ACTA ARITHMETICA
181.1 (2017)

A large family of pseudorandom sequences of k symbols with length pq

by

Huaning Liu and Bo Gao (Xi'an)

1. Introduction. In a series of papers Mauduit and Sárközy (partly with other coauthors) studied finite sequences of k symbols

$$E_N = (e_1, \dots, e_N) \in \mathcal{A}^N,$$

where $\mathcal{A} = \{a_1, \dots, a_k\}$ ($k \in \mathbb{N}, k \geq 2$) is a finite set of k symbols. Write

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

and for $w = (a_{i_1}, \dots, a_{i_l}) \in \mathcal{A}^l$, $D = (d_1, \dots, d_l)$ with non-negative integers $d_1 < \cdots < d_l$,

$$g(E_N, w, M, D) = |\{n : 1 \leq n \leq M,\ (e_{n+d_1}, \dots, e_{n+d_l}) = w\}|.$$

Mauduit and Sárközy [14] introduced the following pseudorandom measures.

Definition 1.1. The *f-well-distribution measure* of E_N is defined as

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

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

Definition 1.2. The *f-correlation measure* of order l of E_N is

$$\gamma_l(E_N) = \max_{w,M,D} |g(E_N, w, M, D) - M/k^l|,$$

where the maximum is taken over all $w \in \mathcal{A}^l$, $D = (d_1, \dots, d_l)$ and M such that $0 \leq d_1 < \cdots < d_l \leq N - M$.

2010 *Mathematics Subject Classification*: Primary 11K45; Secondary 11B50, 94A55, 94A60.
Key words and phrases: pseudorandom sequence, k symbols, cyclotomic class, character sum.
Received 29 February 2016; revised 10 May 2017.
Published online 9 October 2017.

DOI: 10.4064/aa8452-5-2017 © Instytut Matematyczny PAN, 2017

A sequence is considered to be a "good" pseudorandom sequence if both $\delta(E_N)$ and $\gamma_l(E_N)$ (at least for small l) are "small" in terms of N (in particular, both are $o(N)$ as $N \to \infty$, ideally $N^{1/2+\varepsilon}$). A few pseudorandom sequences of k symbols have been studied (see [1], [2], [9], [12], [14]). For example, Mauduit and Sárközy [14] proved the following.

PROPOSITION 1.1 (Mauduit and Sárközy). *Let p be a prime, and let χ be a Dirichlet character modulo p of order $k \geq 2$. Write $N = p-1$, and define the sequence $E_N = (e_1, \ldots, e_N)$ by*

$$e_n = \chi(n).$$

Then

$$\delta(E_N) < 2N^{1/2} \log N, \quad \gamma_l(E_N) < 27klN^{1/2} \log N.$$

Ahlswede, Mauduit and Sárközy [1], [2] gave a large family of sequences of k symbols by using the Dirichlet character.

PROPOSITION 1.2 (Ahlswede, Mauduit and Sárközy). *Assume that $k \in \mathbb{N}$, $k \geq 2$, p is a prime number, χ is a character modulo p of order k, and $f(x) \in \mathbb{F}_p[x]$ has degree h (> 0) and no multiple zero in $\overline{\mathbb{F}}_p$. Define the sequence $E_p = (e_1, \ldots, e_p)$ of kth roots of unity by*

$$e_n = \begin{cases} \chi(f(n)) & \text{for } (f(n), p) = 1, \\ 1 & \text{for } p \mid f(n). \end{cases}$$

Then $\delta(E_p) < 11hp^{1/2} \log p$. Moreover, suppose that $l \in \mathbb{N}$ and at least one of the following assumptions holds:

(i) *$h < p$, $l(k-1) < p$, the prime factorization of k is $k = q_1^{\alpha_1} \cdots q_s^{\alpha_s}$ (where $q_1, \ldots, q_s$ are distinct primes and $\alpha_1, \ldots, \alpha_s \in \mathbb{N}$), and each q_i is a primitive root modulo p.*

(ii) *$l \leq k/(k-1)$ and $h < p$.*

(iii) *$(4l(k-1))^h < p$.*

Then $\gamma_l(E_p) < 10lhkp^{1/2} \log p$.

Mak [12] presented some new families of pseudorandom sequences of k symbols, which generalized the above constructions. Gomez and Winterhof [9] constructed pseudorandom sequences of k symbols by using Dirichlet characters and the Fermat quotient.

PROPOSITION 1.3 (Gomez and Winterhof). *For a prime p and an integer u with $(u, p) = 1$, the Fermat quotient $q_p(u)$ modulo p is defined by*

$$q_p(u) \equiv \frac{u^{p-1} - 1}{p} \pmod{p}, \quad 0 \leq q_p(u) \leq p-1,$$

and we define $q_p(u) = 0$ if $p \mid u$. Let χ be a Dirichlet character modulo p of

order $k \geq 2$. *Define* $E_{p^2} = (e_1, \ldots, e_{p^2})$ *by*

$$e_n = \chi(q_p(n)).$$

Then

$$\delta(E_{p^2}) \ll p^{3/2} \log p, \quad \gamma_l(E_{p^2}) \ll l p^{5/3}.$$

Note that these constructions are with moduli p or p^2. One might wish to look for constructions with composite moduli N, since this type of constructions are more important in cryptography. Throughout this paper we suppose that $N = pq$ and p, q are two distinct primes satisfying "RSA type" conditions with $2 < p < q < 2p$. From the Chinese Remainder Theorem we know that there are common primitive roots of both p and q. Let g be a fixed common primitive roots of both p and q, and let x be an integer satisfying

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

Let $d = (p-1, q-1)$ and $e = (p-1)(q-1)/d$. Following [16], the generalized cyclotomic classes of order d are defined by

$$D_i = \{g^s x^i : s = 0, 1, \ldots, e-1\}, \quad i = 0, 1, \ldots, d-1.$$

It is not hard to prove that

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

We set

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

Hence,

$$\mathbb{Z}_{pq} = P \cup Q_0 \cup \bigcup_{i=0}^{d-1} D_i.$$

The Whiteman generalized cyclotomic classes were applied to construct binary sequences, pseudorandom subsets, and k symbols (see [3], [4], [5], [6], [8] and [11]). For example, Chen, Du and Wu [5] defined and studied the following sequence of k symbols by using the generalized cyclotomic classes.

Proposition 1.4 (Chen, Du and Wu). *Suppose that* $k > 1$ *and* $k \mid d$ *for* $d = (p-1, q-1)$. *Define* $E_N = (e_1, \ldots, e_N) \in \mathbb{Z}_k^N$ *by*

$$e_n = \begin{cases} i \pmod{k} & \text{if } n \in D_i,\ 0 \leq i < d, \\ A & \text{if } n \in P, \\ B & \text{if } n \in Q_0, \end{cases}$$

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

$$\delta(E_N) \ll N^{1/2} \log N, \quad \gamma_2(E_N) \ll N^{3/4} \log N.$$

In this paper we construct a large family of pseudorandom sequences of k symbols with length pq by using generalized cyclotomic classes, and study their properties. The main results are the following.

THEOREM 1.1. *Let $f(x) = a_h x^h + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ with $(a_h, N) = 1$ and $0 < h < p$ $(< q)$. Assume that $f(x)$ as a polynomial over $\mathbb{F}_p$ has no multiple roots in $\overline{\mathbb{F}}_p$ and $f(x)$ as a polynomial over $\mathbb{F}_q$ has no multiple roots in $\overline{\mathbb{F}}_q$. Suppose that $k > 1$ and $k \mid d = (p-1, q-1)$. Define $E_N = (e_1, \ldots, e_N) \in \mathbb{Z}_k^N$ by*

$$e_n = \begin{cases} i \pmod k & \text{if } f(n) \in D_i,\ 0 \le i \le d-1, \\ A & \text{if } f(n) \in P, \\ B & \text{if } f(n) \in Q_0, \end{cases}$$

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

$$\delta(E_N) \ll h^2 N^{1/2} \log N, \tag{1.1}$$

$$\gamma_2(E_N) \ll h N^{3/4}, \tag{1.2}$$

$$\gamma_3(E_N) \ll h N^{3/4}. \tag{1.3}$$

THEOREM 1.2. *Define E_N as in Theorem 1.1, and denote $D = (d_1, \ldots, d_l)$ with $0 \le d_1 < \cdots < d_l < N$. Suppose that $w = (a_{i_1}, \ldots, a_{i_l}) \in \mathbb{Z}_k^l$ and M is a positive integer with $M \le N - d_l$.*

(i) *If $d_i \not\equiv d_j \pmod p$ and $d_i \not\equiv d_j \pmod q$, $1 \le i, j \le l$, then*

$$|g(E_N, w, M, D) - M/k^l| \ll h^2 N^{1/2} \log N. \tag{1.4}$$

(ii) *If $d_1 \equiv \cdots \equiv d_l \pmod p$ or $d_1 \equiv \cdots \equiv d_l \pmod q$, then*

$$|g(E_N, w, M, D) - M/k^l| \ll h N^{3/4}. \tag{1.5}$$

THEOREM 1.3. *Define E_N as in Theorem 1.1. Take $w = (0,0,0,0) \in \mathbb{Z}_k^4$, $D = (d_1, d_2, d_3, d_4)$ and M satisfying*

$$d_1 = 0, \quad d_2 = p, \quad d_3 = q, \quad d_4 = p + q, \quad M = N - p - q.$$

Then

$$g(E_N, w, M, D) - \frac{M}{k^4} = \frac{k-1}{k^4} N + O(h N^{3/4} \log N). \tag{1.6}$$

By Theorem 1.3, $\gamma_4(E_N)$ is extremely large, so the f-correlation γ_l of higher order l could be greater than $c_l N$ provided the prime factors p and q of N are known. Therefore p and q should be kept secret. Furthermore, for $w = (a_{i_1}, \ldots, a_{i_l}) \in \mathbb{Z}_k^l$ and $d_1, \ldots, d_l$, M such that $0 \le d_1 < \cdots < d_l < p$ $(< q)$ and $M \le N - d_l$, from Theorem 1.2 we have

$$|g(E_N, w, M, D) - M/k^l| \ll h^2 N^{1/2} \log N.$$

This suggests that the high order "short range" correlation of E_N is small.

