Chen ZX, Li SQ. Some notes on generalized cyclotomic sequences of length pq. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 23(5): 843–850 Sept. 2008

Some Notes on Generalized Cyclotomic Sequences of Length pq

Zhi-Xiong Chen[1,2] (陈智雄) and Sheng-Qiang Li[3] (李胜强)

[1] *Key Lab of Applied Mathematics, Putian University, Putian 351100, China*

[2] *Key Lab of Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China*

[3] *National Key Lab of Communication, University of Electronic Science and Technology of China, Chengdu 610054, China*

E-mail: ptczx@126.com; shqli_xidian@126.com

Received October 17, 2007; revised May 3, 2008.

Abstract We review the constructions of two main kinds of generalized cyclotomic binary sequences with length pq (the product with two distinct primes). One is the White-generalized cyclotomic sequences, the other is the Ding-Helleseth(DH, for short)-generalized cyclotomic sequences. We present some new pseudo-random properties of DH-generalized cyclotomic sequences using the theory of character sums instead of the theory of cyclotomy, which is a conventional method for investigating generalized cyclotomic sequences.

Keywords stream cipher, generalized cyclotomic sequence, pseudo-random binary sequence, character sum, correlation

1 Introduction

Let m be a positive integer. We identify $\mathbb{Z}_m$, the residue ring modulo m, with the set $\{0, 1, \ldots, m-1\}$ and we denote by $\mathbb{Z}_m^*$ the unit group of $\mathbb{Z}_m$. A partition $\{D_0, D_1, \ldots, D_{d-1}\}$ of $\mathbb{Z}_m^*$ is a family of sets with

$$D_i \cap D_j = \emptyset \quad \text{for} \quad i \neq j; \quad \mathbb{Z}_m^* = \bigcup_{i=0}^{d-1} D_i.$$

If D_0 is a multiplicative subgroup of $\mathbb{Z}_m^*$ and there exist elements $g_1, \ldots, g_{d-1}$ of $\mathbb{Z}_m^*$ such that $D_i = g_i D_0$ for all $i \in [1, d-1]$, then the D_i's are called *classical cyclotomic classes* of order d when m is prime and *generalized cyclotomic classes* of order d when m is composite.

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. The distinguished work is due to Whiteman and Ding *et al.*[1−6] There are different kinds of classical/generalized cyclotomic sequences and most of them have quite good randomness properties, which make them significant in cryptographic applications. For example, the most important classical cyclotomic sequence is the Legendre sequence, which has ideal periodic and aperiodic autocorrelation functions and exhibits large linear complexity[7,8]. A new kind of generalized cyclotomic sequences with respect to $p_1^{e_1} \ldots p_t^{e_t}$ was introduced in [4].

This paper contributes to the generalized cyclotomic sequences with respect to pq, the product with two different prime numbers.

Let p and q be two distinct primes with $\gcd(p-1, q-1) = d$ and $e = (p-1)(q-1)/d$. By the Chinese Remainder Theorem there exists a common primitive root g of both p and q. There also exists an integer x satisfying

$$x \equiv g \pmod{p}, \quad x \equiv 1 \pmod{q}.$$

Below we always fix the definitions of g and x. Since g is a primitive root of both p and q, by the Chinese Remainder Theorem again

$$\begin{aligned} \mathrm{ord}_{pq}(g) &= \mathrm{lcm}(\mathrm{ord}_p(g), \mathrm{ord}_q(g)) \\ &= \mathrm{lcm}(p-1, q-1) = e, \end{aligned}$$

where $\mathrm{ord}_m(g)$ denotes the multiplicative order of g modulo m.

So we have

$$\mathbb{Z}_{pq}^* = \{g^s x^i \pmod{pq} | s = 0, 1, \ldots, e-1, \; i = 0, 1, \ldots, d-1\}.$$

Short Paper

This work was supported in part by the Open Funds of Key Lab of Fujian Province University Network Security and Cryptology (Grant No. 07B005), the Funds of the Education Department of Fujian Province (Grant No. JA07164) and the Natural Science Foundation of Fujian Province of China (Grant No. 2007F3086).

There are two different generalized cyclotomic classes over $\mathbb{Z}_{pq}^*$, one is called *Whiteman-generalized cyclotomic classes*, the other is called *Ding-Helleseth-generalized cyclotomic classes* (DH-generalized cyclotomic classes, for short). Both generalized cyclotomic classes are used for designing binary sequences, which are called Whiteman-generalized cyclotomic sequences and DH-generalized cyclotomic sequences. See below the details.

We conclude this section with the definitions of two important pseudo-random measures, introduced by Mauduit and Sárközy[9], for finite binary sequences. We introduce these notions below with a slight modification.

For a finite binary sequence of length N (for any $N \in \mathbb{N}$)

$$S_N = \{s_1, s_2, \ldots, s_N\} \in \{0,1\}^N.$$

The *well-distribution measure* of S_N is defined as

$$W(S_N) = \max_{a,b,t} \Big| \sum_{j=0}^{t-1} (-1)^{s_{a+jb}} \Big|,$$

where the maximum is taken over all a, b, t such that $a, b, t \in \mathbb{N}$ and $1 \leqslant a \leqslant a + (t-1)b \leqslant N$, while the *correlation measure of order k* of S_N is defined as

$$C_k(S_N) = \max_{M,D} \Big| \sum_{n=1}^{M} (-1)^{s_{n+d_1} + s_{n+d_2} + \cdots + s_{n+d_k}} \Big|,$$

where the maximum is taken over all $D = (d_1, \ldots, d_k)$ with non-negative integers $0 \leqslant d_1 < \cdots < d_k$ and M such that $M + d_k \leqslant N$.

S_N is considered as a "good" pseudo-random sequence, if both $W(S_N)$ and $C_k(S_N)$ (at least for small k) are "small" in terms of N (in particular, both are $o(N)$ as $N \to \infty$). The Legendre sequence forms a "good" pseudo-random sequence[9]. Many other "good" binary sequences were designed in the literature, see for example[10–13].

