the finite field $GF(l^m)$ where $\gcd(l, pq) = 1$, and constructed several classes of cyclic codes with optimal or almost optimal property. Wang et al. [11] derive the linear complexity of Ding-Helleseth sequences of order 2 over $GF(l)$ where $\gcd(l, pq) = 1$. Also, there are a long lot of articles devoted to the investigation the linear complexity of of Ding-Helleseth sequences of another orders over the different finite fields when a field's order and a sequence's period are relatively prime. At the same time, the linear complexity of cyclotomic sequences with period p over $GF(p)$ was investigated in [1, 2].

The purpose of this paper is to study the linear complexity of Ding-Helleseth sequences length pq over the finite fields of orders p and q. We find the linear complexity and the minimal polynomial of these generalized cyclotomic sequences.

2 Preliminaries

First, we briefly repeat the basic definitions and the general information. Let p and q be two odd distinct primes with $\gcd(p-1, q-1) = d$. Define $N = pq$, $e = (p-1)(q-1)/d$. We denote by Z_N the residue class ring modulo N and by Z_N^* the unit group of Z_N. 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 [8]. There also exists an integer x satisfying $x \equiv g (\mathrm{mod}\ p)$, and $x \equiv 1 (\mathrm{mod}\ q)$. By [13] we have

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

where the multiplication is that of Z_N^*.

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

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

$i = 0, 1, ...d-1$. Then

$$Z_N^* = \bigcup_{i=0}^{d-1} D_i, \quad D_i \cap D_j = \varnothing \text{ for } i \neq j,$$

where $\varnothing$ denotes the empty set.

By definition, put $P = \{p, 2p, \ldots, (q-1)p\}$, $Q = \{q, 2q, \ldots, (p-1)q\}$, and $R = \{0\}$. Define $C_0 = \bigcup_{i=0}^{d/2-1} D_{2i}$, $C_1 = \bigcup_{i=0}^{d/2-1} D_{2i+1}$. Then C_0, C_1 is a partition of Z_N^* and C_0, C_1, P, Q, and R is a partition of Z_N. Further, we investigate the linear complexity of three types of sequences based on the partition $Z_N^* = C_0 \cup C_1$.

It is well known that if $s = \{s_i\}$ is a sequence of period N, then the linear complexity $LC_n(s)$ over the finite field $GF(n)$ of order n and the minimal polynomial $m_n(x)$ of this

⋆e-mail: Vladimir.Edemsky@novsu.ru 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.

sequence are defined by

$$LC_n(s) = N - \deg \gcd(x^N - 1, S(x)),$$
$$m_n(x) = (x^N - 1)/\gcd(x^N - 1, S(x)) \quad (1)$$

where $S(x) = s_0 + s_1 x + \ldots + s_{N-1}x^{N-1}$ [3]. It is worth pointing out that the minimal polynomials of $m_n(x)$ defined here may be the reciprocals of the minimal polynomials defined in other references. From (1) we can establish that

$$LC_p(s) = N - \deg \gcd((x^q - 1)^p, S(x)),$$
$$m_p(x) = (x^q - 1)^p/\gcd((x^q - 1)^p, S(x)) \quad (2)$$

and

$$LC_q(s) = N - \deg \gcd((x^p - 1)^q, S(x)),$$
$$m_q(x) = (x^p - 1)^q/\gcd((x^p - 1)^q, S(x)) \quad (3)$$

Let α be a primitive q-th root of unity and β be a primitive p-th root of unity in the extensions of the fields $GF(p)$ and $GF(q)$, respectively. Then, according to (2), (3), in order to find the minimal polynomial and the linear complexity of $\{s_i\}$ over $GF(q)$ or $GF(p)$ it is sufficient to find the roots of $S(x)$ in the set $\{1, \alpha, \ldots, \alpha^{q-1}\}$ or $\{1, \beta, \ldots, \beta^{p-1}\}$ and determine their multiplicity.

Let $H_i^{(p)} = C_i \bmod p$, and $H_i^{(q)} = C_i \bmod q, i = 0, 1$. Here and hereafter $x \bmod n$ denotes the least nonnegative integer that is congruent to x modulo n. Then $H_0^{(p)}, H_0^{(q)}$ are the quadratic residue classes modulo p and q, respectively.