2. Some lemmas. In order to prove the theorems, we need the following lemmas.

LEMMA 2.1 ([13, Lemma 2]). *Let p be a prime number, and let χ be a non-principal character modulo p of order d. Suppose that $f(x) \in \mathbb{F}_p[x]$ has degree l, and $f(x)$ is not a constant multiple of the dth power of a polynomial over $\mathbb{F}_p$. Then for all $a \in \mathbb{Z}$ we have*

$$\Big|\sum_{n\in\mathbb{F}_p} \chi(f(n))\,\mathrm{e}(an/p)\Big| \le sp^{1/2},$$

where $\mathrm{e}(y)=e^{2\pi iy}$, and s denotes the number of distinct zeros of $f(x)$ in $\overline{\mathbb{F}}_p$.

LEMMA 2.2 ([7]). *Let $k, d \in \mathbb{N}$ and let p be a prime number with $d \mid p-1$. Let $r \le k$, $0 \le d_1 < \cdots < d_r < p$, $1 \le \delta_1, \dots, \delta_r < d$ and $(\delta_1, \dots, \delta_r) = 1$. Suppose that $f(x) \in \mathbb{F}_p[x]$ is a polynomial of degree l with no multiple roots in $\overline{\mathbb{F}}_p$. Define*

$$F(n) = f(n+d_1)^{\delta_1} \cdots f(n+d_r)^{\delta_r}$$

and write

$$F(n) = b(n-x_1)^{u_1} \cdots (n-x_s)^{u_s}$$

in $\overline{\mathbb{F}}_p$, where $x_i \ne x_j$ for $i \ne j$. Suppose one of the following assumptions holds:

(i) $k = 2$;
(ii) *d is a prime divisor of $p-1$ and $(4k)^l < p$;*
(iii) *the polynomial $x^{p-1} + \cdots + x + 1$ is irreducible in $\mathbb{F}_w[x]$ for all prime factors w of d.*

Then $(d, u_1, \dots, u_s) = 1$.

NOTATION 2.1. For $a \in \mathbb{Z}$ and $q \in \mathbb{N}$ such that $(a,q) = 1$, let $i_q(a)$ denote the unique integer b such that $0 \le b \le q-1$ and $ab \equiv 1 \pmod q$.

3. The well-distribution measure of E_N. Define

$$\mathcal{H} = \{\chi \bmod N : \chi(g) = 1\} \quad \text{and} \quad G = \{g, g^2, \dots, g^e\}.$$

Then $\mathcal{H}$ is the annihilator of G in $\mathbb{Z}_N^*$. By [10, Theorem 5.6] we know that the order of $\mathcal{H}$ is $|\widehat{\mathbb{Z}_N^*}|/|\widehat{G}| = d$. Denote $\mathcal{H}^* = \mathcal{H} \setminus \{\chi_0\}$.

For any χ modulo N we write $\overline{\chi}$ for the inverse of χ. By the definition of D_i we have

$$
\begin{aligned}
(3.1)\quad f(n)\in D_i &\Leftrightarrow f(n)\equiv g^s x^i \pmod N \text{ for some } s \text{ with } 0\le s\le e-1\\
&\Leftrightarrow \frac{1}{\phi(N)}\sum_{s=0}^{e-1}\sum_{\chi \bmod N}\chi(f(n))\overline{\chi}(g^s x^i)=1\\
&\Leftrightarrow \frac{1}{d}\sum_{\chi\in\mathcal{H}}\chi(f(n))\overline{\chi}(x^i)=1.
\end{aligned}
$$

We further study the properties of $\mathcal{H}$.

THEOREM 3.1. *Assume that $k\ge 1$ and $k\mid d$ for $d=(p-1,q-1)$. For any integers a and r with $r\ge 1$, we have*

$$
\sum_{\chi\in\mathcal{H}^*}\Bigg|\sum_{\substack{i=0\\ i\equiv a \,(\mathrm{mod}\, k)}}^{d-1}\chi(x^i)\Bigg|^r=\frac{d^r}{k^r}(k-1),
$$

$$
\sum_{\chi'\in\mathcal{H}^*}\sum_{\chi''\in\mathcal{H}^*}\Bigg|\sum_{i=0}^{d-1}\chi'(x^i)\sum_{\substack{j=0\\ j\not\equiv i \,(\mathrm{mod}\, k)}}^{d-1}\chi''(x^j)\Bigg|^r=\frac{d^{2r}}{k^r}(k-1).
$$

Suppose that $\chi\in\mathcal{H}^*$ is of order t. Write $\chi^*=\chi_1\chi_2$ with χ_1 a character modulo p of order t_1 and χ_2 a character modulo q of order t_2. Then

$$
t=t_1=t_2.
$$

Proof. From the properties of character sums we get

$$
\begin{aligned}
\sum_{\chi\in\mathcal{H}^*}\Bigg|\sum_{\substack{i=0\\ i\equiv a \,(\mathrm{mod}\, k)}}^{d-1}\chi(x^i)\Bigg|^r
&=\sum_{\substack{\chi_1 \bmod p\ \chi_2 \bmod q\\ \chi_1(g)\chi_2(g)=1\\ \chi_1\chi_2\ne\chi_0}}\Bigg|\sum_{\substack{i=0\\ i\equiv a \,(\mathrm{mod}\, k)}}^{d-1}\chi_1(x^i)\chi_2(x^i)\Bigg|^r\\
&=\sum_{\substack{\chi_1 \bmod p\ \chi_2 \bmod q\\ \chi_1(g)\chi_2(g)=1\\ \chi_1\chi_2\ne\chi_0}}\Bigg|\sum_{\substack{i=0\\ i\equiv a \,(\mathrm{mod}\, k)}}^{d-1}\chi_1(g)^i\Bigg|^r.
\end{aligned}
$$

Write

$$
\chi_1(n)=\begin{cases}\mathrm{e}\Big(\dfrac{m_1\,\mathrm{ind}_{g,p}(n)}{p-1}\Big), & (n,p)=1,\\ 0, & (n,p)>1,\end{cases}
$$

$$
\chi_2(n)=\begin{cases}\mathrm{e}\Big(\dfrac{m_2\,\mathrm{ind}_{g,q}(n)}{q-1}\Big), & (n,q)=1,\\ 0, & (n,q)>1,\end{cases}
$$

where $\mathrm{ind}_{g,p}(n)$ is the unique integer with $n\equiv g^{\mathrm{ind}_{g,p}(n)} \pmod p$, $0\le \mathrm{ind}_{g,p}(n)\le p-2$, and $\mathrm{ind}_{g,q}(n)$ denotes the unique integer with $n\equiv g^{\mathrm{ind}_{g,q}(n)}$

$(\mathrm{mod}\ q)$, $0 \le \mathrm{ind}_{g,q}(n) \le q-2$. Then we have

$$\sum_{\chi\in\mathcal{H}^*}\Bigg|\sum_{\substack{i=0\\ i\equiv a\,(\mathrm{mod}\,k)}}^{d-1}\chi(x^i)\Bigg|^r = \sum_{\substack{m_1=0}}^{p-2}\sum_{\substack{m_2=0\\ \mathrm{e}(\frac{m_1}{p-1})\,\mathrm{e}(\frac{m_2}{q-1})=1\\ m_1^2+m_2^2>0}}^{q-2}\Bigg|\sum_{\substack{i=0\\ i\equiv a\,(\mathrm{mod}\,k)}}^{d-1}\mathrm{e}\Big(\frac{im_1}{p-1}\Big)\Bigg|^r.$$

It is easy to show that

$$\begin{aligned}\mathrm{e}\Big(\frac{m_1}{p-1}\Big)\mathrm{e}\Big(\frac{m_2}{q-1}\Big)=1 &\Leftrightarrow \mathrm{e}\Big(\frac{m_1(q-1)+m_2(p-1)}{(p-1)(q-1)}\Big)=1\\ &\Leftrightarrow (p-1)(q-1)\,|\,m_1(q-1)+m_2(p-1)\\ &\Leftrightarrow \frac{(p-1)(q-1)}{d}\,\Big|\,m_1\frac{q-1}{d}+m_2\frac{p-1}{d}.\end{aligned}$$

