Sequences related to Legendre/Jacobi sequences

Zhixiong Chen a,*, Xiaoni Du b,c, Guozhen Xiao b

a Department of Mathematics, Putian University, Putian, Fujian 351100, China
b National Key Laboratory of I.S.N, Xidian University, Xi’an 710071, China
c Department of Mathematics, Northwest Normal University, Lanzhou 730070, China

Received 6 October 2006; received in revised form 11 February 2007; accepted 13 February 2007

Abstract

Two families of binary sequences are constructed from $d$th order cyclotomic generator and from $d$th order generalized cyclotomic generator with respect to two distinct primes respectively. By using estimates of certain exponential sums over rings or fields, the upper bounds of both the well-distribution measure and the order $k$ (at least for small $k$) correlation measure of the resulting binary sequences are evaluated, and some lower bounds on the linear complexity profile of $d$-ary cyclotomic sequences and $d$-ary generalized cyclotomic sequences are presented. Our results indicate that such binary sequences possess “very good” local pseudo-randomness.

© 2007 Elsevier Inc. All rights reserved.

Keywords: Legendre and Jacobi sequences; Generalized cyclotomic sequences; Exponential sums; Well-distribution measure; Correlation measure of order $k$; Linear complexity profile

1. Introduction

Legendre sequence is a well-known binary sequence with ideal periodic and aperiodic autocorrelation functions, it is also known to exhibit large linear complexity, which makes it significant for cryptographic applications. Jacobi and modified Jacobi sequences are constructed by combining two appropriate Legendre sequences, and they also have good correlation properties and large linear complexity. For more information on this subject the reader is referred to [6,9,8,16,10,13,18,19,21].

Ding et al. applied the theory of cyclotomy, which is an old topic of elementary number theory, to construct and study a family of pseudo-random sequences, which are called (generalized) cyclotomic sequences, which include Legendre sequences, Jacobi and modified Jacobi sequences [6,7,10–12,14,15,22,23,1,2,27]. Most generalized cyclotomic sequences have good periodic/aperiodic correlation properties and large linear complexity, which give them some cryptographic significance. Cyclotomic classes and generalized cyclotomic classes play an important role in constructing generalized cyclotomic sequences.
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 $\mathbb{Z}_{m}^*$ by 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

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

If $D_0$ is a multiplicative subgroup of $\mathbb{Z}_{m}^*$, then there exist elements $g_1, \ldots, g_{d-1}$ of $\mathbb{Z}_{m}^*$ such that $D_i = g_iD_0$ for all $i \in [1,d - 1]$. 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. Different $D_0$ gives different (generalized) cyclotomic classes of order $d$.

Two important measures, the well-distribution measure and the correlation measure of order $k$, were introduced by Mauduit and Sárközy \cite{25} to evaluate the (local) pseudo-randomness of a finite binary sequence:

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

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

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

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

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

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

$S_N$ 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 $N \to \infty$). It was shown in \cite{4} that for a “truely” random sequence $S_N \in \{+1, -1\}^N$ (i.e., choosing $S_N \in \{+1, -1\}^N$ with probability $1/2^N$), both $W(S_N)$ and $C_k(S_N)$ (for some fixed $k$) are around $N^{1/2}$ with “near 1” probability.

For the Legendre sequence $S_p = \{s_1, s_2, \ldots, s_p\} \in \{+1, -1\}^p$ with

$$s_n = \begin{cases} \left( \frac{n}{p} \right), & \text{if } \gcd(n, p) = 1; \\ 1, & \text{if } p | n, \end{cases}$$

it was shown by Mauduit and Sárközy in \cite{25} that

$$W(S_p) = O(p^{1/2} \log(p)) \quad \text{and} \quad C_k(S_p) = O(kp^{1/2} \log(p)),$$

which indicate that the Legendre sequence forms a “good” pseudo-random sequence. Many other “good” (but slightly inferior) binary sequences were designed in the literature, see for example \cite{4, 5, 17, 20, 26, 28, 29} and references therein.

In this article, we continue to study the cyclotomic sequences and generalized cyclotomic sequences of order $d$. We first define cyclotomic classes of order $d$ for $\mathbb{F}_p^*$ and generalized cyclotomic classes of order $d$ for $\mathbb{Z}_{pq}^*$, respectively, where $p, q$ are two distinct primes. Then we define $d$-ary cyclotomic sequences (resp. $d$-ary generalized cyclotomic sequences) from the corresponding cyclotomic classes (resp. generalized cyclotomic classes) and construct binary sequences from $d$-ary cyclotomic sequences and $d$-ary generalized cyclotomic sequences respectively. Using estimates of certain exponential sums, we investigate the well-distribution measure and the correlation measure of order $k$ of the resulting binary sequences and the linear complexity profile of the resulting polyphase (generalized) cyclotomic sequences respectively.

This article is organized as follows. In Section 2, some basic results on the exponential sums over residue ring $\mathbb{Z}_m$ are introduced. In Section 3, polyphase cyclotomic sequences and binary sequences are constructed. The well-distribution measure and the correlation measure of order $k$ of the resulting binary sequences are
estimated. A lower bound on linear complexity profile of the resulting polyphase cyclotomic sequences is presented. Another family of binary sequences and polyphase generalized cyclotomic sequences are constructed in Section 4. A conclusion is drawn in Section 5.