2 Constructions of Generalized Cyclotomic Sequences

In this section, we will introduce two main generalized cyclotomic sequences of length pq. One is the Whiteman-generalized cyclotomic sequences, the other is the DH-generalized cyclotomic sequences.

2.1 Whiteman-Generalized Cyclotomic Sequences

The *Whiteman-generalized cyclotomic classes of order d* with respect to pq are defined by

$$D_i = \{g^s x^i \pmod{pq} | s = 0, 1, \ldots, e-1\},$$

where $i = 0, 1, \ldots, d-1$. D_i's give a partition of $\mathbb{Z}_{pq}^*$, i.e.,

$$\mathbb{Z}_{pq}^* = \bigcup_{i=0}^{d-1} D_i, \ D_i \cap D_j = \emptyset \quad \text{for } i \neq j.$$

Now set

$$R = \{0\},$$
$$Q = \{q, 2q, \ldots, (p-1)q\},$$
$$P = \{p, 2p, \ldots, (q-1)p\}.$$

We also set

$$C_0 = R \cup Q \cup \Big(\bigcup_{i=0}^{\frac{d}{2}-1} D_{2i} \Big), \quad C_1 = P \cup \Big(\bigcup_{i=0}^{\frac{d}{2}-1} D_{2i+1} \Big),$$

$$C_{00} = R \cup Q \cup \Big(\bigcup_{i=0}^{\frac{d}{2}-1} D_i \Big), \quad C_{11} = P \cup \Big(\bigcup_{i=\frac{d}{2}}^{d-1} D_i \Big).$$

It is easy to see that

$$\mathbb{Z}_{pq} = C_0 \cup C_1, \quad C_0 \cap C_1 = \emptyset$$

and

$$\mathbb{Z}_{pq} = C_{00} \cup C_{11}, \quad C_{00} \cap C_{11} = \emptyset.$$

Clearly, if $d > 2$, $C_0 \neq C_{00}$ and $C_1 \neq C_{11}$.

Now we introduce two kinds of *Whiteman-generalized cyclotomic sequences* of order d, the name comes from the use of Whiteman-generalized cyclotomic classes.

Definition 1. *The Whiteman-generalized cyclotomic sequence $\mathcal{S} = \{s_0, s_1, \ldots, s_{pq-1}\}$ of order d and of length pq, which is called W-GCS-I, is defined by*

$$s_i = \begin{cases} 0, & \text{if} \quad i \in C_0; \\ 1, & \text{if} \quad i \in C_1. \end{cases}$$

Another Whiteman-generalized cyclotomic sequence $\mathcal{T} = \{t_0, t_1, \ldots, t_{pq-1}\}$ of order d and of length pq, which is called W-GCS-II, is defined by

$$t_i = \begin{cases} 0, & \text{if} \quad i \in C_{00}; \\ 1, & \text{if} \quad i \in C_{11}. \end{cases}$$

It is easy to see that W-GCS-I can be expressed as

$$s_i = \begin{cases} 1, & \text{if} \quad i \in P; \\ 0, & \text{if} \quad i \in Q \cup R; \\ \dfrac{1-\left(\frac{i}{p}\right)\left(\frac{i}{q}\right)}{2}, & \text{if} \quad i \in \mathbb{Z}_{pq}^*; \end{cases}$$

for $0 \leqslant i \leqslant pq-1$, where $(\frac{\cdot}{\cdot})$ denotes the Legendre symbol. So we deduce

$$(-1)^{s_i} = \begin{cases} -1, & \text{if} \quad i \in P; \\ 1, & \text{if} \quad i \in Q \cup R; \\ \left(\frac{i}{p}\right)\left(\frac{i}{q}\right), & \text{if} \quad i \in \mathbb{Z}_{pq}^*; \end{cases}$$

for $0 \leqslant i \leqslant pq-1$. W-GCS-I is also known as Jacobi sequence[14].

W-GCS-I has several good randomness properties. All these results make it significant in cryptographic applications.

When $d = 2$ (W-GCS-I and W-GCS-II are the same), exact formulas for the linear complexity have been determined in [3] and the (periodic) autocorrelation values have been determined by the generalized cyclotomic numbers in [5]. The linear complexity takes on one of $pq-1$, $(p-1)q$, $(p-1)(q-1)$, $(pq+p+q-3)/2$, $(p-1)(q-1)/2$ and $(p-1)(q+1)/2$, depending on the values of p mod 8 and q mod 8. The autocorrelation is at most five-valued depending on the parity of $(p-1)(q-1)/4$.

Using similar methods, exact formulas for the linear complexity and the (periodic) autocorrelation values of W-GCS-I and W-GCS-II have been determined in [15, 16] when $d = 4$. Results indicate that both sequences have low autocorrelation and high linear complexity.

Many other properties (for the case of $d = 2$), such as pattern distributions of length 2, aperiodic autocorrelation and linear complexity profile, have been also determined in [5, 17]. In particular, for any order $d(\geqslant 2)$, exact formulas for the periodic autocorrelation values have been computed by the theory of character sums in [17]. A trace representation of W-GCS-I has been presented in [14].

Similarly, W-GCS-II also can be described with multiplicative characters of $\mathbb{Z}_{pq}^*$. For any positive integer $m > 1$, a group homomorphism

$$\chi : \mathbb{Z}_m^* \to \mathbb{C}_1^*$$

is called a multiplicative character modulo m, where $\mathbb{C}_1^*$ is the multiplicative group of complex numbers of absolute value 1. A character with $\chi(u) = 1$ for any $u \in \mathbb{Z}_m^*$ is called the principal character and denoted by $\chi_0 = 1$. $\widehat{\mathbb{Z}_m^*}$ is denoted by the set of all multiplicative characters of $\mathbb{Z}_m^*$.

The exponential sums enter into our problem by means of the following well known basic identity.