Legendre sequences $\{l_i^{(q)}\}$ and $\{l_i^{(p)}\}$ of lengths q and p defined as

$$l_i^{(q)} = \begin{cases} 1, & \text{if } i \bmod q \in H_0^{(q)}, \\ 0, & \text{otherwise} \end{cases}$$

and

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

The linear complexity and the minimal polynomial of Legendre sequence over the finite field of any order were studied in [12].

Let us introduce subsidiary polynomials $S^{(q)}(x) = \sum_{i=0}^{q-1} l_i^{(q)} x^i$ and $S^{(p)}(x) = \sum_{i=0}^{p-1} l_i^{(p)} x^i$. By [12] over $GF(q)$ we have

$$S^{(q)}(\alpha) = \begin{cases} S^{(q)}(\alpha^j), & \text{if } j \bmod q \in H_0^{(q)}, \\ S^{(q)}(\alpha^g), & \text{if } j \bmod q \in H_1^{(q)}, \end{cases}$$
$$\text{and } S^{(q)}(\alpha) + S^{(q)}(\alpha^g) = -1. \quad (4)$$

Similarly, over $GF(p)$ we see that

$$S^{(p)}(\beta) = \begin{cases} S^{(q)}(\beta^j), & \text{if } j \bmod p \in H_0^{(p)}, \\ S^{(p)}(\alpha^g), & \text{if } j \bmod p \in H_1^{(p)}, \end{cases} \text{ and}$$
$$S^{(p)}(\alpha) + S^{(p)}(\alpha^g) = -1. \quad (5)$$

The following statement was discussed in [12].

Lemma 1 *$S^{(q)}(\alpha)$ and $S^{(q)}(\alpha^g)$ are zeros of the polynomial*

$$\begin{cases} z^2 + z - (q-1)/4, & \text{if } q \equiv 1 (\bmod 4), \\ z^2 + z + (q+1)/4, & \text{if } q \equiv 3 (\bmod 4). \end{cases}$$

If there exist $j : j \neq 0$ and $S^{(q)}(\alpha^j) = 0$ then without loss of generality, we can choose α such that $S^{(q)}(\alpha) = 0$. Thus, by (4) and lemma 1 we have

$$\{j \mid S^{(q)}(\alpha^j) = 0, j = 1, \ldots, q-1\} = \begin{cases} H_0^{(q)}, & \text{if } q \equiv 1 (\bmod p) \text{ and } q \equiv 1 (\bmod 4), \\ & \text{or } q \equiv -1 (\bmod p) \text{ and } q \equiv 3 (\bmod 4), \\ \varnothing, & \text{otherwise.} \end{cases} \quad (6)$$

3 Subsidiary lemmas

The following lemmas are needed for the sequel.

According to the Chinese Remainder Theorem

$$Z_N \cong Z_p \times Z_q$$

relatively to isomorphism $\varphi(x) = (x \bmod p, x \bmod q)$. Put, by definition $F_k = \varphi^{-1}(\{k\} \times H_0^{(q)}), k = 1, \ldots, p-1$. From our definitions it follows that

$$C_0 = \bigcup_{k=1}^{p-1} F_k. \quad (7)$$

Define $S_0(x) = \sum_{i \in C_0} x^i$. Then, by (7) we have $S_0(x) = \sum_{k=1}^{p-1} \sum_{i \in F_k} x^i$

Lemma 2 *Let $F_k = \varphi^{-1}(\{k\} \times H_0^{(q)})$. Then there exist polynomials $g_k(x) = \sum_{j=1}^{(q-1)/2} x^{b_{j,k}}, k = 0, 1 \ldots, p-1,\ 0 \leq b_{j,k} < q$ such that $\sum_{i \in F_k} x^i = x^k g_k(x^p)$.*

Proof. Suppose $i \in F_k$; then by definition of F_k it follows that $i \equiv k \pmod p$. So, there exist $b_{i,k},\ 0 \leq b_{j,k} < q$ such that $i = k + b_{i,k}p$.

By Lemma 2 we obtain that

$$S_0(x) = \sum_{k=1}^{p-1} x^k g_k(x^p). \quad (8)$$

Lemma 3 *Let $S_0(x) = \sum_{i \in C_0} x^i$. Then:*

(i) $S_0(x) \equiv (q-1)/2(1 - (x-1)^{p-1}) \pmod{(x-1)^p}$ in the ring $GF(p)[x]$;

(ii) $S_0(x) \equiv (p-1)\left(-1/2 + T(x)(x-1)^{(q-1)/2}\right) \pmod{(x-1)^q}$ in the ring $GF(q)[x]$, where $T(1) \neq 0$.