Hence,

$$\frac{p-1}{d}\,\Big|\,m_1,\qquad \frac{q-1}{d}\,\Big|\,m_2.$$

Therefore

$$\sum_{\chi\in\mathcal{H}^*}\Bigg|\sum_{\substack{i=0\\ i\equiv a\,(\mathrm{mod}\,k)}}^{d-1}\chi(x^i)\Bigg|^r = \sum_{0\le n_1\le d-1}\sum_{\substack{0\le n_2\le d-1\\ \frac{(p-1)(q-1)}{d}\,\mid\, n_1\frac{(p-1)(q-1)}{d^2}+n_2\frac{(p-1)(q-1)}{d^2}\\ n_1^2+n_2^2>0}}\Bigg|\sum_{\substack{i=0\\ i\equiv a\,(\mathrm{mod}\,k)}}^{d-1}\mathrm{e}\Big(\frac{in_1}{d}\Big)\Bigg|^r$$

$$= \sum_{0\le n_1\le d-1}\sum_{\substack{0\le n_2\le d-1\\ n_1+n_2\equiv 0\,(\mathrm{mod}\,d)\\ n_1^2+n_2^2>0}}\Bigg|\sum_{\substack{i=0\\ i\equiv a\,(\mathrm{mod}\,k)}}^{d-1}\mathrm{e}\Big(\frac{in_1}{d}\Big)\Bigg|^r = \sum_{1\le n_1\le d-1}\Bigg|\sum_{\substack{i=0\\ i\equiv a\,(\mathrm{mod}\,k)}}^{d-1}\mathrm{e}\Big(\frac{in_1}{d}\Big)\Bigg|^r$$

$$= \sum_{1\le n_1\le d-1}\Big|\mathrm{e}\Big(\frac{an_1}{d}\Big)\sum_{0\le j\le d/k-1}\mathrm{e}\Big(\frac{jn_1}{d/k}\Big)\Big|^r = \frac{d^r}{k^r}\sum_{\substack{1\le n_1\le d-1\\ \frac{d}{k}\,|\,n_1}}1=\frac{d^r}{k^r}(k-1).$$

Similarly we have

$$\sum_{\chi'\in\mathcal{H}^*}\sum_{\chi''\in\mathcal{H}^*}\Bigg|\sum_{i=0}^{d-1}\chi'(x^i)\sum_{\substack{j=0\\ j\not\equiv i\,(\mathrm{mod}\,k)}}^{d-1}\chi''(x^j)\Bigg|^r$$

$$= \sum_{\substack{\chi_1'\bmod p\\ \chi_1'(g)\chi_2'(g)=1\\ \chi_1'\chi_2'\ne\chi_0}}\sum_{\chi_2'\bmod q}\sum_{\substack{\chi_1''\bmod p\\ \chi_1''(g)\chi_2''(g)=1\\ \chi_1''\chi_2''\ne\chi_0}}\sum_{\chi_2''\bmod q}\Bigg|\sum_{i=0}^{d-1}\chi_1'(g)^i\sum_{\substack{j=0\\ j\not\equiv i\,(\mathrm{mod}\,k)}}^{d-1}\chi_1''(g)^j\Bigg|^r$$

$$= \sum_{\substack{m_1'=0}}^{p-2}\sum_{\substack{m_2'=0\\ \mathrm{e}(\frac{m_1'}{p-1})\,\mathrm{e}(\frac{m_2'}{q-1})=1\\ (m_1')^2+(m_2')^2>0}}^{q-2} \sum_{\substack{m_1''=0}}^{p-2}\sum_{\substack{m_2''=0\\ \mathrm{e}(\frac{m_1''}{p-1})\,\mathrm{e}(\frac{m_2''}{q-1})=1\\ (m_1'')^2+(m_2'')^2>0}}^{q-2} \left|\sum_{i=0}^{d-1}\mathrm{e}\Big(\frac{im_1'}{p-1}\Big) \sum_{\substack{j=0\\ j\not\equiv i\,(\mathrm{mod}\,k)}}^{d-1}\mathrm{e}\Big(\frac{jm_1''}{p-1}\Big)\right|^r$$

$$= \sum_{\substack{0\le n_1'\le d-1\\ n_1'+n_2'\equiv 0\,(\mathrm{mod}\,d)\\ (n_1')^2+(n_2')^2>0}}\sum_{0\le n_2'\le d-1} \sum_{\substack{0\le n_1''\le d-1\\ n_1''+n_2''\equiv 0\,(\mathrm{mod}\,d)\\ (n_1'')^2+(n_2'')^2>0}}\sum_{0\le n_2''\le d-1} \left|\sum_{i=0}^{d-1}\mathrm{e}\Big(\frac{in_1'}{d}\Big) \sum_{\substack{j=0\\ j\not\equiv i\,(\mathrm{mod}\,k)}}^{d-1}\mathrm{e}\Big(\frac{jn_1''}{d}\Big)\right|^r$$

$$= \sum_{1\le n_1'\le d-1}\sum_{1\le n_1''\le d-1} \left|\sum_{i=0}^{d-1}\mathrm{e}\Big(\frac{in_1'}{d}\Big) \sum_{\substack{j=0\\ j\not\equiv i\,(\mathrm{mod}\,k)}}^{d-1}\mathrm{e}\Big(\frac{jn_1''}{d}\Big)\right|^r$$

$$= \sum_{1\le n_1'\le d-1}\sum_{1\le n_1''\le d-1} \left|\sum_{i=0}^{d-1}\mathrm{e}\Big(\frac{in_1'}{d}\Big) \sum_{\substack{j=0\\ j\equiv i\,(\mathrm{mod}\,k)}}^{d-1}\mathrm{e}\Big(\frac{jn_1''}{d}\Big)\right|^r$$

$$= \sum_{1\le n_1'\le d-1}\sum_{1\le n_1''\le d-1} \left|\sum_{i=0}^{d-1}\mathrm{e}\Big(\frac{i(n_1'+n_1'')}{d}\Big) \sum_{0\le j\le d/k-1}\mathrm{e}\Big(\frac{jn_1''}{d/k}\Big)\right|^r$$

$$= \frac{d^{2r}}{k^r} \sum_{\substack{1\le n_1'\le d-1\\ n_1'+n_1''\equiv 0\,(\mathrm{mod}\,d)\\ \frac{d}{k}\,|\,n_1''}}\sum_{1\le n_1''\le d-1} 1$$

$$= \frac{d^{2r}}{k^r} \sum_{\substack{1\le n_1''\le d-1\\ \frac{d}{k}\,|\,n_1''}} 1 = \frac{d^{2r}}{k^r}(k-1).$$

Furthermore, for $\chi\in\mathcal{H}^*$ we write $\chi^*=\chi_1\chi_2$, where

$$\chi_1(n)=\begin{cases}\mathrm{e}\Big(\dfrac{m_1\,\mathrm{ind}_{g,p}(n)}{p-1}\Big), & (n,p)=1,\\ 0, & (n,p)>1,\end{cases}$$

$$\chi_2(n)=\begin{cases}\mathrm{e}\Big(\dfrac{m_2\,\mathrm{ind}_{g,q}(n)}{q-1}\Big), & (n,q)=1,\\ 0, & (n,q)>1,\end{cases}$$

for some $0\le m_1\le p-2$ and $0\le m_2\le q-2$. From $\chi_1(g)\chi_2(g)=1$ we know that

$$\frac{(p-1)(q-1)}{d}\,\Big|\,m_1\frac{q-1}{d}+m_2\frac{p-1}{d},\qquad \frac{p-1}{d}\,\Big|\,m_1,\qquad \frac{q-1}{d}\,\Big|\,m_2.$$

Then

$$\chi_1(n) = \begin{cases} \mathrm{e}\Big(\dfrac{n_1 \operatorname{ind}_{g,p}(n)}{d}\Big), & (n,p)=1,\\ 0, & (n,p)>1, \end{cases}$$

$$\chi_2(n) = \begin{cases} \mathrm{e}\Big(\dfrac{n_2 \operatorname{ind}_{g,q}(n)}{d}\Big), & (n,q)=1,\\ 0, & (n,q)>1, \end{cases}$$

for some $0 \le n_1 \le d-1$, $0 \le n_2 \le d-1$, $n_1+n_2 \equiv 0 \pmod d$ and $n_1^2+n_2^2 > 0$. Therefore $\operatorname{ord}\chi = \operatorname{ord}\chi_1 = \operatorname{ord}\chi_2$. ∎

Remark 3.1. From Theorem 3.1 we know that any $\chi \in \mathcal{H}^*$ can be expressed as $\chi = \chi_p\chi_q$, where χ_p is a non-principal character modulo p, χ_q is a non-principal character modulo q, and $\operatorname{ord}\chi = \operatorname{ord}\chi_1 = \operatorname{ord}\chi_2$.