Lemma 1[18]. Let $\#\widehat{\mathbb{Z}_m^*}$ denote the cardinality of $\widehat{\mathbb{Z}_m^*}$. For any element $u \in \mathbb{Z}_m^*$,

$$\sum_{\chi \in \widehat{\mathbb{Z}_m^*}} \chi(u) = \begin{cases} 0, & \text{if} \quad u \neq 1; \\ \#\widehat{\mathbb{Z}_m^*}, & \text{otherwise.} \end{cases}$$

And for any character $\chi \in \widehat{\mathbb{Z}_m^*}$,

$$\sum_{u \in \mathbb{Z}_m^*} \chi(u) = \begin{cases} 0, & \text{if} \quad \chi \neq \chi_0; \\ \#\widehat{\mathbb{Z}_m^*}, & \text{otherwise.} \end{cases}$$

We note that $\mathbb{Z}_m^*$ and $\widehat{\mathbb{Z}_m^*}$ in Lemma 1 can be replaced by any subgroups of $\mathbb{Z}_m^*$ and $\widehat{\mathbb{Z}_m^*}$, respectively.

Now from the construction of W-GCS-II and by Lemma 1, one can deduce

$$(-1)^{t_i} = \begin{cases} -1, & \text{if} \quad i \in P; \\ 1, & \text{if} \quad i \in Q \cup R; \\ \dfrac{2}{d} \displaystyle\sum_{j=0}^{\frac{d}{2}-1} \sum_{\chi \in G^*} \overline{\chi}(i)\chi(x^j), & \text{if} \quad i \in \mathbb{Z}_{pq}^*; \end{cases}$$

where $G = \{\chi \in \widehat{\mathbb{Z}_{pq}^*} | \chi(g^l) = 1, l = 0, 1, \ldots, e-1\}$ is a cyclic subgroup of multiplicative characters group $\widehat{\mathbb{Z}_{pq}^*}$, $G^* = G \setminus \{\chi_0\}$.

Using certain exponential sums, we estimate the well-distribution measure and the correlation measure of order k of W-GCS-II in [19]. We prove below that the upper bounds of both measures are very close to that of "truly" random sequences.

Proposition 1[19]. *Let $\mathcal{T} = \{t_0, t_1, \ldots, t_{pq-1}\}$ be the W-generalized cyclotomic sequence of order d defined as in Definition 1. Then the well-distribution measure of $\mathcal{T}$ satisfies*

$$W(\mathcal{T}) < 36p^{\frac{1}{2}}q^{\frac{1}{2}}\log(pq)\log(1+d) + p + q + 1$$

and the correlation measure of order k (small) of $\mathcal{T}$ satisfies

$$C_k(\mathcal{T}) < 9k4^k p^{\frac{1}{2}} q^{\frac{1}{2}} \log^k(1+d)\log(pq) + k(p+q+1).$$

2.2 DH-Generalized Cyclotomic Sequences

The *DH-generalized cyclotomic classes of order d* with respect to pq are defined by

$$D'_j = \Big\{ g^{ds+j}x^l \pmod{pq} | s = 0, 1, \ldots, \frac{e}{d} - 1,$$

$$l = 0, 1, \ldots, d-1\Big\},$$

where $j = 0, 1, \ldots, d-1$. (See [4] for the general case). Clearly,

$$\mathbb{Z}_{pq}^* = \bigcup_{j=0}^{d-1} D'_j,\ D'_i \cap D'_j = \emptyset \quad \text{for} \quad i \neq j.$$

Let P, Q, R be defined as in Subsection 2.1. Define

$$C'_0 = R \cup Q \cup \Big(\bigcup_{j=0}^{\frac{d}{2}-1} D'_{2j}\Big), \quad C'_1 = P \cup \Big(\bigcup_{j=0}^{\frac{d}{2}-1} D'_{2j+1}\Big),$$

$$C'_{00} = R \cup Q \cup \Big(\bigcup_{j=0}^{\frac{d}{2}-1} D'_j\Big), \quad C'_{11} = P \cup \Big(\bigcup_{j=\frac{d}{2}}^{d-1} D'_j\Big).$$

Then C'_0, C'_1 and C'_{00}, C'_{11} give a partition of $\mathbb{Z}_{pq}$, respectively, that is,

$$\mathbb{Z}_{pq} = C'_0 \cup C'_1,\ C'_0 \cap C'_1 = \emptyset$$

and

$$\mathbb{Z}_{pq} = C'_{00} \cup C'_{11},\ C'_{00} \cap C'_{11} = \emptyset.$$

Clearly, if $d > 2$, $C'_0 \neq C'_{00}$ and $C'_1 \neq C'_{11}$.

Below we define the *DH-generalized cyclotomic sequences* of order d, the name comes from the use of DH-generalized cyclotomic classes.

Definition 2. *The DH-generalized cyclotomic sequence $\mathcal{U} = \{u_0, u_1, \ldots, u_{pq-1}\}$ of order d and of length pq, which is called DH-GCS-I, is defined by*

$$u_i = \begin{cases} 0, & \text{if} \quad i \in C'_0; \\ 1, & \text{if} \quad i \in C'_1. \end{cases}$$

Another DH-generalized cyclotomic sequence $\mathcal{V} = \{v_0, v_1, \ldots, v_{pq-1}\}$ of order d and of length pq, which is called DH-GCS-II, is defined by

$$v_i = \begin{cases} 0, & \text{if} \quad i \in C'_{00}; \\ 1, & \text{if} \quad i \in C'_{11}. \end{cases}$$

Like W-GCS-I and W-GCS-II in Definition 1, DH-GCS-I and DH-GCS-II also can be described by virtue of multiplicative characters of $\mathbb{Z}_{pq}^*$.

According to the construction of DH-GCS-I, we deduce

$$(-1)^{u_i} = \begin{cases} -1, & \text{if} \quad i \in P; \\ 1, & \text{if} \quad i \in Q \cup R; \\ \left(\frac{i}{q}\right), & \text{if} \quad i \in \mathbb{Z}_{pq}^*; \end{cases}$$

for $0 \leqslant i \leqslant pq-1$.