Proof. At the beginning, we prove the first statement. It is clear that $g_k(x^p) \equiv (q-1)/2 \pmod{(x-1)^p}$; then by (4) we see that $S_0(x) \equiv -(q-1)(x + x^2 + \cdots + x^{p-1})/2 \pmod{(x-1)^p}$ in $GF(p)[x]$. The statement (i) of this lemma follows from the last congruence.

Further, $S_0(x) = \sum_{k=1}^{p-1} \sum_{i \in F_k} x^i$. From the definition of F_k it follows that $F_k \bmod q = H_0^{(q)}$, hence $\sum_{i \in F_k} x^i \equiv \sum_{i \in H_0^{(q)}} x^i (\bmod (x-1)^q)$, i.e. $\sum_{i \in F_k} x^i \equiv S^{(q)}(x) (\bmod (x-1)^q)$ over $GF(q)[x]$. To conclude the proof, it remains to note that by [1] we have $S^{(q)}(x) \equiv -1/2 + T(x)(x-1)^{(q-1)/2} (\bmod (x-1)^q)$, where $T(1) \neq 0$.

Lemma 4 *Let $S_0^{(n)}(x)$ be a formal derivative of order n of the polynomial $S_0(x)$ over $GF(p)$ and $0 \leq n < p$. Then*

$$S_0^{(n)}(x) = \sum_{k=n}^{p-1} k(k-1)\ldots(k-n+1)x^{k-n} g_k(x^p).$$

Proof. Since $\left(x^k g_k(x^p)\right)' = kx^{k-1}g_k(x^p)$ we have

$$\left(x^k g_k(x^p)\right)^{(n)} = \begin{cases} k(k-1)\dots(k-n+1)x^{k-n}g_k(x^p), & \text{if } k \geq n, \\ 0, & \text{if } k < n. \end{cases}$$

The conclusion of this lemma then follows from (8).

4 The linear complexity of the first class of sequences

First, we consider Ding-Helleseth-generalized cyclotomic sequence $t = \{t_i\}$ defined by

$$t_i = \begin{cases} 1, \text{ if } i \bmod N \in C_0 \cup P \cup R, \\ 0, \text{ otherwise.} \end{cases} \quad (9)$$

4.1 The linear complexity of sequences over $GF(p)$

In this subsection we regard t as a sequence over the finite field $GF(p)$. Let $S_t(x) = \sum_{i=0}^{N} t_i x^i$. From our definitions it follows that $S_t(x) = S_0(x) + 1 + x^p + \cdots + x^{(q-1)p}$. Since $1 + x^p + \cdots + x^{(q-1)p} = (x^q - 1)^p/(x-1)^p$, by (8) we see that

$$S_t(x) = S_0(x) + 1 + x^p + \cdots + x^{(q-1)p} = \sum_{k=1}^{p-1} x^k g_k(x^p) + \left(1 + x + \cdots + x^{(q-1)}\right)^p. \quad (10)$$

Before we give the main result of this section, we establish the following lemma.

Lemma 5 *Let $F_k = \varphi^{-1}(\{k\} \times H_0^{(q)})$. Then $\sum_{i \in F_k} \alpha^{vi} = S^{(q)}(\alpha^v)$ for any $v: \ 0 < v < p$.*

Proof. From definition of F_k it follows that $F_k \bmod q = H_0^{(q)}$. So, $\sum_{i \in F_k} \alpha^{vi} = \sum_{i \in H_0^{(q)}} \alpha^{vi}$. To conclude the proof, it remains to note that $\sum_{i \in H_0^{(q)}} \alpha^{vi} = S^{(q)}(\alpha^v)$.

Further, using Lemmas 5 and 2, we can write the following statement.

Corollary 6 *If $S^{(q)}(\alpha^v) = 0$ then $g_k(\alpha^{pv}) = 0$.*

Denote $\omega_0(x) = \prod_{i \in H_0^{(q)}}(x - \alpha^i)$ and $\omega_1(x) = \prod_{i \in H_1^{(q)}}(x - \alpha^i)$.