As usual, we suppose that a binary sequence is always defined over \{0, 1\}.

2. Exponential sums over rings

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 \(\chi(x) = 1\) for any \(x \in \mathbb{Z}_m^*\) is called the principal character and denoted by \(\chi_0 = 1\). \(\mathbb{Z}_m^*\) is denoted by the set of all multiplicative characters of \(\mathbb{Z}_m^*\). It is easy to see that \(\mathbb{Z}_m^*\) forms a group, which is isomorphic to \(\mathbb{Z}_m^*\), with the principal character \(\chi_0\) as the neutral element under the multiplication of characters.

For any \(\chi \in \widehat{\mathbb{Z}}_m^*\), we set \(\overline{\chi}(x) = \chi(x^{-1})\), i.e., \(\overline{\chi}\) is the inverse of \(\chi\). For convenience, we extend the definition \(\chi\) to \(\mathbb{Z}_m\) only by defining \(\chi(x) = 0\) for \(x\) with \(\gcd(x, m) > 1\).

**Lemma 1** [24]. Let \(\#\widehat{\mathbb{Z}}_m^*\) denote the cardinality of \(\widehat{\mathbb{Z}}_m^*\). For any element \(x \in \mathbb{Z}_m^*\),
\[
\sum_{\chi \in \widehat{\mathbb{Z}}_m^*} \chi(x) = \begin{cases} 0, & \text{if } x \neq 1; \\ \#\widehat{\mathbb{Z}}_m^*, & \text{otherwise}. \end{cases}
\]

And for any character \(\chi \in \widehat{\mathbb{Z}}_m^*\),
\[
\sum_{\chi \in \widehat{\mathbb{Z}}_m^*} \chi(x) = \begin{cases} 0, & \text{if } \chi \neq \chi_0; \\ \#\widehat{\mathbb{Z}}_m^*, & \text{otherwise}. \end{cases}
\]

**Remark 1.** \(\mathbb{Z}_m^*\) and \(\widehat{\mathbb{Z}}_m^*\) in Lemma 1 can be replaced by any finite Abelian groups \(G\) and \(\widehat{G}\), the character group of \(G\), respectively.

When \(m = p\) is a prime. Let \(g\) be a fixed primitive root modulo \(p\). For each \(x \in \mathbb{F}_p^*\), let \(\text{ind}(x)\) denote the index (or discrete logarithm) of \(x\) to the base \(g\) so that
\[
g^{\text{ind}(x)} \equiv x \pmod{p}.
\]

We add the condition
\[
1 \leq \text{ind}(x) < p - 1
\]
to make the value of index unique.

\(\mathbb{F}_p^*\), the multiplicative characters group of \(\mathbb{F}_p^*\), is exactly equal to the following set:
\[
\left\{ \chi_a | \chi_a(x) = \exp\left(\frac{2\pi ia \cdot \text{ind}(x)}{p - 1}\right) \text{ for all } x \in \mathbb{F}_p^* \text{ and } a \in \mathbb{Z}_{p-2} \right\}.
\]

\(\mathbb{F}_p^*\) forms a cyclic group with the principal character \(\chi_0 = 1\) under the multiplication of characters.

**Lemma 2.** Let \(1 \leq d \leq p - 1\) and \(d | p - 1\). Let \(g\) be a primitive root of \(\mathbb{F}_p^*\). For \(0 \leq x < x + y \leq p - 1\), the following bound holds:
\[
\left| \sum_{\chi \neq 1} \sum_{j=0}^{x-y} \chi(g^j) \right| < 2d \log(1 + d),
\]
where \(\chi \in \widehat{\mathbb{F}}_p^*\).
Proof. For each \( \chi \neq 1 \) with \( \chi^d = 1 \), we have

\[
\sum_{j=x}^{x+d-1} \chi(g^j) = \chi(g^x) \sum_{j=0}^{d-1} \chi(g^j) = 0.
\]

Now the result follows from the proof of [20, Lemma 3]. \( \square \)

**Lemma 3** [25]. Suppose that \( p \) is a prime, \( \chi \) is a non-principal multiplicative character modulo \( p \) of order \( d \), \( f(x) \in \mathbb{F}_p[x] \) has \( s \) distinct roots in \( \mathbb{F}_p \) and it is not a constant multiple of a \( d \)th power of a polynomial over \( \mathbb{F}_p \). Let \( y \) be a real number with \( 0 < y \leq p \). Then any \( x \in \mathbb{R} \):

\[
\left| \sum_{x < n < x+y} \chi(f(n)) \right| < 9sp^{1/2}\log(p).
\]

3. Sequences related to the Legendre sequences

In this section, let \( p \) be a prime and \( p - 1 = df \). Let \( g \) be a generator of \( \mathbb{F}_p^* \). The cyclotomic classes of order \( d \) give a partition of \( \mathbb{F}_p^* \) defined by

\[
D_l = \{ g^{dj+i} | j = 0, 1, \ldots, f - 1 \}, \quad l = 0, 1, \ldots, d - 1.
\]

The cyclotomic sequence \( \mathcal{S} \) is \( \{ s_1, s_2, \ldots \} \) of order \( d \) over \( \mathbb{Z}_d \) with respect to the prime \( p \) is defined by

\[
s_n := \begin{cases} 
1, & \text{if} \quad \lfloor n \mod p \rfloor \in D_l; \\
0, & \text{if} \quad \gcd(n, p) \neq 1,
\end{cases}
\]

for each \( n \geq 1 \), where \( l = 0, 1, \ldots, d - 1 \). \( \mathcal{S} \) is also called the polyphase (or \( d \)-ary) cyclotomic sequence.

