Chen ZX, Du XN, Wu CH. Pseudo-randomness of certain sequences of k symbols with length pq. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 26(2): 276–282 Mar. 2011. DOI 10.1007/s11390-011-1130-y

Pseudo-Randomness of Certain Sequences of k Symbols with Length pq

Zhi-Xiong Chen[1,2] (陈智雄), *Member*, *CCF*, Xiao-Ni Du[2,3,*] (杜小妮)
and Chen-Huang Wu[1] (吴晨煌), *Member*, *CCF*

[1] *Department of Mathematics, Putian University, Putian 351100, China*

[2] *State Key Lab. of ISN, Xidian University, Xi'an 710071, China*

[3] *College of Mathematics and Information Science, Northwest Normal University, Lanzhou 30070, China*

E-mail: {ptczx, ymldxn, wuchenhuang2008}@126.com

Received March 24, 2010; revised November 25, 2010.

Abstract The theory of finite pseudo-random binary sequences was built by C. Mauduit and A. Sárközy and later extended to sequences of k symbols (or k-ary sequences). Certain constructions of pseudo-random sequences of k symbols were presented over finite fields in the literature. In this paper, two families of sequences of k symbols are constructed by using the integers modulo pq for distinct odd primes p and q. The upper bounds on the well-distribution measure and the correlation measure of the families sequences are presented in terms of certain character sums over modulo pq residue class rings. And low bounds on the linear complexity profile are also estimated.

Keywords stream ciphers, pseudo-random sequences, well-distribution measure, correlation measure, discrete logarithm, modulo pq residue class rings, character sums

1 Introduction

In a series of papers starting from [1], Mauduit and Sárközy (partly with further coauthors) introduced certain measures of pseudo-randomness and studied finite binary pseudo-random sequences. For a finite binary sequence of length N

$$E_N = \{e_1, \ldots, e_N\} \in \{-1, +1\}^N.$$

The *well-distribution measure* of E_N is defined by

$$W(E_N) = \max_{a,b,t} \Big| \sum_{j=0}^{t-1} e_{a+bj} \Big|,$$

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

$$C_\ell(E_N) = \max_{M,D} \Big| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_\ell} \Big|,$$

where the maximum is taken over all $D = (d_1, \ldots, d_\ell)$ and M such that $0 \leqslant d_1 < \cdots < d_\ell \leqslant N - M$.

It was shown in [2] that for a "truly" random binary sequence E_N both pseudo-random measures $W(E_N)$ and $C_\ell(E_N)$ are "small". More precisely, the order of magnitude of $W(E_N)$ and $C_\ell(E_N)$ (for fixed ℓ) is $N^{1/2}$ and $N^{1/2}(\log N)^{c(\ell)}$ for some fixed value $c(\ell)$, respectively.

In [3] this theory was extended to sequences of k symbols (or k-ary sequences) and further studied in [4-6]. In particular, very recently the theory of pseudo-random lattices of k symbols was built in [7]. There are two different ways of extension which are shown to be "nearly equivalent"[3]. The following one is more suitable for our purpose.

Let $k \in \mathbb{N}$, $k \geqslant 2$, and let $\mathcal{A} = \{\beta_1, \beta_2, \ldots, \beta_k\}$ be a finite set of k symbols. Let

$$E_N = \{e_1, e_2, \ldots, e_N\} \in \mathcal{A}^N$$

be a sequence of these symbols of length N. Write

$$x(E_N, a, M, u, v) = \#\{j | 0 \leqslant j \leqslant M-1, e_{u+jv} = a\}$$

Short Paper

The work was partially supported by the National Natural Science Foundation of China under Grant No. 61063041, the Program for New Century Excellent Talents of Universities in Fujian Province under Grant No. JK2010047 and the Funds of the Education Department of Gansu Province under Grant No. 1001-09.

*Corresponding Author

for $a \in \mathcal{A}$ and

$$g(E_N, w, M, D) = \#\{n | 1 \leqslant n \leqslant M, (e_{n+d_1}, \ldots, e_{n+d_\ell}) = w\}$$

for $w = (a_1, \ldots, a_\ell) \in \mathcal{A}^\ell$ and $D = (d_1, \ldots, d_\ell)$ with non-negative integers $d_1 < \cdots < d_\ell$. Then following [3], the *well-distribution measure* (more precisely, the f-well-distribution measure in [3], where "f" for frequency) of E_N is defined as

$$\delta(E_N) = \max_{a,M,u,v} \left| x(E_N, a, M, u, v) - \frac{M}{k} \right|,$$

where the maximum is taken over all $a \in \mathcal{A}$ and positive M, u, v with $u + (M-1)v \leqslant N$. Let

$$\gamma_\ell(E_N, D) = \max_{w,M} \left| g(E_N, w, M, D) - \frac{M}{k^\ell} \right|,$$

where the maximum is taken over all $w \in \mathcal{A}^\ell$ and M such that $M + d_\ell \leqslant N$, then the *correlation measure of order* ℓ (i.e., the f-correlation measure of order ℓ in [3]) of E_N is defined as

$$\gamma_\ell(E_N) = \max_D \gamma_\ell(E_N, D),$$

where the maximum is taken over all $D = (d_1, \ldots, d_\ell)$.