Theorem 7 *Let $\{t_i\}$ be defined by* (9)*. Then we have:*

1. *$LC_p(t) = p(q+1)/2$ and $m(x) = (x-1)^p \omega_1^p(x)$ if $q \equiv 1 \pmod p$ and $q \equiv 1 \pmod 4$,*
2. *$LC_p(t) = p(q-1)/2 + 1$ and $m(x) = (x-1)\omega_1^p(x)$ if $q \equiv -1 \pmod p$ and $q \equiv 3 \pmod 4$,*
3. *$LC_p(t) = pq - p + 1$ and $m(x) = (x^q - 1)^p/(x-1)^{p-1}$ if $q \equiv -1 \pmod p$ and $q \equiv 1 \pmod 4$,*
4. *$LC_p(t) = pq$ and $m(x) = (x^q - 1)^p$ otherwise.*

Proof. First of all, we note that $S_t(1) = (p-1)(q-1)/2 + q = (q+1)/2$. Thus, if $q \not\equiv -1 \pmod p$ then $S_t(1) \neq 0$. Otherwise, if $q \equiv -1 \pmod p$ then $S_t(1) = 0$ and by Lemma 3 and (10) we obtain that $S_t(x) \equiv 1 - (x-1)^{p-1} + (1 + x + \cdots + x^{(q-1)})^p \pmod{(x^p - 1)}$ or $S_t(x) \equiv (x-1)^{p-1} + \left((1-1) + (x-1) + \cdots + (x^{(q-1)} - 1)\right)^p \pmod{(x^p - 1)}$.

So, we have that in this case 1 is a root of the polynomial $S_t(x)$ of multiplicity $p-1$.

Suppose $v = 1, \dots, q-1$; then by Lemma 3 and (10) we obtain $S_t(\alpha^v) = (p-1)S^{(q)}(\alpha^v)$. So, by (6) $S_t(\alpha^v) = 0$ if and only if $v \in H_0^{(q)}$ and $q \equiv 1 \pmod p$ and $q \equiv 1 \pmod 4$ or $q \equiv -1 \pmod p$ and $q \equiv 3 \pmod 4$. If $S_t(\alpha^v) = 0$ then by Lemma 4 and Corollary 6 we obtain that α^v is a root of $S_t(x)$ of multiplicity p. The conclusion of this theorem then follows from (2).

Our examples $p = 7, q = 29$; $p = 3, q = 13$; $p = 3, q = 17$; $p = 5, q = 3$ show that all the cases of Theorem 7 are possible.

4.2 The linear complexity of sequences over $GF(q)$

Now, we consider the linear complexity of $\{t_i\}$ over $GF(q)$. In this case we see that

$$S_t(x) = S_0(x) + 1 + x^p + \cdots + x^{(q-1)p} = \sum_{k=1}^{p-1} x^k g_k(x^p) + (x^p - 1)^{q-1}. \quad (11)$$

Theorem 8 *Let $\{t_i\}$ be defined by* (9)*. Then:*

1. *$LC_q(t) = pq - q + 1$ and $m_q(x) = (x-1)(1 + x + \cdots + x^{p-1})^q$ if $p \equiv 1 \pmod q$,*
2. *$LC_q(t) = pq$ and $m_q(x) = (x^q - 1)^p$ otherwise.*

Proof. By definition, $S(1) = (p-1)(q-1)/2 + q$, thus $S(1) = -(p-1)/2$. If $p \not\equiv 1 (\bmod q)$ then $S_t(1) \neq 0$. Suppose $p \equiv 1 (\bmod q)$; then $S_t(1) = 0$ and by (11) and Lemma 3 we can establish that $S_t(x) \equiv (x^p - 1)^{q-1} (\bmod (x-1)^q)$. So, 1 is a root of multiplicity $q-1$ of $S_t(x)$ for $p \equiv 1 (\bmod q)$.

Let $v: \ 0 < v < q$. Then by (11) $S_t(\beta^v) = (q-1)(\beta + \beta^2 + \cdots + \beta^{p-1})/2 + q = -(\beta^p - 1)/(2(\beta - 1)) + 1/2 = 1/2$, i.e. $S_t(\beta^v) \neq 0$. The conclusion of this theorem then follows from (3).