When \( d = 2 \), the cyclotomic sequence defined as above is the Legendre sequence, whose linear complexity has been presented in [16] and pattern distributions in [12]. When \( d \) is an odd prime, the linear complexity of the corresponding cyclotomic sequence can be found in [15].

Now we suppose that \( d > 2 \) is even in this section. We define a binary sequence \( \mathcal{H} \) from the cyclotomic sequence \( \mathcal{S} \) (defined as in (1)) of order \( d \) over \( \mathbb{Z}_d \):

\[
u_n = \begin{cases} 
0, & \text{if} \quad 0 \leq s_n < \frac{d}{2} - 1; \\
1, & \text{if} \quad \frac{d}{2} \leq s_n \leq d - 1,
\end{cases}
\]

for each \( n \geq 1 \). Obviously the period of \( \mathcal{H} \) is \( p \). Equivalently, if we set

\[
C_0 = D_0 \cup D_1 \cup \cdots \cup D_{\frac{d}{2}-1}, \quad C_1 = D_{\frac{d}{2}} \cup D_{\frac{d}{2}+1} \cup \cdots \cup D_{d-1}
\]

then we have

\[
u_n = \begin{cases} 
0, & \text{if} \quad \lfloor n \mod p \rfloor \in C_0; \\
1, & \text{if} \quad \lfloor n \mod p \rfloor \in C_1; \\
0, & \text{if} \quad \gcd(n, p) \neq 1.
\end{cases}
\]

One can define different \( C_0, C_1 \) to construct different binary sequence. For example, if we set

\[
C'_0 = \bigcup_{i=0}^{\frac{d}{2}-1} D_{2i}, \quad C'_1 = \bigcup_{i=0}^{\frac{d}{2}-1} D_{2i+1}
\]

then a binary sequence can be constructed in a similar way as in (3) with \( C'_0, C'_1 \) in place of \( C_0, C_1 \). In fact this sequence is the Legendre sequence. Another example is the Hall’s sextic residue sequence \( (h_i) \), which is defined as follows:

\[1\] In this case, \( d = 6 \).
for \( i \geq 1 \). The linear complexity and trace representation of the Hall’s sextic residue sequence are determined in [22,23] respectively.

### 3.1. Distribution and correlation of \( U^n \)

Suppose \( U^n \) is defined as in (3) and \( \hat{U}_p^n \) is the set of all multiplicative characters of \( \mathbb{F}_p^* \). Let

\[
\mathcal{G} = \left\{ \chi \in \hat{U}_p^n | \chi^d = 1 \right\}.
\]

It is easy to see that \( \mathcal{G} \) is a cyclic subgroup of \( \hat{U}_p^n \) with \( \#\mathcal{G} = d \). From the definition of \( U^n \), we have

\[
\frac{1}{d} \sum_{j=0}^{d-1} \mathcal{Z}(n) \chi(g^j) = \begin{cases} 1, & \text{if } [n \mod p] \in C_0; \\ 0, & \text{if } [n \mod p] \in C_1, \end{cases}
\]

for any \( n \geq 1 \) with \( \gcd(p, n) = 1 \) by Lemma 1 and Remark 1. Hence for any \( n \geq 1 \) with \( \gcd(p, n) = 1 \),

\[
(-1)^n = 2 \frac{1}{d} \sum_{j=0}^{d-1} \sum_{x \in \mathcal{G}} \mathcal{Z}(n) \chi(g^j) = \begin{cases} +1, & \text{if } [n \mod p] \in C_0; \\ -1, & \text{if } [n \mod p] \in C_1, \end{cases}
\]

where \( \mathcal{G} = \mathcal{G} \setminus \{ \chi_0 \} \).

**Theorem 1.** Let \( \mathcal{U}_p = \{u_1, u_2, \ldots, u_p\} \) be a sequence generated as in (3). Then the well-distribution measure of \( \mathcal{U}_p \) satisfies:

\[
W(\mathcal{U}_p) < 36p^{1/2} \log(p) \log(1 + d).
\]

**Proof.** According to Eq. (4), for any \( a, b, t \in \mathbb{N} \) with \( 1 \leq a < a + (t - 1)b \leq p \),

\[
\sum_{i=0}^{t-1} (-1)^{u_i+ib} = 2 \frac{1}{d} \sum_{j=0}^{d-1} \sum_{x \in \mathcal{G}} \mathcal{Z}(a + ib) \chi(g^j) = 2 \frac{1}{d} \sum_{x \in \mathcal{G}} \chi(g^j) \sum_{i=0}^{t-1} \mathcal{Z}(a + ib)
\]

\[
\leq 2 \frac{1}{d} \sum_{x \in \mathcal{G}} \chi(g^j) \cdot \sum_{i=0}^{t-1} \mathcal{Z}(a + ib).
\]

Now by Lemmas 2 and 3, we obtain the desired result. \( \square \)