When $d = 2$, exact formulas for the linear complexity and the (periodic) autocorrelation values of DH-GCS-I have been presented in [20, 21]. The linear complexity takes on one of $pq-1$, $(q-1)p$, $(pq-p+q-1)/2$ and $(pq+p+q-3)/2$, depending on the value q mod 8. The sequence is cryptographically attractive as far as linear complexity is concerned. The autocorrelation is four-valued or six-valued, depending on the value q mod 4, while one of the autocorrelation values is "large". So these sequences are not fit for some special applications, such as radar systems, spread-spectrum communication systems and CDMA systems.

Let $H = \langle g^d \rangle$ be a subgroup of $\mathbb{Z}_{pq}^*$ generated by g^d. Let $\mathcal{A} = \{\chi \in \widehat{\mathbb{Z}_{pq}^*} | \chi(h) = 1, \text{ for all } h \in H\}$. Obviously, $\mathcal{A}$ is a subgroup of $\widehat{\mathbb{Z}_{pq}^*}$ with cardinality $\#\mathcal{A} = d^2$ by [18, Theorem 5.6]. Let $\mathcal{A}^* = \mathcal{A} \setminus \{\chi_0\}$. It is easy to see that for any $\chi \in \mathcal{A}$, there exist $\chi_p \in \mathbb{Z}_p^*$ and $\chi_q \in \mathbb{Z}_q^*$ such that $\chi = \chi_p \chi_q$ with $\chi_p^d = 1$ and $\chi_q^d = 1$, where $\chi_p \in \widehat{\mathbb{Z}_p^*}$ and $\chi_q \in \widehat{\mathbb{Z}_q^*}$.

According to the construction of DH-GCS-II and by Lemma 1, for any $0 \leqslant i \leqslant pq-1$ with $\gcd(i, pq) = 1$, we have

$$\sum_{l=0}^{d-1} \sum_{j=0}^{\frac{d}{2}-1} \sum_{\chi \in \mathcal{A}} \overline{\chi}(i)\chi(g^j x^l) = \begin{cases} d^2, & \text{if} \quad i \in C'_{00}; \\ 0, & \text{if} \quad i \in C'_{11}. \end{cases}$$

Then, for any $0 \leqslant i \leqslant pq-1$ with $\gcd(i, pq) = 1$, we have

$$\sum_{l=0}^{d-1} \sum_{j=0}^{\frac{d}{2}-1} \sum_{\chi \in \mathcal{A}^*} \overline{\chi}(i)\chi(g^j x^l) = \begin{cases} \dfrac{d^2}{2}, & \text{if} \quad i \in C'_{00}; \\ -\dfrac{d^2}{2}, & \text{if} \quad i \in C'_{11}. \end{cases}$$

So, we deduce

$$(-1)^{v_i} = \begin{cases} -1, & \text{if} \quad i \in P; \\ 1, & \text{if} \quad i \in Q \cup R; \\ \dfrac{2}{d^2} \displaystyle\sum_{l=0}^{d-1} \sum_{j=0}^{\frac{d}{2}-1} \times & \\ \displaystyle\sum_{\chi \in \mathcal{A}^*} \overline{\chi}(i)\chi(g^j x^l), & \text{if} \quad i \in \mathbb{Z}_{pq}^*; \end{cases} \tag{1}$$

for $0 \leqslant i \leqslant pq-1$.

We present two pseudorandom measures for DH-GCS-II in the following section.

3 Pseudorandom Measures for DH-Generalized Cyclotomic Sequences

Theorem 1. *Suppose $\mathcal{V} = \{v_0, v_1, \ldots, v_{pq-1}\}$ is the DH-generalized cyclotomic sequence of order d defined as in Definition 2. Then the well-distribution measure of $\mathcal{V}$ satisfies*:

$$W(\mathcal{V}) < 36pq^{\frac{1}{2}} \log(q) \log(1+d) + p + q - 1.$$

Theorem 2. *Suppose $\mathcal{V} = \{v_0, v_1, \ldots, v_{pq-1}\}$ is the DH-generalized cyclotomic sequence of order d defined as in Definition 2. Then the correlation measure of order k (small) of $\mathcal{V}$ holds*:

$$C_k(\mathcal{V}) < 9k4^k pq^{1/2} \log(q) \log^k(1+d) + k(p+q-1).$$

In order to prove Theorems 1 and 2, we need the following statements.

We recall that $\mathcal{A} = \{\chi \in \widehat{\mathbb{Z}^*_{pq}} | \chi(h) = 1, \text{ for all, } h \in H\}$ and $\mathcal{A}^* = \mathcal{A} \setminus \{\chi_0\}$. For any $\chi \in \mathcal{A}$, there exist $\chi_p \in \mathbb{Z}_p^*$ and $\chi_q \in \mathbb{Z}_q^*$ such that $\chi = \chi_p\chi_q$ with $\chi_p^d = 1$ and $\chi_q^d = 1$, where $\chi_p \in \widehat{\mathbb{Z}^*_p}$ and $\chi_q \in \widehat{\mathbb{Z}^*_q}$. Let

$$\begin{aligned}
\mathcal{A}^{**} &= \{\chi_p\chi_q | \chi_p^d = 1, \chi_q^d = 1, \chi_p \neq 1, \chi_q \neq 1, \\
&\qquad \chi_p \in \widehat{\mathbb{Z}^*_p}, \chi_q \in \widehat{\mathbb{Z}^*_q}\}, \\
\mathcal{A}_p^{**} &= \{\chi_p\chi_q | \chi_p^d = 1, \chi_p \neq 1, \chi_q = 1, \chi_p \in \widehat{\mathbb{Z}^*_p}\}, \\
\mathcal{A}_q^{**} &= \{\chi_p\chi_q | \chi_q^d = 1, \chi_p = 1, \chi_q \neq 1, \chi_q \in \widehat{\mathbb{Z}^*_q}\}.
\end{aligned}$$

So $\mathcal{A}^* = \mathcal{A}^{**} \cup \mathcal{A}_p^{**} \cup \mathcal{A}_q^{**}$.