It is expected that both $\delta(E_N)$ and $\gamma_\ell(E_N)$ (at least for small ℓ) are "small" in terms of N (in particular, both are $o(N)$ as $N \to \infty$, and ideally it is $N^{1/2+\varepsilon}$). And E_N is considered as a "good" pseudo-random sequence if both $\delta(E_N)$ and $\gamma_\ell(E_N)$ are "small".

Certain construction of "good" sequences $E_p = \{e_1, e_2, \ldots, e_p\}$ of k symbols was defined in [3] using a multiplicative character χ of order k (k is a divisor of $p-1$) of finite fields $\mathbb{Z}_p$ by

$$e_n = \begin{cases} \chi(n), & \text{if } (n,p) = 1, \\ 1, & \text{otherwise,} \end{cases} \qquad n = 1, 2, \ldots.$$

Such a sequence satisfies

$$\delta(E_p) \ll p^{1/2} \log p, \quad \gamma_\ell(E_p) \ll \ell k p^{1/2} \log p$$

for $\ell < p$. This construction was extended in [4-5] using polynomials $f(x) \in \mathbb{Z}_p[x]$ with no multiple zeros.

For the purpose of applications, it is a natural idea to construct other families of pseudo-random sequences of k symbols. In this article, we will present new constructions of pseudo-random sequences of k symbols using $\mathbb{Z}_{pq}$, the residue class ring modulo pq.

Throughout this paper, the implied constant in the symbol "$\ll$" is absolute. We recall that the notation $U \ll V$ is equivalent to the assertion that the inequality $|U| \leqslant cV$ holds for some constant $c > 0$. The notation $\#C$ denotes the cardinality of the set C.

2 Sequences of k Symbols

2.1 Constructions

Throughout this paper, let $N = pq$, where p and q are two distinct odd primes satisfying "RSA type"[8] with

$$2 < p < q < 2p.$$

Let $d = \gcd(p-1, q-1)$ and $e = \mathrm{lcm}(p-1, q-1)$. By the Chinese Remainder Theorem there exists a common primitive root g of both p and q. In fact, suppose that a is a primitive root modulo p, and b is a primitive root modulo q, then we get the common primitive root

$$g \equiv qi_q a + pi_p b \pmod{pq},$$

where $qi_q \equiv 1 \bmod p$ and $pi_p \equiv 1 \bmod q$. For example, $g = 5$ for $p = 3$ and $q = 7$. There also exists an integer ω satisfying

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

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

$$\begin{aligned} ord_N(g) &= \mathrm{lcm}(ord_p(g), ord_q(g)) \\ &= \mathrm{lcm}(p-1, q-1) = e \end{aligned}$$

where $ord_m(g)$ denotes the multiplicative order of g modulo m.

In $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$, the residue class ring modulo N, the (Whiteman) generalized cyclotomic classes of order d are defined by

$$D_i = \{g^s \omega^i | s = 0, 1, \ldots, e-1\}, \ i = 0, 1, \ldots, d-1.$$

It is easy to see that

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

We set

$$\begin{aligned} &Q = \{q, 2q, \ldots, (p-1)q\}, \quad Q_0 = Q \cup \{0\}, \\ &P = \{p, 2p, \ldots, (q-1)p\}. \end{aligned}$$

The (Whiteman) generalized cyclotomic classes were applied to constructing binary sequences in numerous references, see, e.g., [8-15]. In this article, we will extend the constructions of binary sequences to sequences of k symbols.

Let k be a positive integer. From now on, we always suppose $\mathcal{A} = \mathbb{Z}_k = \{0, 1, \ldots, k-1\}$. We define the first family of sequences of k symbols using generalized cyclotomic classes above.

Definition 1. $E_N^{(1)} = \{e_1^{(1)}, e_2^{(1)}, \ldots, e_N^{(1)}\} \in \mathbb{Z}_k^N$ *is defined by*

$$e_n^{(1)} = \begin{cases} j \pmod k, & \text{if } n \in D_j,\ 0 \leqslant j < d, \\ A, & \text{if } n \in P, \\ B, & \text{if } n \in Q_0, \end{cases}$$

for $n = 0, 1, \ldots, N-1$ *and fixed elements* $A, B \in \mathbb{Z}_k$.

We remark that if $k = 2$, $E_N^{(1)}$ is the Jacobi sequence, whose properties were studied by Rivat and Sárközy[8].

Let $ind_p(x)$ denote the index (discrete logarithm) of x (to the base g) so that

$$g^{ind_p(x)} \equiv x \pmod p.$$

We add the condition

$$1 \leqslant ind_p(x) \leqslant p-1$$

to make the value of index unique. Similarly, one can define $ind_q(x) \in [1, q-1]$. Then we define the second family of sequences of k symbols.