**Theorem 2.** Let \( \mathcal{U}_p = \{u_1, u_2, \ldots, u_p\} \) be a sequence generated as in (3). Then the correlation measure of order \( k \) of \( \mathcal{U}_p \) holds:

\[
C_k(\mathcal{U}_p) < 9k4^k p^{1/2} \log^k(1 + d) \log(p).
\]

**Proof.** According to Eq. (4), for integers \( D = (d_1, \ldots, d_k) \) and \( M \) with \( 0 \leq d_1 < \cdots < d_k \leq p - M \), we have

\[
\sum_{n=1}^{M} (-1)^{u_{d_1} + u_{d_2} + \cdots + u_{d_k}} = 2^k \frac{1}{d^k} \sum_{n=1}^{M} \prod_{j=1}^{k} \left( \sum_{i=0}^{d_j-1} \mathcal{Z}(n + d_j) \chi(g^i) \right)
\]

\[
= 2^k \frac{1}{d^k} \sum_{x_1, \ldots, x_k \in \mathcal{G}} \sum_{i_1=0}^{d_j-1} \chi_1(g^{i_1}) \cdots \sum_{i_k=0}^{d_k-1} \chi_k(g^{i_k}) \sum_{n=1}^{M} \prod_{j=1}^{k} \mathcal{Z}(n + d_j)
\]

\[
= 2^k \frac{1}{d^k} \sum_{x_1 \in \mathcal{G}} \sum_{i_1=0}^{d_j-1} \chi_1(g^{i_1}) \cdots \sum_{x_k \in \mathcal{G}} \chi_k(g^{i_k}) \sum_{n=1}^{M} \prod_{j=1}^{k} \mathcal{Z}(n + d_j) \quad (*)
\]
We recall that $\mathcal{G}$ is a cyclic subgroup of $\widehat{\mathbb{F}}_p^*$ with $\# \mathcal{G} = d$. Suppose $\psi$ is a generator of $\mathcal{G}$, i.e., the order of $\psi$ is $d$. Then for each $\gamma_j$, $1 \leq j \leq k$, there exists an integer $x_j \in [1, d - 1]$ such that $\gamma_j = \psi^{x_j}$. So by Lemma 3 we obtain

$$\left| \sum_{n=1}^{M} \prod_{j=1}^{k} \gamma_j(n + d_j) \right| = \left| \sum_{n=1}^{M} \prod_{j=1}^{k} \psi^{x_j}(n + d_j) \right| = \left| \sum_{n=1}^{M} \psi\left((n + d_1)^{x_1} \cdots (n + d_k)^{x_k}\right) \right| < 9kp^{1/2}\log(p).$$

Hence

$$\frac{2k}{d^2} \cdot 9kp^{1/2}\log(p) \cdot \left| \sum_{j=1}^{d} \sum_{i=0}^{d-1} \chi_1(g^i) \cdots \sum_{j=1}^{d} \sum_{i=0}^{d-1} \chi_d(g^i) \right| = \frac{2k}{d^2} \cdot 9kp^{1/2}\log(p) \cdot \prod_{j=1}^{M} \sum_{i=0}^{d-1} \chi_j(g^i).$$

We complete the proof by Lemma 2. □

We note that the construction of $\mathcal{U}_p$ is an extension of a binary sequence derived from discrete logarithm in [29]. Theorems 1 and 2 indicate that $\mathcal{U}_p$ forms a “good” (but slightly inferior) pseudorandom binary sequence, which is somewhat superior to the sequence in [29].

### 3.2. Linear complexity of $\mathcal{S}^{\infty}$

Ding [15] determined the linear complexity (and minimal polynomials) of the $d$th order cyclotomic sequences over $\mathbb{Z}_d$ when $d$ is an odd prime. We recall that the linear complexity profile of a sequence $S = \{s_0, s_1, \cdots\}$ over the ring $\mathbb{Z}_d$ is the function $L(S, N)$ defined for every positive integer $N$, as the least order $L$ of a linear recurrence relation over $\mathbb{Z}_d$

$$s_n = c_1 s_{n-1} + \cdots + c_L s_{n-L},$$

for all $L \leq n \leq N - 1$, which $S$ satisfies. We use the convention that $L(S, N) = 0$ if the first $N$ elements of $S$ are all zero and $L(S, N) = N$ if the first $N - 1$ elements of $S$ are zero and $s_{N-1} \neq 0$. The value

$$L(S) = \sup_{N \geq 1} L(S, N)$$

is called the linear complexity of the sequence $S$, see for example [3,6]. For the linear complexity of any periodic sequence of period $t$ one easily verifies that $L(S) = L(S, 2t) \leq t$. It is desirable to have sequences with large linear complexity for cryptographic applications.

**Proposition 1** [15]. The $d$th order cyclotomic sequence $\mathcal{S}^{\infty} = \{s_1, s_2, \ldots\}$ is defined as in (1). If $d$ is an odd prime then the linear complexity $L(\mathcal{S}^{\infty})$ satisfies

$$L(\mathcal{S}^{\infty}) = \begin{cases} p - 1, & \text{if } d \notin D_0; \\ \frac{(d-1)(p-1)}{d}, & \text{if } d \in D_0. \end{cases}$$

**Theorem 3**. The $d$th order cyclotomic sequence $\mathcal{S}^{\infty} = \{s_1, s_2, \ldots\}$ is defined as in (1). The linear complexity profile $L(\mathcal{S}^{\infty}, N)$ satisfies

$$L(\mathcal{S}^{\infty}, N) \geq \frac{N + 1}{1 + 9p^{1/2}\log(p)} - 1.$$

for $N < p$ and any $d$ (prime or composite).