Lemma 2. *With notations as the above, let g and x be defined as in Section 1. Then we have*

(i) $\sum_{l=0}^{d-1} \chi(x^l) = 0$ *for any* $\chi \in \mathcal{A}^{**} \cup \mathcal{A}_p^{**}$;

(ii) $\sum_{l=0}^{d-1} \chi(x^l) = d$ *for any* $\chi \in \mathcal{A}_q^{**}$;

(iii) $\sum_{\chi \in \mathcal{A}_q^{**}} \left| \sum_{j=0}^{\frac{d}{2}-1} \chi(g^j) \right| < 2d \log(1+d)$.

Proof. By the definitions of x and g in Section 1, we have

$$\begin{aligned}
\sum_{l=0}^{d-1} \chi(x^l) &= \sum_{l=0}^{d-1} (\chi_p\chi_q)(x^l) \\
&= \sum_{l=0}^{d-1} \chi_p(x^l)\chi_q(x^l) = \sum_{l=0}^{d-1} \chi_p(g^l).
\end{aligned}$$

Then $\chi_p \neq 1$ yields (i), while $\chi_p = 1$ yields (ii). Now we prove (iii). Since

$$\sum_{\chi \in \mathcal{A}_q^{**}} \Big| \sum_{j=0}^{\frac{d}{2}-1} \chi(g^j) \Big| = \sum_{\substack{\chi_q \neq 1 \\ \chi_q^d = 1}} \Big| \sum_{j=0}^{\frac{d}{2}-1} \chi_q(g^j) \Big|$$

$$\leqslant \sum_{\substack{\chi_q \neq 1 \\ \chi_q^d = 1}} \frac{2}{|1 - \chi_q(g)|},$$

then the result follows from [12, Lemma 3]. □

Lemma 3[9]**.** *Suppose that q is a prime, χ_q is a non-principal multiplicative character modulo q of order d, $f(x) \in \mathbb{Z}_q[x]$ has s distinct roots in $\overline{\mathbb{Z}}_q$ and it is not a constant multiple of a d-th power of a polynomial over $\mathbb{Z}_q$. Let y be a real number with $0 < y \leqslant q$. Then any $x \in \mathbb{R}$:*

$$\Big| \sum_{x < n \leqslant x+y} \chi_q(f(n)) \Big| < 9sq^{1/2} \log(q).$$

Proof of Theorem 1. According to (1), for any non-negative integers a, b, t with $0 \leqslant a \leqslant a+(t-1)b \leqslant pq-1$, we have at most $\delta = p+q-1$ elements $i (0 \leqslant i \leqslant t-1)$ with $a + ib \in P \cup Q \cup R$. Hence, we get

$$\begin{aligned}
\Big| \sum_{i=0}^{t-1} (-1)^{v_{a+ib}} \Big| &\leqslant \Big| \sum_{\substack{i=0 \\ a+ib \in \mathbb{Z}^*_{pq}}}^{t-1} (-1)^{v_{a+ib}} \Big| + \delta \\
&= \frac{2}{d^2} \Big| \sum_{\substack{i=0 \\ a+ib \in \mathbb{Z}^*_{pq}}}^{t-1} \sum_{l=0}^{d-1} \sum_{j=0}^{\frac{d}{2}-1} \sum_{\chi \in \mathcal{A}^*} \overline{\chi}(a+bi)\chi(g^j x^l) \Big| + \delta \\
&= \frac{2}{d^2} \Big| \sum_{\chi \in \mathcal{A}^*} \sum_{l=0}^{d-1} \sum_{j=0}^{\frac{d}{2}-1} \chi(g^j x^l) \sum_{\substack{i=0 \\ a+ib \in \mathbb{Z}^*_{pq}}}^{t-1} \overline{\chi}(a+bi) \Big| + \delta \\
&= \frac{2}{d^2} \Big| \sum_{\chi \in \mathcal{A}^*} \sum_{l=0}^{d-1} \chi(x^l) \sum_{j=0}^{\frac{d}{2}-1} \chi(g^j) \sum_{\substack{i=0 \\ a+ib \in \mathbb{Z}^*_{pq}}}^{t-1} \overline{\chi}(a+bi) \Big| + \delta \\
&= \frac{2}{d^2} \Big| d \sum_{\chi \in \mathcal{A}_q^{**}} \sum_{j=0}^{\frac{d}{2}-1} \chi(g^j) \sum_{\substack{i=0 \\ a+ib \in \mathbb{Z}^*_{pq}}}^{t-1} \overline{\chi}(a+bi) \Big| + \delta \\
&\leqslant \frac{2}{d} \sum_{\chi \in \mathcal{A}_q^{**}} \Big| \sum_{j=0}^{\frac{d}{2}-1} \chi(g^j) \Big| \Big| \sum_{\substack{i=0 \\ a+ib \in \mathbb{Z}^*_{pq}}}^{t-1} \overline{\chi}(a+bi) \Big| + \delta.
\end{aligned}$$

We note that the set $\{a + ib \in \mathbb{Z}^*_{pq} | i = 0, \ldots, t-1\}$ can be divided into at most p blocks, and each block modulo q is contained in $\mathbb{Z}_q^*$. So for $\chi \in \mathcal{A}_q^{**}$

$$\begin{aligned}
\Big| \sum_{\substack{i=0 \\ a+ib \in \mathbb{Z}^*_{pq}}}^{t-1} \overline{\chi}(a+bi) \Big| &= \Big| \sum_{\substack{i=0 \\ a+ib \in \mathbb{Z}^*_{pq}}}^{t-1} \overline{\chi_q}(a+bi) \Big| \\
&< 9pq^{\frac{1}{2}} \log(q)
\end{aligned}$$

by Lemma 3. Hence by Lemma 2(iii) we have

$$\Big|\sum_{i=0}^{t-1}(-1)^{v_{a+ib}}\Big| \leqslant 4\log(1+d)\cdot 9pq^{\frac{1}{2}}\log(q)+\delta.$$