Now we study the well-distribution measure of E_N. For any $a \in \mathbb{Z}_k$ and $M, u, v \in \mathbb{N}$ with $1 \le u \le u+(M-1)v \le N$, by (3.1) we have

$$\begin{aligned} (3.2)\qquad x(E_N,a,M,u,v) &= |\{j : 0 \le j \le M-1,\ e_{u+jv} = a\}| \\ &\le \sum_{\substack{j=0\\ f(u+jv)\in\mathbb{Z}_N^*\\ e_{u+jv}=a}}^{M-1} 1 + \sum_{\substack{j=0\\ f(u+jv)\in P\cup Q_0}}^{M-1} 1 = \sum_{i=0}^{d-1} \sum_{\substack{j=0\\ f(u+jv)\in D_i\\ e_{u+jv}=a}}^{M-1} 1 + O(h(p+q-1)) \\ &= \sum_{i=0}^{d-1} \sum_{\substack{j=0\\ f(u+jv)\in D_i\\ i\equiv a \,(\mathrm{mod}\, k)}}^{M-1} 1 + O(hN^{1/2}) \\ &= \frac{1}{d} \sum_{\substack{i=0\\ i\equiv a \,(\mathrm{mod}\, k)}}^{d-1} \sum_{j=0}^{M-1} \sum_{\chi\in\mathcal{H}} \chi(f(u+jv))\overline{\chi}(x^i) + O(hN^{1/2}) \\ &= \frac{M}{k} + \frac{1}{d} \sum_{\chi\in\mathcal{H}^*} \Bigg(\sum_{\substack{i=0\\ i\equiv a \,(\mathrm{mod}\, k)}}^{d-1} \overline{\chi}(x^i) \Bigg) \sum_{j=0}^{M-1} \chi(f(u+jv)) + O(hN^{1/2}). \end{aligned}$$

From the trigonometric sum we get

$$\begin{aligned} (3.3)\qquad \sum_{j=0}^{M-1} \chi(f(u+jv)) &= \frac{1}{N} \sum_{j=0}^{M-1} \sum_{n=1}^{N} \sum_{|r|<N/2} \mathrm{e}\Big(\frac{r(n-(u+jv))}{N}\Big)\chi(f(n)) \\ &= \frac{1}{N} \sum_{|r|<N/2} \sum_{j=0}^{M-1} \mathrm{e}\Big(\frac{-r(u+jv)}{N}\Big) \sum_{n=1}^{N} \chi(f(n))\,\mathrm{e}\Big(\frac{rn}{N}\Big). \end{aligned}$$

Hence we derive

$$\begin{aligned}\sum_{n=1}^{N}\chi(f(n))\,\mathrm{e}\Big(\frac{rn}{N}\Big) &= \sum_{c=0}^{q-1}\sum_{d=0}^{p-1}\chi(f(cp+dq))\,\mathrm{e}\Big(\frac{r(cp+dq)}{N}\Big)\\ &= \sum_{c=0}^{q-1}\chi_q(f(cp))\,\mathrm{e}\Big(\frac{rc}{q}\Big)\sum_{d=0}^{p-1}\chi_p(f(dq))\,\mathrm{e}\Big(\frac{rd}{p}\Big)\\ &= \sum_{c=0}^{q-1}\chi_q(f(c))\,\mathrm{e}\Big(\frac{ri_q(p)c}{q}\Big)\sum_{d=0}^{p-1}\chi_p(f(d))\,\mathrm{e}\Big(\frac{ri_p(q)d}{p}\Big).\end{aligned}$$

By Lemma 2.1 we have

$$\sum_{c=0}^{q-1}\chi_q(f(c))\,\mathrm{e}\Big(\frac{ri_q(p)c}{q}\Big)\ll hq^{1/2},\quad \sum_{d=0}^{p-1}\chi_p(f(d))\,\mathrm{e}\Big(\frac{ri_p(q)d}{p}\Big)\ll hp^{1/2},$$

therefore

$$\sum_{n=1}^{N}\chi(f(n))\,\mathrm{e}\Big(\frac{rn}{N}\Big)\ll h^2N^{1/2}. \tag{3.4}$$

It is not hard to show that

$$\begin{aligned}&\sum_{|r|<N/2}\Big|\sum_{j=0}^{M-1}\mathrm{e}\Big(\frac{-r(u+jv)}{N}\Big)\Big| \\ &\quad= M+\sum_{0<|r|<N/2}\Big|\sum_{j=0}^{M-1}\mathrm{e}\Big(\frac{-r(u+jv)}{N}\Big)\Big|\\ &\quad\le M+2\sum_{0<|r|<N/2}\frac{1}{\big|1-\mathrm{e}\big(\frac{-rv}{N}\big)\big|}=M+2\sum_{0<|r|<N/2}\frac{1}{\big|1-\mathrm{e}\big(\frac{r}{N}\big)\big|}\\ &\quad= M+\sum_{0<|r|<N/2}\frac{1}{\big|\sin\frac{\pi r}{N}\big|}\le M+\sum_{0<|r|<N/2}\frac{N}{2|r|}\\ &\quad= M+\sum_{0<r<N/2}\frac{N}{2r}\le M+\sum_{0<r<N/2}\frac{N}{r}\ll N\log N.\end{aligned} \tag{3.5}$$

From (3.2)–(3.5) and Theorem 3.1 we immediately get

$$\begin{aligned}&|x(E_N,a,M,u,v)-M/k|\\ &\ll\frac{1}{d}\Big|\sum_{\chi\in\mathcal{H}^*}\Big(\sum_{\substack{i=0\\ i\equiv a\,(\mathrm{mod}\,k)}}^{d-1}\overline{\chi}(x^i)\Big)\sum_{j=1}^{M-1}\chi(f(u+jv))\Big|+hN^{1/2}\ll h^2N^{1/2}\log N.\end{aligned}$$

Therefore

$$\delta(E_N) = \max_{a,M,u,v} |x(E_N, a, M, u, v) - M/k| \ll h^2 N^{1/2} \log N.$$

This proves (1.1).

4. The correlation measure of order 2 and 3 of E_N. For any $w = (a_{i_1}, a_{i_2}) \in \mathbb{Z}_k^2$ and $D = (d_1, d_2)$ with $0 \le d_1 < d_2 < N - M$, by (3.1) we have

$$\begin{aligned} g(E_N, w, M, D) &= |\{m : 1 \le m \le M,\, e_{m+d_1} = a_{i_1},\, e_{m+d_2} = a_{i_2}\}| \\ &= \sum_{\substack{m=1 \\ f(m+d_1)\in\mathbb{Z}_N^* \\ f(m+d_2)\in\mathbb{Z}_N^* \\ e_{m+d_1}=a_{i_1} \\ e_{m+d_2}=a_{i_2}}}^{M} 1 + O(hN^{1/2}) = \sum_{i=0}^{d-1}\sum_{j=0}^{d-1} \sum_{\substack{m=1 \\ f(m+d_1)\in D_i \\ f(m+d_2)\in D_j \\ e_{m+d_1}=a_{i_1} \\ e_{m+d_2}=a_{i_2}}}^{M} 1 + O(hN^{1/2}) \\ &= \frac{1}{d^2} \sum_{i\equiv a_{i_1} \pmod k}^{d-1} \sum_{j\equiv a_{i_2} \pmod k}^{d-1} \sum_{m=1}^{M} \sum_{\chi_1\in\mathcal{H}} \overline{\chi}_1(x^i)\chi_1(f(m+d_1)) \\ &\qquad \times \sum_{\chi_2\in\mathcal{H}} \overline{\chi}_2(x^j)\chi_2(f(m+d_2)) + O(hN^{1/2}). \end{aligned}$$

Using the methods in Section 3 we get

$$\begin{aligned} &\frac{1}{d^2} \sum_{i\equiv a_{i_1} \pmod k}^{d-1} \sum_{j\equiv a_{i_2} \pmod k}^{d-1} \sum_{\substack{m=1 \\ (f(m+d_2),N)=1}}^{M} \sum_{\chi_1\in\mathcal{H}^*} \overline{\chi}_1(x^i)\chi_1(f(m+d_1)) \\ &\qquad\qquad \ll h^2 N^{1/2} \log N, \\ &\frac{1}{d^2} \sum_{i\equiv a_{i_1} \pmod k}^{d-1} \sum_{j\equiv a_{i_2} \pmod k}^{d-1} \sum_{\substack{m=1 \\ (f(m+d_1),N)=1}}^{M} \sum_{\chi_2\in\mathcal{H}^*} \overline{\chi}_2(x^j)\chi_2(f(m+d_2)) \\ &\qquad\qquad \ll h^2 N^{1/2} \log N. \end{aligned}$$

Therefore

$$\begin{aligned} (4.1)\qquad & g(E_N, w, M, D) \\ &= \frac{M}{k^2} + \frac{1}{d^2} \sum_{\chi_1\in\mathcal{H}^*} \Bigg(\sum_{i\equiv a_{i_1} \pmod k}^{d-1} \overline{\chi}_1(x^i) \Bigg) \sum_{\chi_2\in\mathcal{H}^*} \Bigg(\sum_{j\equiv a_{i_2} \pmod k}^{d-1} \overline{\chi}_2(x^j) \Bigg) \\ &\qquad \times \sum_{m=1}^{M} \chi_1(f(m+d_1))\chi_2(f(m+d_2)) + O(h^2 N^{1/2} \log N). \end{aligned}$$

Note that $\mathcal{H}$ is cyclic. Let $\chi' \in \mathcal{H}^*$ be a generator of $\mathcal{H}$. For $\chi_1, \chi_2 \in \mathcal{H}^*$, we write

$$\chi_1 = (\chi')^{b_1}, \quad \chi_2 = (\chi')^{b_2}, \quad 1 \le b_1, b_2 \le d-1.$$

Define

$$\chi^* = (\chi')^{(b_1,b_2)}, \quad \delta_1 = b_1/(b_1,b_2), \quad \delta_2 = b_2/(b_1,b_2).$$

Then

$$\chi_1 = (\chi^*)^{\delta_1}, \quad \chi_2 = (\chi^*)^{\delta_2}, \quad 1 \le \delta_1, \delta_2 \le d-1, \quad (\delta_1,\delta_2) = 1.$$

Notice that the order of χ^* is a divisor of d with $\operatorname{ord}\chi^* > 1$. Thus we have

$$\begin{aligned}(4.2)\qquad &\sum_{m=1}^{M} \chi_1(f(m+d_1))\chi_2(f(m+d_2))\\ &= \sum_{m=1}^{M} \chi^*\big(f(m+d_1)^{\delta_1} f(m+d_2)^{\delta_2}\big)\\ &= \frac{1}{N}\sum_{m=1}^{N} \chi^*\big(f(m+d_1)^{\delta_1} f(m+d_2)^{\delta_2}\big) \sum_{u=1}^{M}\sum_{|a|<N/2} \mathrm{e}\Big(\frac{a(m-u)}{N}\Big)\\ &= \frac{1}{N}\sum_{|a|<N/2}\sum_{u=1}^{M} \mathrm{e}\Big(-\frac{au}{N}\Big) \sum_{m=1}^{N} \chi^*\big(f(m+d_1)^{\delta_1} f(m+d_2)^{\delta_2}\big)\,\mathrm{e}\Big(\frac{am}{N}\Big).\end{aligned}$$