**Proof.** Suppose $L(\mathcal{S}^{\infty}, N) = L$ and

$$0 = s_{n+L} + c_{L-1}s_{n+L-1} + c_{L-2}s_{n+L-2} + \cdots + c_0 s_n$$

$^2$ A comparison of certain binary sequences constructed in a similar way was made in [5].
for all \(0 < n \leq N - L\), where \(c_0, c_1, \ldots, c_{L-1} \in \mathbb{Z}_d\). So

\[
1 = g^0 = g^{n_0 + \ell + nL - 1 + \ell + 2nL - 2 + \cdots + c_0 a},
\]

Let \(\chi \in \hat{\mathbb{F}_p}\) be a multiplicative character of order \(d\). From Eq. (1) it is easy to see that

\[
\chi(g^n) = \chi(i).
\]

We obtain

\[
\chi(1) = \chi(g^{n_0 + \ell + nL - 1 + \ell + 2nL - 2 + \cdots + c_0 a}) = \chi((n + L)(n + L - 1)^{d-1} \cdots n^a).
\]

Hence we have

\[
\sum_{n=1}^{N-L} \chi(1) = \sum_{n=1}^{N-L} \chi((n + L)(n + L - 1)^{d-1} \cdots n^a).
\]

By Lemma 3,

\[
N - L \leq 9(L + 1)p^{1/2} \log(p),
\]

we obtain the desired result. \(\square\)

The bound in Theorem 3 is of the order of magnitude \(O(Np^{-1/2} \log^{-1}(p))\).

4. Sequences related to the Jacobi sequences

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

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

Since \(g\) is a primitive root of both \(p\) and \(q\), by the Chinese Remainder Theorem again

\[
\ord_n(g) = \text{lcm}(\ord_p(g), \ord_q(g)) = \text{lcm}(p - 1, q - 1) = e,
\]

where \(\ord_n(g)\) denotes the multiplicative order of \(g\) modulo \(m\).

The generalized cyclotomic classes of order \(d\) with respect to \(p\) and \(q\) are defined by

\[
D_i = \{g^s x^i | s = 0, 1, \ldots, e - 1\}, \quad i = 0, 1, \ldots, d - 1.
\]

It is easy to see that

\[
Z_n^* = \bigcup_{i=0}^{d-1} D_i, \quad D_i \cap D_j = \emptyset \quad \text{for} \quad i \neq j.
\]

We set

\[
Q = \{q, 2q, \ldots, (p - 1)q\}, \quad Q_0 = Q \cup \{0\}, \quad P = \{p, 2p, \ldots, (q - 1)p\}.
\]

One can define the \(d\)-ary generalized cyclotomic sequence \(\mathcal{R}^\infty = \{r_1, r_2, \ldots\}\) of order \(d\) over \(\mathbb{Z}_d\) with respect to two distinct primes \(p\) and \(q\):

\[
r_i := \begin{cases} 
1, & \text{if } [i \mod n] \in D_l, l = 0, 1, \ldots, d - 1; \\
A, & \text{if } [i \mod n] \in P; \\
B, & \text{if } [i \mod n] \in Q_0,
\end{cases}
\]

for each \(i \geq 1\), where \(A\) and \(B\) are fixed numbers chosen from \(\{0, 1, \ldots, d - 1\}\), each \(D_i\) is defined as in (5). \(\mathcal{R}^\infty\) is periodic with \(n = pq\). The generalized cyclotomic binary sequence \(\mathcal{Y}^\infty = \{v_1, v_2, \ldots\}\) of order \(d\) with respect to the primes \(p\) and \(q\) is defined by

\[
v_i := \begin{cases} 
0, & \text{if } 0 \leq r_i \leq \frac{d}{2} - 1 \text{ or } r_i = B; \\
1, & \text{if } \frac{d}{2} \leq r_i \leq d - 1 \text{ or } r_i = A,
\end{cases}
\]
for all $i \geq 1$. $V^\infty$ is periodic with period $n = pq$. If we suppose

$$C_0 = Q_0 \cup \left( \bigcup_{i=0}^{d-1} D_i \right); \quad C_1 = P \cup \left( \bigcup_{i=0}^{d-1} D_i \right),$$

then we have

$$Z_n = C_0 \cup C_1, \quad C_0 \cap C_1 = \emptyset.$$ 

So the binary sequence $V^\infty = \{v_1, v_2, \ldots\}$ defined as in (7) is equivalent to

$$v_i = \begin{cases} 0, & \text{if } [i \ mod \ n] \in C_0; \\ 1, & \text{if } [i \ mod \ n] \in C_1, \end{cases}$$

(8)

for all $i \geq 1$.

We remark that when $d = 2$, the linear complexity of $V^\infty$ has been determined in [9], when $d = 4$, the linear complexity of $V^\infty$ has been determined in [1].