□

Proof of Theorem 2. According to (1), for integers $D=(d_1,\ldots,d_k)$ and M with $0\leqslant d_1<\cdots<d_k\leqslant pq-M$, there are at most $k\delta$, where $\delta=p+q-1$, elements m $(0\leqslant m\leqslant M<pq-1)$ such that at least one number $m+d_j\in P\cup Q\cup R$, where $1\leqslant j\leqslant k$. Hence, we got

$$\begin{aligned}&\Big|\sum_{m=0}^{M-1}(-1)^{v_{m+d_1}+v_{m+d_2}+\cdots+v_{m+d_k}}\Big|\\ &\leqslant\Big|\sum_{\substack{m=0\\ m+d_j\in\mathbb{Z}_{pq}^*\\ 1\leqslant j\leqslant k}}^{M-1}(-1)^{v_{m+d_1}+v_{m+d_2}+\cdots+v_{m+d_k}}\Big|+k\delta\end{aligned}$$

$$\begin{aligned}&=\frac{2^k}{d^{2k}}\Big|\sum_{\substack{m=0\\ m+d_j\in\mathbb{Z}_{pq}^*\\ 1\leqslant j\leqslant k}}^{M-1}\prod_{j=1}^{k}\Big(\sum_{l=0}^{d-1}\sum_{i=0}^{\frac{d}{2}-1}\\ &\quad\sum_{\chi\in\mathcal{A}^*}\overline{\chi}(m+d_j)\chi(g^ix^l)\Big)\Big|+k\delta\\ &=\frac{2^k}{d^{2k}}\Big|\sum_{\substack{m=0\\ m+d_j\in\mathbb{Z}_{pq}^*\\ 1\leqslant j\leqslant k}}^{M-1}\prod_{j=1}^{k}\Big(\sum_{\chi\in\mathcal{A}^*}\overline{\chi}(m+d_j)\\ &\quad\sum_{l=0}^{d-1}\chi(x^l)\sum_{i=0}^{\frac{d}{2}-1}\chi(g^i)\Big)\Big|+k\delta\\ &=\frac{2^k}{d^k}\Big|\sum_{\substack{m=0\\ m+d_j\in\mathbb{Z}_{pq}^*\\ 1\leqslant j\leqslant k}}^{M-1}\prod_{j=1}^{k}\Big(\sum_{\chi\in\mathcal{A}_q^{**}}\overline{\chi}(m+d_j)\\ &\quad\sum_{i=0}^{\frac{d}{2}-1}\chi(g^i)\Big)\Big|+k\delta\\ &=\frac{2^k}{d^k}\Big|\sum_{\psi_1,\ldots,\psi_k\in\mathcal{A}_q^{**}}\sum_{i_1=0}^{\frac{d}{2}-1}\psi_1(g^{i_1})\cdots\\ &\quad\sum_{i_k=0}^{\frac{d}{2}-1}\psi_k(g^{i_k})\sum_{\substack{m=0\\ m+d_j\in\mathbb{Z}_{pq}^*\\ 1\leqslant j\leqslant k}}^{M-1}\prod_{j=1}^{k}\overline{\psi}_j(m+d_j)\Big|+k\delta\end{aligned}$$

$$\begin{aligned}&=\frac{2^k}{d^k}\Big|\sum_{\psi_1\in\mathcal{A}_q^{**}}\sum_{i_1=0}^{\frac{d}{2}-1}\psi_1(g^{i_1})\cdots\sum_{\psi_k\in\mathcal{A}_q^{**}}\\ &\quad\sum_{i_k=0}^{\frac{d}{2}-1}\psi_k(g^{i_k})\sum_{\substack{m=0\\ m+d_j\in\mathbb{Z}_{pq}^*\\ 1\leqslant j\leqslant k}}^{M-1}\prod_{j=1}^{k}\overline{\psi}_j(m+d_j)\Big|+k\delta.\end{aligned}$$

Since $\mathcal{A}_q^{**}\cup\{1\}$ is a cyclic subgroup of $\widehat{\mathbb{Z}_q^*}$, let ϕ be a generator of $\mathcal{A}_q^{**}\cup\{1\}$. Then for each $\overline{\psi}_j$, $1\leqslant j\leqslant k$, there exists an integer $\alpha_j\in[1,d-1]$ such that $\overline{\psi}_j=\phi^{\alpha_j}$. So, by Lemma 3 we obtain

$$\begin{aligned}&\Big|\sum_{\substack{m=0\\ m+d_j\in\mathbb{Z}_{pq}^*\\ 1\leqslant j\leqslant k}}^{M-1}\prod_{j=1}^{k}\overline{\psi}_j(m+d_j)\Big|=\Big|\sum_{\substack{m=0\\ m+d_j\in\mathbb{Z}_{pq}^*\\ 1\leqslant j\leqslant k}}^{M-1}\prod_{j=1}^{k}\phi^{\alpha_j}(m+d_j)\Big|\\ &=\Big|\sum_{\substack{m=0\\ m+d_j\in\mathbb{Z}_{pq}^*\\ 1\leqslant j\leqslant k}}^{M-1}\phi((m+d_1)^{\alpha_1}\cdots(m+d_k)^{\alpha_k})\Big|\\ &\leqslant 9kpq^{1/2}\log(q).\end{aligned}$$