Definition 2. $E_N^{(2)} = \{e_1^{(2)}, e_2^{(2)}, \ldots, e_N^{(2)}\} \in \mathbb{Z}_k^N$ *is defined by*

$$e_n^{(2)} = \begin{cases} ind_p(n) + ind_q(n) \pmod k, & \text{if } n \in \mathbb{Z}_N^*, \\ A, & \text{if } n \in P, \\ B, & \text{if} n \in Q_0, \end{cases}$$

for $n = 0, 1, \ldots, N-1$ *and fixed elements* $A, B \in \mathbb{Z}_k$.

Some related sequences are studied in [16-17], mainly concentrating on the properties of linear complexity, see, e.g., [18] for the notion.

2.2 Pseudo-Randomness

In this subsection, we consider the well-distribution measure and correlation measure of $E_N^{(1)}$ and $E_N^{(2)}$, respectively. The theory of character sums plays an important role in our proofs.

For any positive integer $m > 1$, we identify $\mathbb{Z}_m$, the residue ring modulo m, with the set $\{0, 1, \ldots, m-1\}$. $\mathbb{Z}_m^* = \{x \in \mathbb{Z}_m | \gcd(x, m) = 1\}$ is a group under integer multiplication modulo m. 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 $\chi_0 = 1$. We denote by $\widehat{\mathbb{Z}_m^*}$ the set of all multiplicative characters of $\mathbb{Z}_m^*$. It is easy to see that $\widehat{\mathbb{Z}_m^*}$ forms a group with the principal character χ_0 as the neutral element under the multiplication of characters.

For convenience, we extend χ to $\mathbb{Z}_m$ only by defining $\chi(x) = 0$ for x with $\gcd(x, m) > 1$.

Lemma 1[19]. *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 $\chi \in \widehat{\mathbb{Z}_m^*}$,

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

We remark that $\mathbb{Z}_m^*$ 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.

It is obvious that when $m = pq$ (p, q are distinct prime numbers), for each $\chi \in \widehat{\mathbb{Z}_m^*}$, there exist $\chi_p \in \widehat{\mathbb{Z}_p^*}$ and $\chi_q \in \widehat{\mathbb{Z}_q^*}$ such that

$$\chi(x) = \chi_p(x)\chi_q(x), \quad x \in \mathbb{Z}_m^*.$$

Lemma 2[8]. *Let* p, q *be distinct odd prime numbers and* $h(x) = h_l x^l + \cdots + h_1 x + h_0 \in \mathbb{Z}[x]$ *and* $a \in \mathbb{Z}$. *Let* χ *be a primitive multiplicative character modulo* pq *and write* $\chi = \chi_p \chi_q$, *where* χ_p *is a character modulo* p *of order* $t_p > 1$ *and* χ_q *is a character modulo* q *of order* $t_q > 1$. *Let* X, Y *be real numbers with* $0 < Y \leqslant pq$.

(i) If $h(x)$, *as a polynomial in* $\mathbb{F}_p[x]$, *is not a constant multiple of a* t_p*-th power of a polynomial in* $\mathbb{F}_p[x]$ *and it has* s_p *distinct zeros in* $\overline{\mathbb{F}}_p$, *then*

$$\Big| \sum_{x=1}^{pq} \chi(h(x)) e_{pq}(ax) \Big| \leqslant s_p p^{1/2} q$$

and

$$\Big| \sum_{X < x \leqslant X+Y} \chi(h(x)) \Big| \leqslant s_p p^{1/2} q (1 + \log(pq)).$$

Similar results hold if we interchange the roles of p *and* q *with corresponding parameters* t_q *and* s_q.

(ii) If conditions of (i) hold for both p *and* q, *then we have*

$$\Big| \sum_{x=1}^{pq} \chi(h(x)) e_{pq}(ax) \Big| \leqslant s_p s_q p^{1/2} q^{1/2}$$

and

$$\Big| \sum_{X < x \leqslant X+Y} \chi(h(x)) \Big| \leqslant s_p s_q p^{1/2} q^{1/2} (1 + \log(pq)).$$

Theorem 1. *Suppose $k > 1$ and $k|d$ for $d = \gcd(p-1, q-1)$. Then the well-distribution measure of $E_N^{(1)}$ defined in Definition 1 satisfies*

$$\delta(E_N^{(1)}) \ll N^{1/2} \log N.$$

Proof. Let

$$\mathcal{H} = \{\chi^{d/k} : \chi \in \widehat{\mathbb{Z}_N^*}, \quad \chi(g^i) = 1, \quad 0 \leqslant i < e\}.$$

Obviously $\mathcal{H}$ is a cyclic subgroup of $\widehat{\mathbb{Z}_N^*}$ with $\#\mathcal{H} = k$ by Theorem 5.6 of [19]. Let $\mathcal{H}^* = \mathcal{H} \setminus \{\chi_0\}$. Each $\chi \in \mathcal{H}^*$ is a primitive multiplicative character.