We also remark that if we define

$$C'_0 = Q_0 \cup \left( \bigcup_{i=0}^{d-1} D_{2i} \right); \quad C'_1 = P \cup \left( \bigcup_{i=0}^{d-1} D_{2i+1} \right)$$

and

$$w_i = \begin{cases} 0, & \text{if } [i \ mod \ n] \in C'_0; \\ 1, & \text{if } [i \ mod \ n] \in C'_1, \end{cases}$$

for all $i \geq 1$, then the sequence $(w_i)$ can be expressed as

$$(-1)^{w_i} = \begin{cases} 1, & \text{if } [i \ mod \ n] \in Q_0; \\ -1, & \text{if } [i \ mod \ n] \in P; \\ \left(\frac{i}{i}\right)_{(q)}, & \text{if } [i \ mod \ n] \in \mathbb{Z}_n^+, \end{cases}$$

The correlation and linear complexity profile of $(w_i)$ have been estimated in [27].

In this section, we always suppose that $d \geq 2$ is even.

### 4.1. Distribution and correlation of $V^\infty$

Let $\mathcal{H} = \{ x \in \mathbb{Z}_p : \chi(g^i) = 1, i = 0, 1, \ldots, e-1 \}$. Obviously $\mathcal{H}$ is a cyclic subgroup of $\mathbb{Z}_n^*$ with $\#\mathcal{H} = d$ by [24, Theorem 5.6]. Let $\mathcal{H}^* = \mathcal{H} \setminus \{0\}$.

From (8) and by Lemma 1 and Remark 1, for any $i \geq 1$ with $\gcd(i, n) = 1$

$$\sum_{j=0}^{d-1} \sum_{g \in \mathcal{H}} \chi(i) \chi(x^j) = \begin{cases} d, & [i \ mod \ n] \in C_0; \\ 0, & [i \ mod \ n] \in C_1. \end{cases}$$

Then we have

$$\sum_{j=0}^{d-1} \sum_{g \in \mathcal{H}^*} \chi(i) \chi(x^j) = \begin{cases} \frac{d}{2}, & [i \ mod \ n] \in C_0; \\ -\frac{d}{2}, & [i \ mod \ n] \in C_1, \end{cases}$$

for any $i \geq 1$ with $\gcd(i, n) = 1$. Hence we obtain

$$(-1)^w = \begin{cases} +1, & \text{if } [i \ mod \ n] \in Q_0; \\ -1, & \text{if } [i \ mod \ n] \in P; \\ \left(\frac{i}{i}\right)_{(q)}, & \text{if } [i \ mod \ n] \in \mathbb{Z}_n^+, \end{cases}$$

(9)
Lemma 4. Let \( g \) and \( x \) be defined as in Section 4 above. Let \( \mathscr{H} = \{ \chi \in \hat{\mathbb{Z}}^*_n | \chi(g^i) = 1, i = 0, 1, \ldots, e - 1 \} \). Then the following bound holds:

\[
\sum_{\chi \in \mathscr{H}} \left| \sum_{j=0}^{d-1} \chi(x^j) \right| < 2d \log(1 + d).
\]

Proof. Each \( \chi \in \mathscr{H} \) is a primitive multiplicative character and it can be expressed as \( \chi = \chi_p \chi_q \), where \( \chi_p \) is a character modulo \( p \) of order \( d_p > 1 \) and \( \chi_q \) is a character modulo \( q \) of order \( d_q > 1 \). By the definitions of \( \mathscr{H} \) and \( x \), we have

\[
\chi(x^j) = \chi_p(x^j) \chi_q(x^j) = \chi_p(g^j).
\]

Hence we obtain

\[
\sum_{\chi \in \mathscr{H}} \left| \sum_{j=0}^{d-1} \chi(x^j) \right| = \sum_{\chi_p \neq \chi_p} \left| \sum_{j=0}^{d-1} \chi_p(x^j) \right| < 2d \log(1 + d). \quad \square
\]

Lemma 5 [28]. Let \( p, q \) be distinct prime numbers and \( f(x) = a_nx^n + \cdots + a_1x + a_0 \in \mathbb{Z}[x] \) and \( a \in \mathbb{Z} \). Let \( \chi \) be a primitive multiplicative character modulo \( pq \) and write \( \chi = \chi_p \chi_q \), where \( \chi_p \) is a character modulo \( p \) of order \( d_p > 1 \) and \( \chi_q \) is a character modulo \( q \) of order \( d_q > 1 \). If \( f(x) \) is not the constant multiple of the \( d_p \)-power of a polynomial in \( \mathbb{F}_p[x] \) and it has \( s_q \) distinct zeros in \( \mathbb{F}_p \), \( f(x) \) is not the constant multiple of the \( d_q \)-power of a polynomial in \( \mathbb{F}_q[x] \) and it has \( s_q \) distinct zeros in \( \mathbb{F}_q \), then

\[
\left| \sum_{i=1}^{pq} \chi(f(i))e_{pq}(ai) \right| \leq s_p s_q p^{1/2} q^{1/2},
\]

and

\[
\left| \sum_{X < i < X + Y} \chi(f(i)) \right| \leq s_p s_q p^{1/2} q^{1/2} (1 + \log(pq)),
\]

where \( X, Y \) are real numbers and \( 0 < Y \leq pq \).