Write $\chi^* = \chi_p\chi_q$ with χ_p a character modulo p of order $t_p > 1$ and χ_q a character modulo q of order $t_q > 1$, where t_p, t_q are divisors of d. We have

$$\begin{aligned}&\sum_{m=1}^{N} \chi^*\big(f(m+d_1)^{\delta_1} f(m+d_2)^{\delta_2}\big)\,\mathrm{e}\Big(\frac{am}{N}\Big)\\ &\quad= \sum_{u=0}^{q-1}\sum_{v=0}^{p-1} \chi^*\big(f(up+vq+d_1)^{\delta_1} f(up+vq+d_2)^{\delta_2}\big)\,\mathrm{e}\Big(\frac{a(up+vq)}{N}\Big)\\ &\quad= \sum_{u=0}^{q-1} \chi_q\big(f(up+d_1)^{\delta_1} f(up+d_2)^{\delta_2}\big)\,\mathrm{e}\Big(\frac{au}{q}\Big)\\ &\qquad\times \sum_{v=0}^{p-1} \chi_p\big(f(vq+d_1)^{\delta_1} f(vq+d_2)^{\delta_2}\big)\,\mathrm{e}\Big(\frac{av}{p}\Big)\\ &\quad= \sum_{u=0}^{q-1} \chi_q\big(f(u+d_1)^{\delta_1} f(u+d_2)^{\delta_2}\big)\,\mathrm{e}\Big(\frac{ai_q(p)u}{q}\Big)\\ &\qquad\times \sum_{v=0}^{p-1} \chi_p(f(v+d_1)^{\delta_1} f(v+d_2)^{\delta_2})\,\mathrm{e}\Big(\frac{ai_p(q)v}{p}\Big).\end{aligned}$$

We consider three cases.

Case I: $d_1 \not\equiv d_2 \pmod p$ and $d_1 \not\equiv d_2 \pmod q$. From Lemmas 3.1 and 3.2 we get

$$\sum_{u=0}^{q-1} \chi_q\big(f(u+d_1)^{\delta_1} f(u+d_2)^{\delta_2}\big)\, \mathrm{e}\left(\frac{a i_q(p) u}{q}\right) \ll hq^{1/2},$$
$$\sum_{v=0}^{p-1} \chi_p\big(f(v+d_1)^{\delta_1} f(v+d_2)^{\delta_2}\big)\, \mathrm{e}\left(\frac{a i_p(q) v}{p}\right) \ll hp^{1/2}.$$

Then

$$\sum_{m=1}^{N} \chi^*\big(f(m+d_1)^{\delta_1} f(m+d_2)^{\delta_2}\big)\, \mathrm{e}\left(\frac{am}{N}\right) \ll h^2 N^{1/2}. \tag{4.3}$$

Case II: $d_1 \equiv d_2 \pmod p$ and $d_1 \not\equiv d_2 \pmod q$. By Lemmas 3.1 and 3.2 we get

$$\sum_{u=0}^{q-1} \chi_q\big(f(u+d_1)^{\delta_1} f(u+d_2)^{\delta_2}\big)\, \mathrm{e}\left(\frac{a i_q(p) u}{q}\right) \ll hq^{1/2}.$$

On the other hand, we easily have

$$\begin{aligned}
&\sum_{v=0}^{p-1} \chi_p\big(f(v+d_1)^{\delta_1} f(v+d_2)^{\delta_2}\big)\, \mathrm{e}\left(\frac{a i_p(q) v}{p}\right) \\
&\qquad = \sum_{v=0}^{p-1} \chi_p^{\delta_1+\delta_2}(f(v+d_1))\, \mathrm{e}\left(\frac{a i_p(q) v}{p}\right) \\
&\qquad = \begin{cases} O(hp^{1/2}) & \text{if } t_p \nmid \delta_1+\delta_2, \\ \displaystyle\sum_{v=0}^{p-1} \mathrm{e}\left(\frac{a i_p(q) v}{p}\right) + O(h) & \text{if } t_p \mid \delta_1+\delta_2, \end{cases} \\
&\qquad = \begin{cases} O(hp^{1/2}) & \text{if } t_p \nmid \delta_1+\delta_2, \\ O(h) & \text{if } t_p \mid \delta_1+\delta_2 \text{ and } p \nmid a, \\ p+O(h) & \text{if } t_p \mid \delta_1+\delta_2 \text{ and } p \mid a, \end{cases} \\
&\qquad = \begin{cases} O(p) & \text{if } t_p \mid \delta_1+\delta_2 \text{ and } p \mid a, \\ O(hp^{1/2}) & \text{otherwise.} \end{cases}
\end{aligned}$$

Therefore

$$\begin{aligned}
&\sum_{m=1}^{N} \chi^*\big(f(m+d_1)^{\delta_1} f(m+d_2)^{\delta_2}\big)\, \mathrm{e}\left(\frac{am}{N}\right) \\
&\qquad = \begin{cases} O(hN^{3/4}) & \text{if } t_p \mid \delta_1+\delta_2 \text{ and } p \mid a, \\ O(h^2 N^{1/2}) & \text{otherwise.} \end{cases}
\end{aligned} \tag{4.4}$$

Case III: $d_1 \not\equiv d_2 \pmod p$ and $d_1 \equiv d_2 \pmod q$. Using similar methods we obtain

$$\sum_{m=1}^{N} \chi^*\big(f(m+d_1)^{\delta_1} f(m+d_2)^{\delta_2}\big)\,\mathrm{e}\Big(\frac{am}{N}\Big) = \begin{cases} O(hN^{3/4}) & \text{if } t_q \mid \delta_1+\delta_2 \text{ and } q \mid a,\\ O(h^2N^{1/2}) & \text{otherwise.}\end{cases} \tag{4.5}$$

Now combining (4.2)–(4.5) we immediately get

$$\begin{aligned}\sum_{m=1}^{M} \chi_1(f(m+d_1))\chi_2(f(m+d_2)) &\ll \frac{1}{N}\sum_{|a|<N/2}\Big|\sum_{u=1}^{M}\mathrm{e}\Big(-\frac{au}{N}\Big)\Big|\cdot h^2N^{1/2}\\ &\quad+\frac{1}{N}\sum_{\substack{|a|<N/2\\ p\mid a}}\Big|\sum_{u=1}^{M}\mathrm{e}\Big(-\frac{au}{N}\Big)\Big|\cdot hN^{3/4}+\frac{1}{N}\sum_{\substack{|a|<N/2\\ q\mid a}}\Big|\sum_{u=1}^{M}\mathrm{e}\Big(-\frac{au}{N}\Big)\Big|\cdot hN^{3/4}\\ &\ll \frac{1}{N}\Big(M+\sum_{1\le a<N/2}\frac{N}{a}\Big)\cdot h^2N^{1/2}+\frac{1}{N}\Big(M+\sum_{\substack{1\le a<N/2\\ p\mid a}}\frac{N}{a}\Big)\cdot hN^{3/4}\\ &\quad+\frac{1}{N}\Big(M+\sum_{\substack{1\le a<N/2\\ q\mid a}}\frac{N}{a}\Big)\cdot hN^{3/4}\\ &\ll hN^{3/4}.\end{aligned} \tag{4.6}$$

Then from (4.1), (4.6) and Theorem 3.1 we have

$$\begin{aligned}&|g(E_N,w,M,D)-M/k^2|\\ &\quad\ll \frac{1}{d^2}\sum_{\chi_1\in\mathcal{H}^*}\Big|\sum_{\substack{i=0\\ i\equiv a_{i_1}\,(\mathrm{mod}\,k)}}^{d-1}\overline{\chi}_1(x^i)\Big|\sum_{\chi_2\in\mathcal{H}^*}\Big|\sum_{\substack{j=0\\ j\equiv a_{i_2}\,(\mathrm{mod}\,k)}}^{d-1}\overline{\chi}_2(x^j)\Big|\cdot hN^{3/4}\\ &\qquad+h^2N^{1/2}\log N\\ &\quad\ll hN^{3/4}.\end{aligned}$$

Therefore $\gamma_2(E_N) \ll hN^{3/4}$. This proves (1.2).