Let ω be defined as in Subsection 2.1. According to the definition of $E_N^{(1)}$, we see that

$$e_n^{(1)} \equiv j \pmod k \Leftrightarrow n \in D_j \Leftrightarrow \chi(n\omega^{-j}) = 1$$

for $n \in \mathbb{Z}_N^*$ and $\chi \in \mathcal{H}^*$.

For all $a \in \mathbb{Z}_k$ and positive integers M, u, v with $1 \leqslant u + (M-1)v \leqslant N$, we use Lemma 1 to represent the following equation

$$\begin{aligned}
&x(E_N^{(1)}, a, M, u, v)\\
&= \#\{j | 0 \leqslant j \leqslant M-1, e_{u+jv}^{(1)} = a\}\\
&\leqslant \sum_{\substack{0\leqslant j\leqslant M-1\\ u+jv\in\mathbb{Z}_N^*}} \frac{1}{k}\sum_{\chi\in\mathcal{H}} \chi((u+jv)\omega^{-a}) + \sum_{\substack{0\leqslant j\leqslant M-1\\ u+jv\in P\cup Q_0}} 1\\
&= \frac{1}{k}\sum_{\chi\in\mathcal{H}} \chi(\omega^{-a}) \sum_{\substack{0\leqslant j\leqslant M-1\\ u+jv\in\mathbb{Z}_N^*}} \chi(u+jv) + (p+q-1)\\
&\leqslant \frac{M}{k} + \frac{1}{k}\sum_{\chi\in\mathcal{H}^*} \chi(\omega^{-a}) \sum_{\substack{0\leqslant j\leqslant M-1\\ u+jv\in\mathbb{Z}_N^*}} \chi(u+jv) + (p+q-1).
\end{aligned}$$

And hence we derive

$$\begin{aligned}
&\Big|x(E_N^{(1)}, a, M, u, v) - \frac{M}{k}\Big|\\
&\leqslant \frac{1}{k}\Big|\sum_{\chi\in\mathcal{H}^*} \chi(\omega^{-a}) \sum_{\substack{0\leqslant j\leqslant M-1\\ u+jv\in\mathbb{Z}_N^*}} \chi(u+jv)\Big| + (p+q-1)\\
&\leqslant \frac{1}{k}\sum_{\chi\in\mathcal{H}^*} \Big|\sum_{\substack{0\leqslant j\leqslant M-1\\ u+jv\in\mathbb{Z}_N^*}} \chi(u+jv)\Big| + (p+q-1)\\
&\leqslant (p+q-1) + \begin{cases} p, & \text{if } q|v,\\ q, & \text{if } p|v,\\ N^{1/2}(1+\log N), & \text{if } v \in \mathbb{Z}_N^*. \end{cases}
\end{aligned}$$

The last inequality follows from Lemma 2. Together with the restriction on p, q of "RSA" type, we complete the proof. □

Theorem 2. *Suppose $k > 1$ and $k|d$ for $d = \gcd(p-1, q-1)$ and $D = (d_1, \ldots, d_\ell)$ with $\ell < N$ and $0 \leqslant d_1 < \cdots < d_\ell < N$.*

(i) If $d_1 \equiv d_2 \equiv \cdots \equiv d_\ell \pmod p$ or $d_1 \equiv d_2 \equiv \cdots \equiv d_\ell \pmod q$, we have

$$\gamma_\ell(E_N^{(1)}, D) \ll \ell N^{3/4} \log N.$$

(ii) If $d_i \not\equiv d_j \pmod p$ and $d_i \not\equiv d_j \pmod q$ for all $1 \leqslant i, j \leqslant \ell$ and $i \neq j$, we have

$$\gamma_\ell(E_N^{(1)}, D) \ll \ell^2 N^{1/2} \log N.$$

In particular, the correlation measure of order 2 of $E_N^{(1)}$ satisfies

$$\gamma_2(E_N^{(1)}) \ll N^{3/4} \log N.$$

Proof. For all $w = (a_1, \ldots, a_\ell) \in \mathbb{Z}_k^\ell$, and $D = (d_1, \ldots, d_\ell)$ and M such that $d_1 < d_2 < \cdots < d_\ell$ and $M + d_\ell \leqslant N$, there are at most $\ell(p+q-1)$ many $n \in \mathbb{Z}_N$ such that $n + d_i \notin \mathbb{Z}_N^*$ for all $1 \leqslant i \leqslant \ell$. So we have