Hence, we have

$$\begin{aligned}&\Big|\sum_{m=0}^{M-1}(-1)^{v_{m+d_1}+v_{m+d_2}+\cdots+v_{m+d_k}}\Big|\\ &\leqslant\frac{2^k}{d^k}\cdot 9kpq^{\frac{1}{2}}\log(q)\cdot\Big|\sum_{\psi_1\in\mathcal{A}_q^{**}}\sum_{i_1=0}^{\frac{d}{2}-1}\\ &\quad\psi_1(g^{i_1})\cdots\sum_{\psi_k\in\mathcal{A}_q^{**}}\sum_{i_k=0}^{\frac{d}{2}-1}\psi_k(g^{i_k})\Big|+k\delta\\ &\leqslant\frac{2^k}{d^k}\cdot 9kpq^{\frac{1}{2}}\log(q)\cdot\prod_{j=1}^{k}\Big|\sum_{\psi_j\in\mathcal{A}_q^{**}}\sum_{i_j=0}^{\frac{d}{2}-1}\psi_j(g^{i_j})\Big|+k\delta\\ &\leqslant\frac{2^k}{d^k}\cdot 9kpq^{\frac{1}{2}}\log(q)\prod_{j=1}^{k}\sum_{\psi_j\in\mathcal{A}_q^{**}}\Big|\sum_{i_j=0}^{\frac{d}{2}-1}\psi_j(g^{i_j})\Big|+k\delta\\ &\leqslant\frac{2^k}{d^k}\cdot 9kpq^{\frac{1}{2}}\log(q)\cdot(2d\log(1+d))^k+k\delta\\ &\leqslant 9k4^kpq^{\frac{1}{2}}\log(q)\log^k(1+d)+k\delta.\end{aligned}$$

□

The bound in Theorem 1 is of order $O(pq^{1/2}\log(q)\log(d))$ and the bound in Theorem 2 is of order $O(pq^{1/2}\log(q)\log^k(d))$, where the implied constant only depends on k. While in the most interesting case, when $|p-q|$ is small, the bound in

Theorems 1 and 2 is of order $O(q^{3/2}\log(q)\log(d))$ and $O(q^{3/2}\log(q)\log^k(d))$, respectively.

4 Final Remarks and Conclusion

To the best of our knowledge, W-GCS-I, W-GCS-II, DH-GCS-I and DH-GCS-II are the main generalized cyclotomic sequences of length pq. Many slight modifications based on these four sequences are introduced in the literature.

1) In [22], the generalized cyclotomic sequence $\mathcal{X} = \{x_0, x_1, \ldots, x_{pq-1}\}$ of order $d = 2$ has been defined based on DH-GSC-I (or DH-GSC-II), that is, let $Q = Q_0 \cup Q_1$ and $P = P_0 \cup P_1$, where

$$\begin{aligned} Q_0 &= \{g^{2s} \pmod q | s = 0, 1, \ldots, (q-1)/2-1\},\\ Q_1 &= \{g^{2s+1} \pmod q | s = 0, 1, \ldots, (q-1)/2-1\},\\ P_0 &= \{g^{2s} \pmod p | s = 0, 1, \ldots, (p-1)/2-1\},\\ P_1 &= \{g^{2s+1} \pmod p | s = 0, 1, \ldots, (p-1)/2-1\}. \end{aligned}$$

Then (we note that $d = 2$),

$$C_0'' = R \cup pQ_0 \cup qP_0 \cup D_0',\ C_1'' = pQ_1 \cup qP_1 \cup D_1',$$

and the sequence is defined by

$$x_i = \begin{cases} 0, & \text{if} \quad i \in C_0'';\\ 1, & \text{if} \quad i \in C_1''. \end{cases}$$

The sequence has $(pq-1)/2$ 1's and $(pq+1)/2$ 0's, which is of optimum balance. It has large linear complexity, which takes on one of pq, $pq-1$, $pq-(q-1)/2$, $pq-(q-1)/2-1$, $(pq+1)/2$ and $(pq-1)/2$, depending on the values p mod 8 and q mod 8[22]. It also has three-valued, or four-valued, or five-valued autocorrelation values[23]. But the values are not low.

2) Similarly, [24] introduces a modification of DH-GCS-II of order $d = 4$. The sequence $\mathcal{Y} = \{y_0, y_1, \ldots, y_{pq-1}\}$ is defined by

$$y_i = \begin{cases} 0, & \text{if} \quad i \in C_0''';\\ 1, & \text{if} \quad i \in C_1''', \end{cases}$$

where

$$\begin{aligned} C_0''' &= R \cup pQ_0' \cup pQ_1' \cup qP_0' \cup qP_1' \cup D_0' \cup D_1',\\ C_1''' &= pQ_2' \cup pQ_3' \cup qP_2' \cup qP_3' \cup D_2' \cup D_3', \end{aligned}$$

where

$$\begin{aligned} Q_i' &= \{g^{4s+i} \pmod q | s = 0, 1, \ldots, (q-1)/4-1\},\\ P_i' &= \{g^{4s+i} \pmod p | s = 0, 1, \ldots, (p-1)/4-1\}, \end{aligned}$$

for $i = 0, 1, 2, 3$. It also has large linear complexity[24]. These results have been extended to the case of any even number d[25].

3) [26] introduces a modification $\mathcal{Z} = \{z_0, z_1, \ldots, z_{pq-1}\}$ of DH-GCS-I of any order d by defining

$$z_i = \begin{cases} 0, & \text{if} \quad i \in \widetilde{C_0};\\ 1, & \text{if} \quad i \in \widetilde{C_1}, \end{cases}$$

where

$$\begin{aligned} Q_i'' &= \{g^{ds+i} \pmod q | s = 0, 1, \ldots, (q-1)/d-1\},\\ P_i'' &= \{g^{ds+i} \pmod p | s = 0, 1, \ldots, (p-1)/d-1\} \end{aligned}$$

$i = 0, 1, \ldots, d-1$, and

$$\widetilde{C_0} = R \cup \Big(\bigcup_{j=0}^{\frac{d}{2}-1} pQ_{2j}''\Big) \cup \Big(\bigcup_{j=0}^{\frac{d}{2}-1} qP_{2j}'\Big) \cup \Big(\bigcup_{j=0}^{\frac{d}{2}-1} D_{2j}'\Big),$$

$$\widetilde{C_1} = \Big(\bigcup_{j=0}^{\frac{d}{2}-1} pQ_{2j+1}''\Big) \cup \Big(\bigcup_{j=0}^{\frac{d}{2}-1} qP_{2j+1}'\Big) \cup \Big(\bigcup_{j=0}^{\frac{d}{2}-1} D_{2j+1}'\Big).$$

The trace representation of $\mathcal{Z}$ has been determined in [26]. By Key's method, a different idea from [3, 8, 15, 20, 22–24], the linear complexity is derived from the trace representation. Although the linear complexity is large, the autocorrelation values may not be low since $(-1)^{z_i} = (i/q)$ for any $i \in \mathbb{Z}_{pq}^*$.