For all $w=(a_{i_1},a_{i_2},a_{i_3}) \in \mathbb{Z}_k^3$ and $D=(d_1,d_2,d_3)$ with $0 \le d_1 < d_2 < d_3 < N-M$, by (3.1) and the methods used in proving (1.2) we have

$$
\begin{aligned}
(4.7)\quad & g(E_N, w, M, D) \\
&= |\{m : 1 \le m \le M, e_{m+d_1} = a_{i_1}, e_{m+d_2} = a_{i_2}, e_{m+d_3} = a_{i_3}\}| \\
&= \sum_{\substack{m=1 \\ f(m+d_1)\in\mathbb{Z}_N^* \\ f(m+d_2)\in\mathbb{Z}_N^* \\ f(m+d_3)\in\mathbb{Z}_N^* \\ e_{m+d_s}=a_{i_s},\, s=1,2,3}}^{M} 1 + O(hN^{1/2}) = \sum_{i=0}^{d-1}\sum_{j=0}^{d-1}\sum_{r=0}^{d-1} \sum_{\substack{m=1 \\ f(m+d_1)\in D_i \\ f(m+d_2)\in D_j \\ f(m+d_3)\in D_r \\ e_{m+d_s}=a_{i_s},\, s=1,2,3}}^{M} 1 + O(hN^{1/2}) \\
&= \frac{1}{d^3} \sum_{i\equiv a_{i_1} \pmod k}^{d-1} \sum_{j\equiv a_{i_2} \pmod k}^{d-1} \sum_{r\equiv a_{i_3} \pmod k}^{d-1} \sum_{m=1}^{M} \\
&\qquad \times \sum_{\chi_1\in\mathcal{H}} \overline{\chi}_1(x^i)\chi_1(f(m+d_1)) \sum_{\chi_2\in\mathcal{H}} \overline{\chi}_2(x^j)\chi_2(f(m+d_2)) \\
&\qquad \times \sum_{\chi_3\in\mathcal{H}} \overline{\chi}_3(x^r)\chi_3(f(m+d_3)) + O(hN^{1/2}) \\
&= \frac{M}{k^3} + \frac{1}{d^3} \sum_{\chi_1\in\mathcal{H}^*} \Bigg(\sum_{i\equiv a_{i_1} \pmod k}^{d-1} \overline{\chi}_1(x^i) \Bigg) \sum_{\chi_2\in\mathcal{H}^*} \Bigg(\sum_{j\equiv a_{i_2} \pmod k}^{d-1} \overline{\chi}_2(x^j) \Bigg) \\
&\qquad \times \sum_{\chi_3\in\mathcal{H}^*} \Bigg(\sum_{r\equiv a_{i_3} \pmod k}^{d-1} \overline{\chi}_3(x^r) \Bigg) \\
&\qquad \times \sum_{m=1}^{M} \chi_1(f(m+d_1))\chi_2(f(m+d_2))\chi_3(f(m+d_3)) \\
&\quad + O(hN^{3/4}).
\end{aligned}
$$

There exists $\chi^* \in \mathcal{H}^*$ such that

$$
\begin{aligned}
&\chi_1 = (\chi^*)^{\delta_1}, \quad \chi_2 = (\chi^*)^{\delta_2}, \quad \chi_3 = (\chi^*)^{\delta_3}, \\
&1 \le \delta_1, \delta_2, \delta_3 \le d-1, \quad (\delta_1, \delta_2, \delta_3) = 1.
\end{aligned}
$$

Then we get

$$
\begin{aligned}
(4.8)\quad & \sum_{m=1}^{M} \chi_1(f(m+d_1))\chi_2(f(m+d_2))\chi_3(f(m+d_3)) \\
&= \sum_{m=1}^{M} \chi^*\big(f(m+d_1)^{\delta_1} f(m+d_2)^{\delta_2} f(m+d_3)^{\delta_3}\big) \\
&= \frac{1}{N} \sum_{m=1}^{N} \chi^*\big(f(m+d_1)^{\delta_1} f(m+d_2)^{\delta_2} f(m+d_3)^{\delta_3}\big) \sum_{u=1}^{M} \sum_{|a|<N/2} \mathrm{e}\Big(\frac{a(m-u)}{N}\Big)
\end{aligned}
$$

$$= \frac{1}{N} \sum_{|a|<N/2} \sum_{u=1}^{M} \mathrm{e}\Big(-\frac{au}{N}\Big) \times \sum_{m=1}^{N} \chi^*\big(f(m+d_1)^{\delta_1} f(m+d_2)^{\delta_2} f(m+d_3)^{\delta_3}\big)\, \mathrm{e}\Big(\frac{am}{N}\Big).$$

Write $\chi^* = \chi_p \chi_q$ with χ_p a character modulo p of order $t_p > 1$ and χ_q a character modulo q of order $t_q > 1$, where t_p, t_q are divisors of d. We have

$$\begin{aligned}
&\sum_{m=1}^{N} \chi^*\big(f(m+d_1)^{\delta_1} f(m+d_2)^{\delta_2} f(m+d_3)^{\delta_3}\big)\, \mathrm{e}\Big(\frac{am}{N}\Big) \\
&\quad = \sum_{u=0}^{q-1} \sum_{v=0}^{p-1} \chi^*\big(f(up+vq+d_1)^{\delta_1} f(up+vq+d_2)^{\delta_2} f(up+vq+d_3)^{\delta_3}\big) \\
&\qquad\qquad \times \mathrm{e}\Big(\frac{a(up+vq)}{N}\Big) \\
&\quad = \sum_{u=0}^{q-1} \chi_q\big(f(up+d_1)^{\delta_1} f(up+d_2)^{\delta_2} f(up+d_3)^{\delta_3}\big)\, \mathrm{e}\Big(\frac{au}{q}\Big) \\
&\qquad\qquad \times \sum_{v=0}^{p-1} \chi_p\big(f(vq+d_1)^{\delta_1} f(vq+d_2)^{\delta_2} f(vq+d_3)^{\delta_3}\big)\, \mathrm{e}\Big(\frac{av}{p}\Big) \\
&\quad = \sum_{u=0}^{q-1} \chi_q\big(f(u+d_1)^{\delta_1} f(u+d_2)^{\delta_2} f(u+d_3)^{\delta_3}\big)\, \mathrm{e}\Big(\frac{ai_q(p)u}{q}\Big) \\
&\qquad\qquad \times \sum_{v=0}^{p-1} \chi_p(f(v+d_1)^{\delta_1} f(v+d_2)^{\delta_2} f(v+d_3)^{\delta_3})\, \mathrm{e}\Big(\frac{ai_p(q)v}{p}\Big).
\end{aligned}$$

Using the methods applied in proving (1.2) we get

$$\sum_{m=1}^{N} \chi^*\big(f(m+d_1)^{\delta_1} f(m+d_2)^{\delta_2} f(m+d_3)^{\delta_3}\big)\, \mathrm{e}\Big(\frac{am}{N}\Big) = \begin{cases} O(hN^{3/4}) & \text{if } p \mid a \text{ or } q \mid a, \\ O(h^2 N^{1/2}) & \text{otherwise.} \end{cases} \tag{4.9}$$

So from (4.8), (4.9) and Theorem 3.1 we have

$$\begin{aligned}
&\sum_{m=1}^{M} \chi_1(f(m+d_1))\chi_2(f(m+d_2))\chi_3(f(m+d_3)) \\
&\ll \frac{1}{N} \sum_{|a|<N/2} \Big|\sum_{u=1}^{M} \mathrm{e}\Big(-\frac{au}{N}\Big)\Big| \cdot h^2 N^{1/2} \\
&\quad + \frac{1}{N} \sum_{\substack{|a|<N/2 \\ p \mid a}} \Big|\sum_{u=1}^{M} \mathrm{e}\Big(-\frac{au}{N}\Big)\Big| \cdot hN^{3/4} + \frac{1}{N} \sum_{\substack{|a|<N/2 \\ q \mid a}} \Big|\sum_{u=1}^{M} \mathrm{e}\Big(-\frac{au}{N}\Big)\Big| \cdot hN^{3/4}
\end{aligned} \tag{4.10}$$

$$\ll \frac{1}{N}\Bigg(M + \sum_{1\le a<N/2} \frac{N}{a}\Bigg)\cdot h^2N^{1/2} + \frac{1}{N}\Bigg(M + \sum_{\substack{1\le a<N/2\\ p\mid a}} \frac{N}{a}\Bigg)\cdot hN^{3/4}$$
$$+ \frac{1}{N}\Bigg(M + \sum_{\substack{1\le a<N/2\\ q\mid a}} \frac{N}{a}\Bigg)\cdot hN^{3/4}$$
$$\ll hN^{3/4}.$$

Now combining (4.7) and (4.10) we get

$$|g(E_N, w, M, D) - M/k^3|$$
$$\ll \frac{1}{d^3}\sum_{\chi_1\in\mathcal{H}^*}\Bigg|\sum_{\substack{i=0\\ i\equiv a_{i_1}\,(\mathrm{mod}\,k)}}^{d-1}\overline{\chi}_1(x^i)\Bigg|\sum_{\chi_2\in\mathcal{H}^*}\Bigg|\sum_{\substack{j=0\\ j\equiv a_{i_2}\,(\mathrm{mod}\,k)}}^{d-1}\overline{\chi}_2(x^j)\Bigg|$$
$$\times\sum_{\chi_3\in\mathcal{H}^*}\Bigg|\sum_{\substack{r=0\\ r\equiv a_{i_3}\,(\mathrm{mod}\,k)}}^{d-1}\overline{\chi}_3(x^r)\Bigg|\cdot hN^{3/4} + hN^{3/4}$$
$$\ll hN^{3/4}.$$

Therefore $\gamma_3(E_N) \ll hN^{3/4}$. This completes the proof of (1.3). Similarly we can get (1.4) and (1.5).