$$\begin{aligned}
&g(E_N^{(1)}, w, M, D)\\
&= \#\{m | 1 \leqslant m \leqslant M, (e_{m+d_1}^{(1)}, \ldots, e_{m+d_\ell}^{(1)}) = w\}\\
&\leqslant \sum_{m=1}^{M} \prod_{\substack{j=1\\ m+d_j\in\mathbb{Z}_N^*}}^{\ell} \Big(\frac{1}{k}\sum_{\chi\in\mathcal{H}} \chi((m+d_j)\omega^{-a_j})\Big) +\\
&\quad \ell(p+q-1)\\
&\leqslant \frac{1}{k^\ell}\sum_{m=1}^{M} \sum_{\chi_1,\ldots,\chi_\ell\in\mathcal{H}} \prod_{\substack{j=1\\ m+d_j\in\mathbb{Z}_N^*}}^{\ell} \chi_j((m+d_j)\omega^{-a_j}) +\\
&\quad \ell(p+q-1)\\
&\leqslant \frac{M}{k^\ell} + \frac{1}{k^\ell}\sum_{m=1}^{M} \sum_{\substack{\chi_1,\ldots,\chi_\ell\in\mathcal{H}\\ (\chi_1,\ldots,\chi_\ell)\neq\{\chi_0\}^\ell}} \cdot\\
&\qquad \prod_{\substack{j=1\\ m+d_j\in\mathbb{Z}_N^*}}^{\ell} \chi_j((m+d_j)\omega^{-a_j}) + \ell(p+q-1).
\end{aligned}$$

Since $\mathcal{H}$ is a cyclic group of order k, let ψ be a generator of $\mathcal{H}$. All $\chi_j \in \mathcal{H}$ can be written as $\chi_j = \psi^{\alpha_j}$ for some integer $0 \leqslant \alpha_j \leqslant k-1$. Then we derive

$$\begin{aligned}
&\Big|g(E_N^{(1)}, w, M, D) - \frac{M}{k^\ell}\Big|\\
&\leqslant \ell(p+q-1) + \frac{1}{k^\ell} \sum_{\substack{0\leqslant\alpha_1,\ldots,\alpha_\ell\leqslant k-1\\ (\alpha_1,\ldots,\alpha_\ell)\neq\underline{0}}} \cdot\\
&\qquad \Big|\sum_{\substack{m=1\\ m+d_j\in\mathbb{Z}_N^*}}^{M} \psi((m+d_1)^{\alpha_1}\cdots(m+d_\ell)^{\alpha_\ell})\Big|.
\end{aligned}$$

Let $F(x) = (x+d_1)^{\alpha_1}\cdots(x+d_\ell)^{\alpha_\ell}$. If $d_1 \equiv d_2 \equiv \cdots \equiv d_\ell \pmod p$, then $d_i \not\equiv d_j \pmod q$ for all $1 \leqslant i, j \leqslant \ell$ and $i \neq j$, and hence $F(x)$, as a polynomial in $\mathbb{Z}_q[x]$, is

not a constant multiple of a k-th power of a polynomial in $\mathbb{Z}_q[x]$. So by Lemma 2, we have

$$\begin{aligned}\gamma_\ell(E_N^{(1)}, D) &\leqslant \ell pq^{1/2}(1+\log N) + \ell(p+q-1)\\ &\ll \ell N^{3/4}\log N.\end{aligned}$$

Similarly, if $d_1 \equiv d_2 \equiv \cdots \equiv d_\ell \pmod q$, we have

$$\begin{aligned}\gamma_\ell(E_N^{(1)}, D) &\leqslant \ell qp^{1/2}(1+\log N) + \ell(p+q-1)\\ &\ll \ell N^{3/4}\log N.\end{aligned}$$

And if $d_i \not\equiv d_j \pmod p$ and $d_i \not\equiv d_j \pmod q$ for all $1 \leqslant i, j \leqslant \ell$ and $i \neq j$, we see that $F(x)$ is not a constant multiple of a k-th power of a polynomial neither in $\mathbb{Z}_p[x]$ nor in $\mathbb{Z}_q[x]$. So we have

$$\begin{aligned}\gamma_\ell(E_N^{(1)}, D) &\leqslant \ell^2 N^{1/2}(1+\log N) + \ell(p+q-1)\\ &\ll \ell^2 N^{1/2}\log N.\end{aligned}$$

We complete the proof. □

Theorem 3. *Suppose $k > 1$ and $k|d$ for $d = \gcd(p-1, q-1)$. Then the well-distribution measure of $E_N^{(2)}$ defined in Definition 2 satisfies*

$$\delta(E_N^{(2)}) \ll N^{1/2}\log N.$$

Proof. We write $\boldsymbol{e}(z) = e^{2\pi\sqrt{-1}z} \in \mathbb{C}$ for real z and $\boldsymbol{e}_k(z) = \boldsymbol{e}(z/k)$. Let

$$\chi_p(x) = \boldsymbol{e}_k(ind_p(x))$$

for $x \in \mathbb{Z}_p^*$ and

$$\chi_q(x) = \boldsymbol{e}_k(ind_q(x))$$

for $x \in \mathbb{F}_q^*$. It is easy to see that χ_p (resp. χ_q) is a multiplicative character modulo p (resp. q) of order k. Let

$$\phi = \chi_p\chi_q,$$

i.e., ϕ is a multiplicative character modulo N of order k. Then for $n \in \mathbb{Z}_N^*$ we have

$$\begin{aligned}\boldsymbol{e}_k(\lambda \cdot e_n^{(2)}) &= \boldsymbol{e}_k(\lambda \cdot (ind_p(n) + ind_q(n)))\\ &= \boldsymbol{e}_k(\lambda \cdot ind_p(n)) \cdot \boldsymbol{e}_k(\lambda \cdot ind_q(n))\\ &= \chi_p^\lambda(n)\chi_q^\lambda(n) = (\chi_p\chi_q)(n^\lambda)\\ &= \phi(n^\lambda),\end{aligned}$$

where $\lambda \in \mathbb{Z}_k$.