5 The linear complexity of the second class of sequences

Now, we can also consider the sequence u defined by

$$u_i = \begin{cases} 1, \text{ if } i \bmod N \in C_0 \cup Q \cup R, \\ 0, \text{ otherwise.} \end{cases} \quad (12)$$

Let $S_u(x) = \sum_{i=0}^{N} u_i x^i$. By definition we see that $S_u(x) = S_0(x) + 1 + x^q + \cdots + x^{(p-1)q}$.

5.1 The linear complexity of sequences over $GF(p)$

Here $1+x^q+\cdots+x^{(p-1)q}=(x^{qp}-1)/(x^q-1)=(x^q-1)^{p-1}$, by (8) we see that

$$S_t(x)=S_0(x)+1+x^q+\cdots+x^{(p-1)q}=\sum_{k=1}^{p-1}x^k g_k(x^p)+(x^q-1)^{p-1}. \quad (13)$$

With similar arguments as above we obtain the following results for u.

Theorem 9 *Let $\{u_i\}$ be defined by* (12)*. Then:*

1. $LC_p(u)=pq-(p-1)(q+1)/2$ *and* $m_p(x)=(x-1)\omega_0(x)\omega_1^p(x)$ *if* $q\equiv 1 \pmod p$ *and* $q\equiv 1 \pmod 4$,
2. $LC_p(u)=pq-(q-1)(p-1)/2$ *and* $m_p(x)=(x-1)^p\omega_0(x)\omega_1^p(x)$ *if* $q\equiv -1 \pmod p$ *and* $q\equiv 3 \pmod 4$,
3. $LC_p(u)=pq-p+1$ *and* $m_p(x)=(x^{pq}-1)/(x-1)^{p-1}$ *if* $q\equiv 1 \pmod p$ *and* $q\equiv 3 \pmod 4$,
4. $LC_p(u)=pq$ *and* $m(x)=(x^q-1)^p$ *otherwise.*

Proof. First of all, we note that $S_u(1)=(p-1)(q-1)/2+p=-(q-1)/2$. Thus, if $q\not\equiv 1 \pmod p$ then $S_u(1)\neq 0$. Otherwise, if $q\equiv 1 \pmod p$ then $S_u(1)=0$ and by Lemma 3 and (13) we obtain that $S_u(x)\equiv (x^q-1)^{p-1} \pmod{(x^p-1)}$.

So, we have that in this case 1 is a root of the polynomial $S_u(x)$ of multiplicity $p-1$.

Suppose $v=1,\ldots,q-1$; then by Lemma 4 and (13) we obtain $S_u(\alpha^v)=(p-1)S^{(q)}(\alpha^v)$. So, by (6) $S_u(\alpha^v)=0$ if and only if $v\in H_0^{(q)}$ and $q\equiv 1 \pmod p$ and $q\equiv 1 \pmod 4$ or $q\equiv -1 \pmod p$ and $q\equiv 3 \pmod 4$. If $S_t(\alpha^v)=0$ then by Lemma 4, Corollary 6, and (13) we obtain that α^v is a root of $S_u(x)$ of multiplicity $p-1$. By (2) this completes the proof of Theorem 9.

Our examples $p=5, q=41$; $p=3, q=11$; $p=5, q=11$; $p=3, q=17$ show that all the cases of Theorem 9 are possible.

5.2 The linear complexity of sequences over $GF(q)$

Here $1+x^q+\cdots+x^{(p-1)q}=(x^{qp}-1)/(x^q-1)=(1+x+\cdots+x^{p-1})^q$, by (8) we see that

$$S_t(x)=S_0(x)+1+x^q+\cdots+x^{(p-1)q}=\sum_{k=1}^{p-1}x^k g_k(x^p)+(1+x+\cdots+x^{p-1})^q. \quad (14)$$

Theorem 10 *Let $\{u_i\}$ be defined by* (12)*. Then:*

1. $LC_q(u)=pq-(q-1)/2$ *and* $m_p(x)=(x^{pq}-1)/(x-1)^{(q-1)/2}$ *if* $p\equiv -1 \pmod q$,
2. $LC_q(u)=pq$ *and* $m(x)=(x^q-1)^p$ *otherwise.*

Proof. By definition, $S_u(1)=(p-1)(q-1)/2+p=(p+1)/2$, such that $S_u(1)\neq 0$ for $p\not\equiv -1 \pmod q$. Suppose $p\equiv -1 \pmod q$; then $S_u(1)=0$ and by (14) and Lemma 3 we can establish that $S_u(x)\equiv 1-2T(x)(x-1)^{(q-1)/2})+(1+x+\cdots+x^{p-1})^q \pmod{(x-1)^{q-1}}$, i.e. $S_u(x)\equiv -2(T(x)x-1)^{(q-1)/2})+(x-1+\cdots+x^{p-1}-1)^q \pmod{(x-1)^{q-1}}$. So, 1 is a root of multiplicity $(q-1)/2$ of $S_u(x)$ for $p\equiv -1 \pmod q$.