We see that all these modifications are obtained only by re-dividing P and Q into different sub-sets, which do not change the constructions of corresponding generalized cyclotomic sequences (DH-GCS-I or DH-GCS-II) essentially.

From the known results, we see that both Whiteman-generalized cyclotomic sequences and DH-generalized cyclotomic sequences have large linear complexity, but the former seems somewhat superior to the latter due to the autocorrelation.

From the construction, DH-GCS-II seems somewhat superior to DH-GCS-I. But it needs to study further, such as the linear complexity and autocorrelation of DH-GCS-II. It is also interesting to consider the linear complexity and the autocorrelation of W-GCS-II.

We also remark that in [13] the well-distribution measure and the correlation measure of order k of W-GCS-I are also estimated and other two families of binary sequences of length pq are constructed in different ways. In fact, an extension of W-GCS-I is considered in [13].

References

[1] Cusick T W, Ding C, Renvall A. Stream Ciphers and Number Theory. Amsterdam: Elsevier, 1998.

[2] Ding C. Binary cyclotomic generators. *Fast Software Encryption, Lecture Notes in Comput. Sci.*, Berlin: Springer-Verlag, Vol. 1008, 1995, pp.20–60.

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

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

[5] Ding C. Autocorrelation values of generalized cyclotomic sequences of order two. *IEEE Transactions on Information Theory*, 1998, 44(4): 1699–1702.

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

[7] Ding C. Pattern distributions of Legendre sequences. *IEEE Transactions on Information Theory*, 1998, 44(4): 1693–1698.

[8] Ding C, Helleseth T, Shan W. On the linear complexity of Legendre sequences. *IEEE Transactions on Information Theory*, 1998, 44(3): 1276–1278.

[9] Mauduit C, Sárközy A. On finite pseudorandom binary sequences I: Measures of pseudorandomness, the Legendre symbol. *Acta Arithmetica*, 1997, 82: 365–377.

[10] Cassaigne J, Mauduit C, Sárközy A. On finite pseudorandom binary sequences, VII: The measures of pseudorandomness. *Acta Arithmetica*, 2002, 103: 97–118.

[11] Chen Z. Finite binary sequences constructed by explicit inversive methods. *Finite Fields and Their Applications*, 2007, DOI: 10.1016/j.ffa.2007.08.002.

[12] Gyarmati K. On a family of pseudorandom binary sequences. *Periodica Mathematica Hungarica*, 2004, 49(2): 45–63.

[13] Rivat J, Sárközy A. Modular constructions of pseudorandom binary sequences with composite moduli. *Periodica Math. Hungarica*, 2005, 51(2): 75–107.

[14] Dai Z D, Gong G, Song H Y. Trace representation of binary Jacobi sequences. Technical Reports CORR 2002-32, 2002, http://www.cacr.math.uwaterloo.ca/.

[15] Bai E, Fu X, Xiao G. On the linear complexity of generalized cyclotomic sequences of order four over Z_{pq}. *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, 2005, E88-A(1): 392–395.

[16] Bai E. Study on construction and randomness analysis of pseudorandom sequences [Dissertation]. Xidian University, China, 2004. (in Chinese)

[17] Brandstätter N, Winterhof A. Some notes on the two-prime generator of order 2. *IEEE Transactions on Information Theory*, 2005, 51(10): 3654–3657.

[18] Lidl R, Niederreiter H. Finite Fields. Reading: Addison-Wesley, MA, 1983.

[19] Chen Z, Du X, Xiao G. Sequences related to Legendre/Jacobi sequences. *Information Sciences*, 2007, 177(21): 4820–4831.

[20] Li S, Chen Z, Sun R, Xiao G. On the randomness of generalized cyclotomic sequences of order two and length *pq*. *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, 2007, E90-A(9): 2037–2041.

[21] Li S, Chen Z, Fu X, Xiao G. The autocorrelation values of new generalized cyclotomic sequences of order two and length *pq*. *Journal of Computer Science and Technology*, 2007, 22(6): 830–834.

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

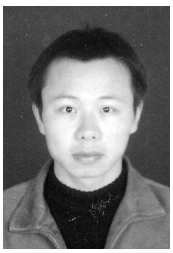
[23] Yan T, Sun R, Xiao G. Autocorrelation and linear complexity of the new generalized cyclotomic sequences. *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, 2007, E90-A (4): 857–864.

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

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

[26] Du X, Yan T, Xiao G. Trace representation of some generalized cyclotomic sequences of length *pq*. *Information Sciences*, 2008, 178(16): 3307–3316.

Zhi-Xiong Chen received the M.S. degree in mathematics from Fujian Normal University in 1999 and Ph.D. degree in cryptography from Xidian University in 2006. Now he is an associate professor at Putian University. His research interests include stream ciphers, elliptic curve cryptography and algebra.



Sheng-Qiang Li received the B.S. degree in mathematics from University of Electronic Science and Technology of China in 2003, and Ph.D. degree in cryptography from Xidian University in 2008. Now he is a lecturer at University of Electronic Science and Technology of China in Chengdu. His research interests include stream ciphers and secure communication.