The proof is similar to that of Theorem 1. We will use ϕ here instead of χ in Theorem 1. Below we present the main skeleton. For all $a \in \mathbb{Z}_k$ and positive integers M, u, v with $1 \leqslant u + (M-1)v \leqslant N$, we get

$$\begin{aligned}&x(E_N^{(2)}, a, M, u, v)\\ &\leqslant \sum_{\substack{0\leqslant j\leqslant M-1\\ u+jv\in\mathbb{Z}_N^*}} \frac{1}{k}\sum_{\lambda=0}^{k-1} \boldsymbol{e}_k(\lambda(e_{u+jv}^{(2)} - a)) + \sum_{\substack{0\leqslant j\leqslant M-1\\ u+jv\in P\cup Q_0}} 1\\ &\leqslant \frac{M}{k} + \frac{1}{k}\sum_{\lambda=1}^{k-1} \boldsymbol{e}_k(-\lambda a)\cdot\\ &\quad \sum_{\substack{0\leqslant j\leqslant M-1\\ u+jv\in\mathbb{Z}_N^*}} \phi((u+jv)^\lambda) + (p+q-1).\end{aligned}$$

Hence we derive

$$\begin{aligned}&\Big|x(E_N^{(2)}, a, M, u, v) - \frac{M}{k}\Big|\\ &\leqslant \frac{1}{k}\sum_{\lambda=1}^{k-1}\Big|\sum_{\substack{0\leqslant j\leqslant M-1\\ u+jv\in\mathbb{Z}_N^*}} \phi((u+jv)^\lambda)\Big| + (p+q-1)\\ &\leqslant (p+q-1) + \begin{cases} p, & \text{if } q|v,\\ q, & \text{if } p|v,\\ N^{1/2}(1+\log N), & \text{if } v \in \mathbb{Z}_N^*,\end{cases}\end{aligned}$$

which completes the proof. □

Theorem 4. *Suppose $k > 1$ and $k|d$ for $d = \gcd(p-1, q-1)$ and $D = (d_1, \ldots, d_\ell)$ with $\ell < N$ and $0 \leqslant d_1 < \cdots < d_\ell < N$.*

(i) If $d_1 \equiv d_2 \equiv \cdots \equiv d_\ell \pmod p$ or $d_1 \equiv d_2 \equiv \cdots \equiv d_\ell \pmod q$ we have

$$\gamma_\ell(E_N^{(2)}, D) \ll \ell N^{3/4}\log N.$$

(ii) If $d_i \not\equiv d_j \pmod p$ and $d_i \not\equiv d_j \pmod q$ for all $1 \leqslant i, j \leqslant \ell$ and $i \neq j$, we have

$$\gamma_\ell(E_N^{(2)}, D) \ll \ell^2 N^{1/2}\log N.$$

In particular, the correlation measure of order 2 of $E_N^{(2)}$ satisfies

$$\gamma_2(E_N^{(2)}) \ll N^{3/4}\log N.$$

Proof. Using the multiplicative character ϕ, we will get the result after following a similar path of the proof of Theorem 2. □

2.3 Linear Complexity Profile

We recall that the *linear complexity profile* of a sequence $S = \{s_1, s_2, \ldots\}$ over the ring $\mathbb{Z}_k$ is the function $L(S, M)$ defined for every positive integer M, as the least order L of a linear recurrence relation over $\mathbb{Z}_k$

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

for all $L+1 \leqslant n \leqslant M$, which S satisfies. The value

$$L(S) = \sup_{M\geqslant 1} L(S, M)$$

is called the *linear complexity* of the sequence S. For the linear complexity of any periodic sequence of period T one easily verifies that $L(S) = L(S, 2T) \leqslant T$. Linear complexity and linear complexity profile are important cryptographic characteristics of sequences and provide information on the predictability and thus unsuitability for cryptography. It is desirable to have sequences with high linear complexity (profile) so that the necessary fragment approaches the length of the sequence itself[18,20]. Very recently, the first author and Winterhof[21] present some partial results of linear complexity profile of k-ary sequences in terms of a new correlation measure related to the correlation measure defined in Introduction. So according to Theorem 1 and the proof of Proposition 2 of [21], for $j = 1, 2$, if $L(E_N^{(j)}, n) < p$ we get

$$L(E_N^{(j)}, n) \geqslant n - \max_{1 \leqslant \ell \leqslant L(E_N^{(j)})+1} k^\ell \gamma_\ell(E_N^{(j)}, D),$$

from which one might derive a lower bound on linear complexity profile for $E_N^{(1)}$ and $E_N^{(2)}$, respectively. However, using the character sums directly, below we will get stronger lower bounds.