Let $v:\ 0<v<q$. Then by (14) $S_t(\beta^v)=(q-1)(\beta+\beta^2+\cdots+\beta^{p-1})/2+0=-(\beta^p-1)/(2(\beta-1))+1/2=1/2$, i.e. $S_t(\beta^v)\neq 0$. The conclusion of this theorem then follows from (3).

6 The linear complexity of the third class of sequences

In conclusion, we study the linear complexity of balanced sequence v.

Let $C_0^{(q)}=qH_0^{(p)}$, $C_0^{(p)}=pH_0^{(q)}$. We consider a sequence v defined by

$$u_i=\begin{cases}1, & \text{if } i \bmod N\in C_0\cup C_0^{(q)}\cup C_0^{(p)},\\ 0, & \text{otherwise.}\end{cases} \quad (15)$$

Then v is balanced sequence. Denote $S_v(x)=\sum_{i=0}^{N-1}v_i x^i$. Then, by definition we have

$$S_v(x)=\sum_{k=0}^{p-1}\sum_{i\in F_k}x^i+\sum_{i\in C_0^{(q)}}x^i+\sum_{i\in C_0^{(p)}}x^i. \quad (16)$$

For any $a\in H_0^{(q)}$ there exist $b_a, 0<b_a<p$ such that $a+b_a q\equiv 0 \pmod p$.

Lemma 11 *Let $E^{(q)}=\{c|\ pc=a+b_a q,\ a,c\in H_0^{(q)}\}$. Then*

$$C_0=\bigcup_{a\in H_0^{(q)}}\{a,a+q,\ldots,a+(p-1)q\}\setminus pE^{(q)}.$$

The statement of this lemma follows immediately from our definitions.

6.1 The linear complexity of sequences over $GF(p)$

In this subsection we regard t as a sequence over the finite field $GF(p)$.

Lemma 12 *Let $S_0(x)=\sum_{i\in C_0}x^i$. Then*

$$S_0(x)=(x^q-1)^{p-1}S^{(q)}(x)-\sum_{i\in pE^{(q)}}x^i$$

Proof. By Lemma 11 we obtain $S_0(x)=\sum_{a\in H_0^{(q)}}(x^a+x^{a+q}+\cdots+x^{a+(p-1)q})-\sum_{i\in pE^{(q)}}x^i$. To conclude the proof, it remains to note that $\sum_{a\in H_0^{(q)}}x^a=S^{(q)}(x)$ and $1+x^q+\cdots+x^{(p-1)q}=(x^q-1)^{p-1}$.

Lemma 13 *Let α be a primitive q-th root of unity in the extension $GF(p)$. Then*

$$\sum_{i\in C_0^{(p)}}\alpha^{ji}=\begin{cases}S^{(q)}(\alpha^j), & \text{if } \left(\frac{p}{q}\right)=1,\\ S^{(q)}(\alpha^{jg}), & \text{if } \left(\frac{p}{q}\right)=-1.\end{cases}$$

Proof. Suppose $\left(\frac{p}{q}\right) = 1$; then $p \in H_0^{(q)}$ and $pH_0^{(q)} = H_0^{(q)} \bmod q$. Combining this with $C_0^{(p)} = pH_0^{(q)}$, we get

$$\sum_{i \in C_0^{(p)}} \alpha^{ji} = \sum_{m \in H_0^{(q)}} \alpha^{jm} = S^{(q)}(\alpha^j).$$

The second formula in this lemma may be proved similarly.

Lemma 14 *Let* $\{v_i\}$ *be defined by* (15). *Then* $S\left(\alpha^j\right) \neq 0$ *for* $j = 1, 2 \ldots, p-1$.

Proof. If exist $j : j \neq 0$ and $S(\alpha^j) = 0$ then without loss of generality, we can choose α such that $S(\alpha) = 0$. We consider two cases.