Theorem 4. Let \( n = pq \) and \( \mathcal{V}_n = \{ v_1, v_2, \ldots, v_n \} \) a sequence defined as in (7). Then the well-distribution measure of \( \mathcal{V}_n \) satisfies:

\[
W(\mathcal{V}_n) < 4n^{1/2}(1 + \log(n)) \log(1 + d) + p + q - 1.
\]

Proof. According to Eq. (9), for any \( a, b, t \in \mathbb{N} \) with \( 1 \leq a \leq a + (t - 1)b \leq n \), we have at most \( \delta = p + q - 1 \) elements \( i(0 \leq i \leq t - 1) \) with \( a + ib \in P \cup Q_0 \). Hence, we get

\[
\left| \sum_{i=0}^{t} (-1)^{v_n+i} \right| \leq \left| \sum_{i=0}^{t} (-1)^{v_n+i} \right| + \delta = \frac{2}{d} \left| \sum_{\chi \in \mathscr{H}} \sum_{j=0}^{q-1} \chi(x^j) \right| + \delta
\]

\[
= \frac{2}{d} \left| \sum_{\chi \in \mathscr{H}} \chi(x^j) \sum_{i=0}^{t-1} \chi(a + ib) \chi(x^i) \right| + \delta \leq \frac{2}{d} \sum_{\chi \in \mathscr{H}} \left| \sum_{i=0}^{q-1} \chi(x^i) \right| \left| \sum_{j=0}^{q-1} \chi(a + ib) \right| + \delta
\]

\[
\leq 4n^{1/2}(1 + \log(n)) \log(1 + d) + \delta.
\]

The last inequality follows from Lemmas 4 and 5. \( \square \)
Theorem 5. Let \( n = pq \) and \( \mathcal{Y}_n = \{v_1, v_2, \ldots, v_n\} \) a sequence defined as in (7). Then the correlation measure of order \( k \) of \( \mathcal{Y}_n \) holds:

\[
C_k(\mathcal{Y}_n) < 4k^2 n^{1/2} \log(1 + d)(1 + \log(n)) + k(p + q - 1).
\]

Proof. According to Eq. (9), for integers \( D = (d_1, \ldots, d_k) \) and \( M \) with \( 0 \leq d_1 < \cdots < d_k \leq n - M \), there are at most \( k\delta \), where \( \delta = p + q - 1 \), elements \( m(1 \leq m \leq M < n) \) such that at least one number \( m + d_j \in P \cup Q_0 \), where \( 1 \leq j \leq k \). Hence, we get

\[
\left| \sum_{m=1}^{M} (-1)^{a_m+d_1+a_m+d_2+\cdots+a_m+d_k} \right| \leq \left| \sum_{m \in P} (-1)^{a_m+d_1+a_m+d_2+\cdots+a_m+d_k} \right| + k\delta
\]

\[
= 2k^2 \delta \left[ \sum_{j=1}^{k} \prod_{i=1}^{n} \left( \sum_{x \in \mathcal{H}} \mathcal{Z}(m + d_j)(x^i) \right) \right] + k\delta
\]

\[
= 2k^2 \delta \left[ \sum_{j=1}^{k} \left( \sum_{x_j \in \mathcal{H}} \mathcal{Z}_1(x^{i_1}) \cdots \sum_{x_k \in \mathcal{H}} \mathcal{Z}_k(x^{i_k}) \right) \sum_{m=1}^{M} \mathcal{Z}_j(m + d_j) \right] + k\delta
\]

Since \( \mathcal{H} \) is a cyclic subgroup of \( \mathbb{Z}_n^* \) with \( \#\mathcal{H} = d \), let \( \phi \) be a generator of \( \mathcal{H} \), i.e., the order of \( \phi \) is \( d \). Then for each \( \mathcal{Z}_j, 1 \leq j \leq k \), there exists an integer \( x_j \in [1, d - 1] \) such that \( \mathcal{Z}_j = \phi^{x_j} \). So by Lemma 5 we obtain

\[
\left| \sum_{m=1}^{M} \prod_{j=1}^{k} \mathcal{Z}_j(m + d_j) \right| = \left| \sum_{m=1}^{M} \prod_{j=1}^{k} \phi^{x_j}(m + d_j) \right| = \left| \sum_{m=1}^{M} \phi((m + d_1)^{x_1} \cdots (m + d_k)^{x_k}) \right| \leq k^2 n^{1/2}(1 + \log(n)).
\]

Hence

\[
(\ast\ast) \leq \frac{2k^2}{d^k} \cdot k^2 n^{1/2}(1 + \log(n)) \cdot \left[ \sum_{j=1}^{k} \sum_{x_j \in \mathcal{H}} \mathcal{Z}_1(x^{i_1}) \cdots \sum_{x_k \in \mathcal{H}} \mathcal{Z}_k(x^{i_k}) \right] + k\delta
\]

\[
\leq \frac{2k^2}{d^k} \cdot k^2 n^{1/2}(1 + \log(n)) \cdot \left[ \prod_{j=1}^{k} \sum_{x_j \in \mathcal{H}} \mathcal{Z}_j(x^{i_j}) \right] + k\delta
\]

\[
\leq \frac{2k^2}{d^k} \cdot k^2 n^{1/2}(1 + \log(n)) \cdot \left[ \prod_{j=1}^{k} \sum_{x_j \in \mathcal{H}} \mathcal{Z}_j(x^{i_j}) \right] + k\delta
\]

Using the bound in Lemma 4, we obtain the desired result. \( \square \)

In the most interesting case, when \( |p - q| \) is small (e.g., when \( p \) and \( q \) are twin primes), the bound in Theorem 4 is of order of \( O(n^{1/2} \log(n) \log(d)) \), the bound in Theorem 5 is of order of \( O(n^{1/2} \log(n) \log^2(d)) \).