5. The correlation measure of order 4 of E_N. Take $w = (0,0,0,0) \in \mathbb{Z}_k^4$, $D = (d_1, d_2, d_3, d_4)$ and M satisfying

$$d_1 = 0, \quad d_2 = p, \quad d_3 = q, \quad d_4 = p+q, \quad M = N - p - q.$$

By (3.1) and the methods in proving (1.3) we have

(5.1) $g(E_N, w, M, D)$
$= |\{m : 1 \le m \le N-p-q,\, e_m = 0,\, e_{m+p} = 0,\, e_{m+q} = 0,\, e_{m+p+q} = 0\}|$
$$= \sum_{\substack{m=1\\ f(m)\in\mathbb{Z}_N^*\\ f(m+p)\in\mathbb{Z}_N^*\\ f(m+q)\in\mathbb{Z}_N^*\\ f(m+p+q)\in\mathbb{Z}_N^*\\ e_m=0\\ e_{m+p}=0\\ e_{m+q}=0\\ e_{m+p+q}=0}}^{N-p-q} 1 + O(hN^{1/2}) = \sum_{j_1=0}^{d-1}\sum_{j_2=0}^{d-1}\sum_{j_3=0}^{d-1}\sum_{j_4=0}^{d-1}\sum_{\substack{m=1\\ f(m)\in D_{j_1}\\ f(m+p)\in D_{j_2}\\ f(m+q)\in D_{j_3}\\ f(m+p+q)\in D_{j_4}\\ e_m=0\\ e_{m+p}=0\\ e_{m+q}=0\\ e_{m+p+q}=0}}^{N-p-q} 1 + O(hN^{1/2})$$

$$= \frac{1}{d^4} \sum_{\substack{j_1=0 \\ j_1\equiv 0 \,(\mathrm{mod}\, k)}}^{d-1} \sum_{\substack{j_2=0 \\ j_2\equiv 0 \,(\mathrm{mod}\, k)}}^{d-1} \sum_{\substack{j_3=0 \\ j_3\equiv 0 \,(\mathrm{mod}\, k)}}^{d-1} \sum_{\substack{j_4=0 \\ j_4\equiv 0 \,(\mathrm{mod}\, k)}}^{d-1}$$
$$\times \sum_{m=1}^{N-p-q} \sum_{\chi_1\in\mathcal{H}} \overline{\chi}_1(x^{j_1})\chi_1(f(m)) \sum_{\chi_2\in\mathcal{H}} \overline{\chi}_2(x^{j_2})\chi_2(f(m+p))$$
$$\times \sum_{\chi_3\in\mathcal{H}} \overline{\chi}_3(x^{j_3})\chi_3(f(m+q)) \sum_{\chi_4\in\mathcal{H}} \overline{\chi}_4(x^{j_4})\chi_4(f(m+p+q))$$
$$+ O(hN^{1/2})$$
$$= \frac{M}{k^4} + \frac{1}{d^4} \sum_{\chi_1\in\mathcal{H}^*} \Bigg(\sum_{\substack{j_1=0 \\ j_1\equiv 0 \,(\mathrm{mod}\, k)}}^{d-1} \overline{\chi}_1(x^{j_1}) \Bigg) \sum_{\chi_2\in\mathcal{H}^*} \Bigg(\sum_{\substack{j_2=0 \\ j_2\equiv 0 \,(\mathrm{mod}\, k)}}^{d-1} \overline{\chi}_2(x^{j_2}) \Bigg)$$
$$\times \sum_{\chi_3\in\mathcal{H}^*} \Bigg(\sum_{\substack{j_3=0 \\ j_3\equiv 0 \,(\mathrm{mod}\, k)}}^{d-1} \overline{\chi}_3(x^{j_3}) \Bigg) \sum_{\chi_4\in\mathcal{H}^*} \Bigg(\sum_{\substack{j_4=0 \\ j_4\equiv 0 \,(\mathrm{mod}\, k)}}^{d-1} \overline{\chi}_4(x^{j_4}) \Bigg)$$
$$\times \sum_{m=1}^{N-p-q} \chi_1(f(m))\chi_2(f(m+p))\chi_3(f(m+q))\chi_4(f(m+p+q))$$
$$+ O(hN^{3/4}).$$

Let $\chi' \in \mathcal{H}^*$ be a generator of $\mathcal{H}$. For $\chi_1, \chi_2, \chi_3, \chi_4 \in \mathcal{H}^*$, we write

$$\chi_1 = (\chi')^{b_1}, \quad \chi_2 = (\chi')^{b_2}, \quad \chi_3 = (\chi')^{b_3}, \quad \chi_4 = (\chi')^{b_4},$$

where $1 \le b_1, b_2, b_3, b_4 \le d-1$. Define

$$\chi^* = (\chi')^{(b_1,b_2,b_3,b_4)}, \quad \delta_i = \frac{b_i}{(b_1,b_2,b_3,b_4)}, \quad i = 1,2,3,4.$$

Then we have

$$\chi_1 = (\chi^*)^{\delta_1}, \quad \chi_2 = (\chi^*)^{\delta_2}, \quad \chi_3 = (\chi^*)^{\delta_3}, \quad \chi_4 = (\chi^*)^{\delta_4},$$
$$1 \le \delta_1, \delta_2, \delta_3, \delta_4 \le d-1, \quad (\delta_1, \delta_2, \delta_3, \delta_4) = 1.$$

Therefore

$$\sum_{m=1}^{N-p-q} \chi_1(f(m))\chi_2(f(m+p))\chi_3(f(m+q))\chi_4(f(m+p+q))$$
$$= \sum_{m=1}^{N-p-q} \chi^*\big(f(m)^{\delta_1} f(m+p)^{\delta_2} f(m+q)^{\delta_3} f(m+p+q)^{\delta_4}\big)$$

$$= \frac{1}{N} \sum_{|a|<N/2} \sum_{u=1}^{N-p-q} \mathrm{e}\Big(-\frac{au}{N}\Big) \times \sum_{m=1}^{N} \chi^*\big(f(m)^{\delta_1} f(m+p)^{\delta_2} f(m+q)^{\delta_3} f(m+p+q)^{\delta_4}\big)\, \mathrm{e}\Big(\frac{am}{N}\Big).$$

Write $\chi^* = \chi_p \chi_q$ with χ_p a character modulo p of order $t_p > 1$ and χ_q a character modulo q of order $t_q > 1$. Then

$$\sum_{m=1}^{N} \chi^*\big(f(m)^{\delta_1} f(m+p)^{\delta_2} f(m+q)^{\delta_3} f(m+p+q)^{\delta_4}\big)\, \mathrm{e}\Big(\frac{am}{N}\Big)$$
$$= \sum_{u=0}^{q-1} \chi_q\big(f(up)^{\delta_1} f(up+p)^{\delta_2} f(up)^{\delta_3} f(up+p)^{\delta_4}\big)\, \mathrm{e}\Big(\frac{au}{q}\Big) \times \sum_{v=0}^{p-1} \chi_p\big(f(vq)^{\delta_1} f(vq)^{\delta_2} f(vq+q)^{\delta_3} f(vq+q)^{\delta_4}\big)\, \mathrm{e}\Big(\frac{av}{p}\Big)$$
$$= \sum_{u=0}^{q-1} \chi_q\big(f(u)^{\delta_1+\delta_3} f(u+p)^{\delta_2+\delta_4}\big)\, \mathrm{e}\Big(\frac{ai_q(p)u}{q}\Big) \times \sum_{v=0}^{p-1} \chi_p\big(f(v)^{\delta_1+\delta_2} f(v+q)^{\delta_3+\delta_4}\big)\, \mathrm{e}\Big(\frac{ai_p(q)v}{p}\Big).$$

By Lemmas 2.1 and 2.2 we get

$$\sum_{u=0}^{q-1} \chi_q(f(u)^{\delta_1+\delta_3} f(u+p)^{\delta_2+\delta_4})\, \mathrm{e}\Big(\frac{ai_q(p)u}{q}\Big) = \begin{cases} q + O(h) & \text{if } t_q \mid \delta_1+\delta_3,\ t_q \mid \delta_2+\delta_4 \text{ and } q \mid a, \\ O(hq^{1/2}) & \text{otherwise,} \end{cases}$$

$$\sum_{v=0}^{p-1} \chi_p(f(v)^{\delta_1+\delta_2} f(v+q)^{\delta_3+\delta_4})\, \mathrm{e}\Big(\frac{ai_p(q)v}{p}\Big) = \begin{cases} p + O(h) & \text{if } t_p \mid \delta_1+\delta_2,\ t_p \mid \delta_3+\delta_4 \text{ and } p \mid a, \\ O(hp^{1/2}) & \text{otherwise.} \end{cases}$$

Then we have

$$\sum_{m=1}^{N} \chi^*(f(m)^{\delta_1} f(m+p)^{\delta_2} f(m+q)^{\delta_3} f(m+p+q)^{\delta_4})\, \mathrm{e}\Big(\frac{am}{N}\Big) = \begin{cases} N + O(hN^{1/2}) & \text{if } t_p \mid \delta_1+\delta_2,\ t_p \mid \delta_3+\delta_4,\ t_q \mid \delta_1+\delta_3,\ t_q \mid \delta_2+\delta_4 \\ & \qquad\qquad \text{and } N \mid a, \\ O(hN^{3/4}) & \text{otherwise.} \end{cases}$$

Write $t = \operatorname{ord} \chi^*$. We get

$$t = d/(b_1, b_2, b_3, b_4).$$

Furthermore, from Theorem 3.1 we know that $t = t_p = t_q$. It is easy to show that

$$\begin{aligned} t_p \,|\, \delta_1 + \delta_2 \;&\Leftrightarrow\; \frac{d}{(b_1, b_2, b_3, b_4)} \,\Big|\, \frac{b_1}{(b_1, b_2, b_3, b_4)} + \frac{b_2}{(b_1, b_2, b_3, b_4)} \\ &\Leftrightarrow\; d \,|\, b_1 + b_2 \;\Leftrightarrow\; \chi_1 = \overline{\chi}_2. \end{aligned}$$