(i) Suppose $\left(\frac{p}{q}\right) = 1$; then by (16), Lemmas 5,13 we have

$$(p-1)S^{(q)}(\alpha) + S^{(q)}(\alpha) + (p-1)/2 = 0.$$

It is impossible.

(ii) Suppose $\left(\frac{p}{q}\right) = -1$; then in this case we obtain

$$(p-1)S^{(q)}(\alpha) + S^{(q)}(\alpha^g) + (p-1)/2 = 0.$$

Hence, by (4) $S^{(q)}(\alpha) = -3/4$.

Let $q \equiv 1 (\bmod 4)$. Therefore, since by Lemma 1 $S^{(q)}(\alpha)$ is a zero of $z^2 + z - (q-1)/4 = 0$ we obtain $q \equiv 1/4 (\bmod p)$. Then $\left(\frac{q}{p}\right) = 1$. Further, by the law of quadratic reciprocity we see

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

We have a contradiction here.

Now, let $q \equiv 3 (\bmod 4)$. In this case by Lemma 1 $S^{(q)}(\alpha)$ is a zero of $z^2 + z + (q+1)/4 = 0$. Hence $9/16 - 3/4 + (q+1)/4 = 0$ or $q \equiv -1/4 (\bmod p)$. Then

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

By the law of quadratic reciprocity and the condition we obtain

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

So, we have a contradiction. This completes the proof of Lemma 14.

Theorem 15 *Let* $\{v_i\}$ *be defined by* (15). *Then* $LC_p(v) = pq$ *and* $m(x) = x^{pq} - 1$.

Proof. By definition, $S_v(1) = (pq-1)/2$, so that $S_v(1) \neq 1$. Further, by Lemma 14 $S_v(\alpha) \neq 0$ and the statements of this theorem follows from (2).

6.2 The linear complexity of sequences over $GF(q)$

With similar arguments as above we obtain the following results for v.

Theorem 16 *Let* $\{v_i\}$ *be defined by* (15). *Then*

1. $LC_q(v) = q(p+1)/2$ *if* $p \equiv 1 (\bmod 4)$ *and* $p \equiv 1 (\bmod q)$ *or* $p \equiv 3 (\bmod 4)$ *and* $p \equiv -1 (\bmod q)$.
2. $LC_q(v) = pq$ *otherwise.*

7 Conclusion

For additive stream ciphering, the linear complexity (span) of the keystream sequence must be large enough. We study the linear complexity of three classes of Ding-Helleseth-generalized cyclotomic sequences of length pq. We derive the linear complexity and the minimal polynomial of above-mentioned sequences over the finite fields of orders p and q, where p and q are two odd distinct primes and obtain series of sequences with high linear complexity. Long periods can also be obtained easily. The sequences from the third class have almost ideal balance property.

References

[1] H. Aly, A.Winterhof, On the k-error linear complexity over Fp of Legendre and Sidelnikov sequences, Des. Codes Cryptogr. **40** (2006) 369–374.

[2] H. Aly, W. Meidl, A. Winterhof, On the k-Error Linear Complexity of Cyclotomic sequences, J. Math. Crypt. **1** (2007) 1–14.

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

[4] Bai E, Liu X, Xiao G. Linear complexity of new generalized cyclotomic sequences of order two of length pq. IEEE Transactions on Information Theory, **51**(5) (2005) 1849-1853.

[5] C. Ding, Linear Complexity of Generalized Cyclotomic Binary Sequences of Order 2. Finite Fields and Their Appl., **3**(1997) 159-174

[6] C. Ding, Cyclic Codes From the Two-Prime Sequences. IEEE Trans. Inf. Theory, **58** (6) (2012) 3881-3891

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

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

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

[10] W. Meidle, Remarks on a cyclotomic sequence. Des. Codes Cryptogr., **51**(2009) 33-43

[11] Q. Wang, Y. Jiang, D. Lin, Linear complexity of Ding-Helleseth sequences of order 2 over $GF(l)$. Crypto. Commun., DOI 10.1007/s12095-015-0138-5

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

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

[14] Yan T, Chen Z, Xiao G. Linear complexity of Ding generalized cyclotomic sequences. Journal of Shanghai University, **11**(1) (2007) 22-26.

[15] Yan T, Hong L, Xiao G. The linear complexity of new generalized cyclotomic binary sequences of order four. Information Sciences, **178**(3)(2008) 807-815.