Theorem 5. *Suppose $k > 1$ and $k|d$ for $d = \gcd(p-1, q-1)$. The linear complexity profile $L(E_N^{(1)}, n)$ of the first n terms of $E_N^{(1)}$ defined in Definition 1 satisfies*

$$L(E_N^{(1)}, n) \gg n^{1/2} N^{-1/4} (\log N)^{-1/2}$$

for $1 \leqslant n < N$.

Proof. Let $L(E_N^{(1)}, n) = L$ and

$$e_{i+L}^{(1)} \equiv c_{L-1} e_{i+L-1}^{(1)} + \cdots + c_0 e_i^{(1)} \pmod{k}$$

for all $1 \leqslant i \leqslant n - L$, where $c_0, c_1, \ldots, c_{L-1} \in \mathbb{Z}_k$. Since otherwise the bound is trivial, we always suppose that $L < p (< q)$. We note that at least $n - L - (L+1)(p + q - 1)$ many $i \in \{1, 2, \ldots, n - L\}$ satisfy

$$i + l \in \mathbb{Z}_N^*, \text{ for all } l = 0, \ldots, L.$$

Let $\mathcal{I} = \{i : 1 \leqslant i \leqslant n - L,\ i + l \in \mathbb{Z}_N^* \text{ for all } l = 0, \ldots, L\}$. Now for $i \in \mathcal{I}$ and $\chi \in \mathcal{H}^*$ defined in the proof of Theorem 1, we obtain

$$\begin{aligned} 1 &= \chi(1) = \chi(\omega^0) \\ &= \chi(\omega^{c_L e_{i+L}^{(1)} + c_{L-1} e_{i+L-1}^{(1)} + \cdots + c_0 e_i^{(1)}}) \\ &= \chi((i+L)^{c_L} (i+L-1)^{c_{L-1}} \cdots i^{c_0}), \end{aligned}$$

where ω is defined as in Subsection 2.1 and $c_L = -1$. So we have

$$\Big| \sum_{i \in \mathcal{I}} \chi((i+L)^{c_L} (i+L-1)^{c_{L-1}} \cdots i^{c_0}) \Big|$$

$$\geqslant n - L - (L+1)(p+q-1).$$

Since $L < p (< q)$, by Lemma 2 we get

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

After simple calculations, we obtain the desired result. □

Theorem 6. *Suppose $k > 1$ and $k|d$ for $d = \gcd(p-1, q-1)$. The linear complexity profile $L(E_N^{(2)}, n)$ of the first n terms of $E_N^{(2)}$ defined in Definition 2 satisfies*

$$L(E_N^{(2)}, n) \gg n^{1/2} N^{-1/4} (\log N)^{-1/2}$$

for $1 \leqslant n < N$.

Proof. Let ϕ be the multiplicative character defined in the proof of Theorem 3. Following the path of Theorem 5 and using the equation

$$\begin{aligned} 1 &= \boldsymbol{e}_k(0) \\ &= \boldsymbol{e}_k(c_L e_{i+L}^{(2)} + c_{L-1} e_{i+L-1}^{(2)} + \cdots + c_0 e_i^{(2)}) \\ &= \phi((i+L)^{c_L} (i+L-1)^{c_{L-1}} \cdots i^{c_0}), \end{aligned}$$

we obtain the result. □

3 Final Remarks

In this paper, we consider distribution and correlation measures for two families of sequences of k-symbols over integers modulo pq. The proofs depend on certain character sums over $\mathbb{Z}_{pq}$. At the same time, we also estimate a lower bound on linear complexity profile for the resulting sequences. It is interesting to consider their exact values of linear complexity. In particular in [22], we present an exact value of linear complexity of $E_N^{(1)}$ when k is a prime.

The sequence $E_N^{(1)}$ is related to the Whiteman-generalized cyclotomic classes over $\mathbb{Z}_N$. Ding and Helleseth introduced a new generalized cyclotomic classes[23], which were called the *Ding-Helleseth-generalized cyclotomic classes* in [11].

For $k|d$ with $d = \gcd(p-1, q-1)$, the Ding-Helleseth-generalized cyclotomic classes were defined by

$$D_j' = \Big\{ g^{ks+j} x^i : s = 0, 1, \ldots, \frac{e}{k} - 1, 0 \leqslant i < d \Big\},$$

where $j = 0, 1, \ldots, k-1$. Then one can define a sequence of k symbols $E_N^{(3)} = \{e_1^{(3)}, e_2^{(3)}, \ldots, e_N^{(3)}\} \in \mathbb{Z}_k^N$ by

$$e_n^{(3)} = \begin{cases} j, & \text{if } n \in D_j',\ j = 0, 1, \ldots, k-1, \\ A, & \text{if } n \in P, \\ B, & \text{if } n \in Q_0, \end{cases}$$

for $n = 0, 1, \ldots, N-1$ and $A, B \in \mathbb{Z}_k$. Indeed, a similar sequence was introduced in [24]. According to the corresponding results in [24], one can find that $E_N^{(3)}$ may possess low k-error linear complexity and large autocorrelation values, so we should be careful when using it. Hence we will not consider the well-distribution measure and the correlation measure of order ℓ for $E_N^{(3)}$.