Remark 2. In [2], the generalized cyclotomic classes of order two (i.e., \( d = 2 \)) are defined by

\[
D_0 = \{ g^{2^i}, g^{2^i}x | s = 0, 1, \ldots, (e - 2)/2 \},
\]

\[
D_1 = \{ g^{2^i+1}, g^{2^i+1}x | s = 0, 1, \ldots, (e - 2)/2 \}.
\]

And the generalized cyclotomic sequence \( (s_i) \) of order two with length \( pq \) is defined by

\[
s_i = \begin{cases} 
0, & [i \mod n] \in D_0; \\
1, & [i \mod n] \in D_1,
\end{cases}
\]
for any $i \in \mathbb{Z}_{pq}$ ($s_i$ is also defined when $i|p$ or $i|q$ in [2]). It is easy to see that for any $i \in \mathbb{Z}_{pq}$,

$$(-1)^i = \left(\frac{i}{q}\right),$$

where $-$ is the Legendre symbol. It indicates that the sequence $(s_i)$ has large autocorrelation for some values, hence it lacks of use although it possesses large linear complexity.

4.2. Linear complexity profile of $\mathcal{R}^\infty$

**Theorem 6.** The $d$-ary generalized cyclotomic sequence $\mathcal{R}^\infty = \{r_1, r_2, \ldots\}$ of order $d$ is defined as in (6). The linear complexity profile $L(\mathcal{R}^\infty, N)$ satisfies

$$L(\mathcal{R}^\infty, N) \geq \sqrt{\frac{(p+q)^2}{4n(1+\log(n))^2}} + \frac{N+1}{n^{1/2}(1+\log(n))} - \frac{p+q}{2n^{1/2}(1+\log(n))} - 1$$

for $1 \leq N < n$.

**Proof.** The proof is similar to that of Theorem 3. Let $L(\mathcal{R}^\infty, N) = L$ and

$$0 = r_{i+1} + c_{i-L}r_{i+L-1} + c_{i-2L}r_{i+2L-2} + \cdots + c_0r_i$$

for all $1 \leq i \leq N - L$, where $c_0, c_1, \ldots, c_{L-1} \in \mathbb{Z}_d$.

We note that at least $N - L - (L+1)(p+q-1)$ many $i \in \{1, 2, \ldots, N - L\}$ satisfy $i + l \in \mathbb{Z}_n^*$ for all $l = 0, \ldots, L$.

For such $i$ and each $\chi \neq 0$ in $\mathcal{R} = \{\chi \in \mathbb{Z}_n^*; |\chi| = 1, i = 0, 1, \ldots, e - 1\}$, we obtain

$$1 = \chi(x^0) = \chi(x^{r_{i+1}} + c_{i-L}r_{i+L-1} + c_{i-2L}r_{i+2L-2} + \cdots + c_0r_i) = \chi((i+L)(i+L-1)^{c_{1}} \cdots r_0).$$

Hence we have

$$\sum_{i=1}^{N-L}(i+L)(i+L-1)^{c_{1}} \cdots r_0 \geq N - L - (L + 1)(p + q - 1).$$

By Lemma 5, we get

$$N - L - (L + 1)(p + q - 1) \leq (L + 1)^2n^{1/2}(1 + \log(n)).$$

After some simple computation we obtain the desired result. \qed

The bound in Theorem 6 is of the order of magnitude $O(N^{1/2}n^{-1/4}\log^{-1/2}(n))$ in the case when $|p - q|$ is small.

5. Conclusions

Using cyclotomic classes and generalized cyclotomic classes of order $d$, we have constructed two families of binary sequences with strong pseudo-random properties. That is, we estimate the upper bounds of two important pseudorandom measures, the well-distribution measure and the correlation measure of order $k$, which is very close to that of “truely” random sequences.

In [28] three families of binary sequences are constructed in different ways with respect to the primes $p$ and $q$, which are extensions of the constructions over $\mathbb{F}_p$. It seems that the binary sequence $Y^\infty = \{v_1, v_2, \ldots\}$ derived from generalized cyclotomic classes with respect to the primes $p$ and $q$ in Section 4 is somewhat superior to those sequences in [28], since the order $k$ correlation measure of those sequences in [28] is large for some special small values $k$.

For $d$-ary cyclotomic sequences and $d$-ary generalized cyclotomic sequences, we have also estimated a lower bound on the linear complexity profile respectively, which is an important cryptographic characteristic of pseudo-random sequences.
Acknowledgements

This work was supported by the National Natural Science Foundation of China (No. 60473028). The research of the first author was also supported in part by the Natural Science Foundation of Fujian Province of China (No. A0540011) and the Science and Technology Foundation of Putian City (No. 2005S04).

The authors wish to thank the anonymous referees for their detailed and very helpful comments and suggestions that improved this article.

References