In this paper, we always suppose that $k|d$ for $d = \gcd(p-1, q-1)$. It is interesting to consider the case of $k \nmid d$.

Acknowledgements The authors wish to thank the editor and the reviewers for their valuable comments.

References

[1] Mauduit C, Sárközy A. On finite pseudo-random binary sequences I: Measures of pseudo-randomness, the Legendre symbol. *Acta Arithmetica*, 1997, 82: 365-377.

[2] Cassaigne J, Mauduit C, Sárközy A. On finite pseudo-random binary sequences, VII: The measures of pseudo-randomness. *Acta Arithmetica*, 2002, 103(2): 97-118.

[3] Mauduit C, Sarközy A. On finite pseudo-random sequences of k symbols. *Indagationes Mathematicae-New Series*, 2002, 13(1): 89-101.

[4] Ahlswede R, Mauduit C, Sárközy A. Large Families of Pseudorandom Sequences of k Symbols and Their Complexity, Part I. General Theory of Information Transfer and Combinatorics, *LNCS* 4123, Springer-Verlag, 2006, pp.293-307.

[5] Ahlswede R, Mauduit C, Sárközy A. Large Families of Pseudorandom Sequences of k Symbols and Their Complexity, Part II. General Theory of Information Transfer and Combinatorics, *LNCS* 4123, Springer-Verlag, 2006, pp.308-325.

[6] Bérczi G. On finite pseudo-random sequences of k symbols. *Periodica Mathematica Hungarica*, 2003, 47(1/2): 29-44.

[7] Mérai L. On finite pseudo-random lattices of k symbols. *Monatshefte für Mathematik*, 2010, 161(2): 173-191.

[8] Rivat J, Sárközy A. Modular constructions of pseudo-random binary sequences with composite moduli. *Periodica Mathematica Hungarica*, 2005, 51(2): 75-107.

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

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

[11] Chen Z, Li S. Some notes on generalized cyclotomic sequences of length pq. *Journal of Computer Science and Technology*, 2008, 23(5): 843-850.

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

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

[14] Du X, Chen Z. Trace representations of generalized cyclotomic sequences of length pq with arbitrary order. *Chinese Journal of Electronics*, 2009, 18(3): 460-464. (In Chinese)

[15] Yan T, Du X, Xiao G, Huang X. Linear complexity of binary Whiteman generalized cyclotomic sequences of order 2^k. *Information Sciences*, 2009, 179(7): 1019-1023.

[16] Green D H, Green P R. Polyphase related-prime sequences. *IEE Proceedings: Computers and Digital Techniques*, 2001, 148(2): 53-62.

[17] Hu Y, Wei S, Xiao G. On the linear complexity of generalised Legendre/Jacobi sequences. *Acta Electronica Sinica*, 2002, 8(2): 113-117. (In Chinese)

[18] Winterhof A. Linear Complexity and Related Complexity Measures. Selected Topics in Information and Coding Theory, Singapore: World Scientific, 2010, pp.3-40.

[19] Lidl R, Niederreiter H. Finite Fields. Cambridge: Cambridge Univ. Press, 1997.

[20] Niederreiter H. Linear complexity and related complexity measures for sequences. In *Proc. INDOCRYPT 2003*, New Delhi, India, Dec. 8-10, 2003, pp.1-17.

[21] Chen Z, Winterhof A. Linear complexity profile of m-ary pseudo-random sequences with small correlation measure. *Indagationes Mathematicae-New Series*, 2010. (To appear)

[22] Chen Z, Du X. Linear complexity and autocorrelation values of a polyphase generalized cyclotomic sequence of length pq. *Frontiers of Computer Science in China*, 2010, 4(4): 529-535.

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

[24] Meidl W. Remarks on a cyclotomic sequence. *Design Codes and Cryptography*, 2009, 51(1): 33-43.

Zhi-Xiong Chen was born in 1972 in Fujian province of China. He received the M.S. degree in mathematics from Fujian Normal University in 1999 and Ph.D. degree in cryptography from Xidian University, China, in 2006, respectively. Now he is an associate professor of Putian University. He is a member of CCF and CACR. His research interests include stream ciphers and elliptic curve cryptography.

Xiao-Ni Du was born in 1972 in Gansu province of China. She received the M.S. degree in computer science from Lanzhou University in 2000 and Ph.D. degree in cryptography from Xidian University, China, in 2008, respectively. Now she is an associate professor of Northwest Normal University. Her research interests include cryptology and information security.

Chen-Huang Wu was born in 1981 in Fujian province of China. He received the M.S. degree in mathematics from Zhangzhou Normal University in 2007. Now he is a lecturer of Putian University. He is a member of CCF and CACR. His research interests include digital signatures and elliptic curve cryptography.