Similarly,

$$t_p \,|\, \delta_3 + \delta_4 \;\Leftrightarrow\; \chi_3 = \overline{\chi}_4, \quad t_q \,|\, \delta_1 + \delta_3 \;\Leftrightarrow\; \chi_1 = \overline{\chi}_3, \quad t_q \,|\, \delta_2 + \delta_4 \;\Leftrightarrow\; \chi_2 = \overline{\chi}_4.$$

Therefore

$$\begin{aligned} (5.2)\qquad &\sum_{m=1}^{N-p-q} \chi_1(f(m))\chi_2(f(m+p))\chi_3(f(m+q))\chi_4(f(m+p+q)) \\ &\qquad = \begin{cases} N + O(hN^{1/2}) & \text{if } \chi_2 = \overline{\chi}_1,\ \chi_3 = \overline{\chi}_1,\ \chi_4 = \chi_1, \\ hN^{3/4} \log N & \text{otherwise.} \end{cases} \end{aligned}$$

Now from (5.1), (5.2) and Theorem 3.1 we obtain

$$\begin{aligned} g(E_N, w, M, D) - \frac{M}{k^4} &= \frac{N}{d^4} \sum_{\chi \in \mathcal{H}^*} \Big| \sum_{\substack{j=0 \\ j \equiv 0 \,(\mathrm{mod}\, k)}}^{d-1} \chi(x^j) \Big|^4 + O(hN^{3/4} \log N) \\ &= \frac{k-1}{k^4} N + O(hN^{3/4} \log N). \end{aligned}$$

This completes the proof of Theorem 1.3.

6. Collisions and avalanche effects. We further study the structure of our family of sequences of k symbols. Collisions and avalanche effects are important notions in cryptography, and can be adapted in the following way (see [15]).

Assume that $\mathcal{A} = \{a_1, \ldots, a_k\}$ is a finite set of k symbols, and $\mathcal{S}$ is a given set (e.g., a set of certain polynomials). To each $s \in \mathcal{S}$ we assign a unique sequence of k symbols

$$E_N = E_N(s) = (e_1, \ldots, e_N) \in \mathcal{A}^N,$$

and let $\mathcal{F} = \mathcal{F}(\mathcal{S})$ denote the family of the sequences of k symbols obtained in this way:

$$(6.1)\qquad \mathcal{F} = \mathcal{F}(\mathcal{S}) = \{E_N(s) : s \in \mathcal{S}\}.$$

Definition 6.1. If $s, s' \in \mathcal{S}, s \neq s'$ and

$$(6.2)\qquad E_N(s) = E_N(s'),$$

then (6.2) is said to be a *collision* in $\mathcal{F} = \mathcal{F}(\mathcal{S})$. If there is no collision in $\mathcal{F} = \mathcal{F}(\mathcal{S})$, then $\mathcal{F}$ is said to be *collision free*.

DEFINITION 6.2. The *collision maximum* $M = M(\mathcal{F}, \mathcal{S})$ is defined by

$$M = M(\mathcal{F}, \mathcal{S}) = \max_{E_N \in \mathcal{F}} |\{s : s \in \mathcal{S} : E_N(s) = E_N\}|.$$

An ideally good family of pseudorandom sequences of k symbols is collision free. If $\mathcal{F}$ is not collision free but the number of collisions is limited, they do not cause many problems.

DEFINITION 6.3. If for any distinct $s, s' \in \mathcal{S}$ many elements of the sequences $E_N(s)$ and $E_N(s')$ are different, then we speak about the *avalanche effect*, and we say that $\mathcal{F} = \mathcal{F}(\mathcal{S})$ has the *avalanche property*. If for any distinct $s, s' \in \mathcal{S}$ at least $((k-1)/k - o(1))N$ elements of $E_N(s)$ and $E_N(s')$ are different then $\mathcal{F}$ is said to have the *strict avalanche property*.

To study collisions and avalanche effects, we introduce the following measure:

DEFINITION 6.4. If $E_N = (e_1, \dots, e_N)$, $E'_N = (e'_1, \dots, e'_N) \in \mathcal{A}^N$, then their distance is defined by

$$d(E_N, E'_N) = |\{n : 1 \le n \le N,\, e_n \ne e'_n\}|.$$

Moreover, if $\mathcal{F}$ is a family from (6.1), then the *distance minimum* of $\mathcal{F}$ is defined by

$$m(\mathcal{F}) = \min_{\substack{s,s' \in \mathcal{S} \\ s \ne s'}} d(E_N(s), E_N(s')).$$

It is not hard to show that the family $\mathcal{F}$ in (6.1) is collision free if and only if $m(\mathcal{F}) > 0$, and $\mathcal{F}$ has the strict avalanche property if

$$m(\mathcal{F}) \ge \left(\frac{k-1}{k} - o(1)\right)N.$$

Now we prove the following results.

THEOREM 6.1. *Let $\mathcal{T} \subset \mathbb{Z}[x]$ be a set of monic polynomials of degree $\le D$. Assume that, for any $f(x) \in \mathcal{T}$, $f(x)$ as a polynomial over $\mathbb{F}_p$ has no multiple roots in $\overline{\mathbb{F}}_p$, and $f(x)$ as a polynomial over $\mathbb{F}_q$ has no multiple roots in $\overline{\mathbb{F}}_q$. Suppose that $k > 1$ and $k \mid d = (p-1, q-1)$. Define $E_N(f) = (e_1, \dots, e_N) \in \mathbb{Z}_k^N$ by*

$$e_n = \begin{cases} i \pmod k & \text{if } f(n) \in D_i,\ 0 \le i \le d-1, \\ A & \text{if } f(n) \in P, \\ B & \text{if } f(n) \in Q_0, \end{cases}$$

for $n = 1, \dots, N$ and fixed $A, B \in \mathbb{Z}_k$, and set

$$\mathcal{F} = \mathcal{F}(\mathcal{T}) = \{E_N(f) : f \in \mathcal{T}\}.$$

Then

$$m(\mathcal{F}) \geq \frac{k-1}{k}(N - (5D + 4D^2)N^{1/2}).$$

If $D < \frac{1}{3}N^{1/4}$, then

$$m(\mathcal{F}) \geq \frac{k-1}{k}(N - (5D + 4D^2)N^{1/2}) > 0.$$

If $D = o(N^{1/4})$, then Theorem 6.1 gives

$$m(\mathcal{F}) \geq \left(\frac{k-1}{k} - o(1)\right)N.$$

So we immediately get the following corollaries.

COROLLARY 6.1. *If $\mathcal{T}$, $\mathcal{F}$ are defined as in Theorem* 6.1 *and $D < \frac{1}{3}N^{1/4}$, then $\mathcal{F}$ is collision free.*

COROLLARY 6.2. *If $\mathcal{T}$, $\mathcal{F}$ are defined as in Theorem* 6.1 *and $D = o(N^{1/4})$, then $\mathcal{F}$ has the strict avalanche property.*

Now we prove Theorem 6.1. For distinct $f, g \in \mathcal{T}$, by (3.1) we get

$$\begin{aligned}
(6.3)\qquad d(E_N(f), E_N(g)) &= |\{n : 1 \leq n \leq N,\, e_n^{(f)} \neq e_n^{(g)}\}| \\
&= \sum_{\substack{n=1 \\ e_n^{(f)} \neq e_n^{(g)} \\ (f(n)g(n),N)=1}}^{N} 1 + \sum_{\substack{n=1 \\ e_n^{(f)} \neq e_n^{(g)} \\ (f(n)g(n),N)>1}}^{N} 1 \\
&= \sum_{\substack{i=0 \\ i \not\equiv j \,(\mathrm{mod}\, k)}}^{d-1} \sum_{j=0}^{d-1} \sum_{\substack{n=1 \\ f(n) \in D_i \\ g(n) \in D_j}}^{N} 1 + \sum_{\substack{n=1 \\ e_n^{(f)} \neq e_n^{(g)} \\ (f(n)g(n),N)>1}}^{N} 1 \\
&= \frac{1}{d^2} \sum_{\substack{i=0 \\ i \not\equiv j \,(\mathrm{mod}\, k)}}^{d-1} \sum_{j=0}^{d-1} \sum_{n=1}^{N} \sum_{\chi_1 \in \mathcal{H}} \overline{\chi}_1(x^i)\chi_1(f(n)) \sum_{\chi_2 \in \mathcal{H}} \overline{\chi}_2(x^j)\chi_2(g(n)) \\
&\quad + \sum_{\substack{n=1 \\ e_n^{(f)} \neq e_n^{(g)} \\ (f(n)g(n),N)>1}}^{N} 1
\end{aligned}$$

$$= \frac{1}{d^2} \sum_{\substack{i=0 \\ i\not\equiv j \,(\mathrm{mod}\, k)}}^{d-1} \sum_{j=0}^{d-1} \sum_{\substack{n=1 \\ (f(n)g(n),N)=1}}^{N} 1 + \sum_{\substack{n=1 \\ e_n^{(f)} \neq e_n^{(g)} \\ (f(n)g(n),N)>1}}^{N} 1$$

$$+ \frac{1}{d^2} \sum_{\substack{i=0 \\ i\not\equiv j \,(\mathrm{mod}\, k)}}^{d-1} \sum_{j=0}^{d-1} \sum_{\substack{n=1 \\ (g(n),N)=1}}^{N} \sum_{\chi_1 \in \mathcal{H}^*} \overline{\chi}_1(x^i)\chi_1(f(n))$$

$$+ \frac{1}{d^2} \sum_{\substack{i=0 \\ i\not\equiv j \,(\mathrm{mod}\, k)}}^{d-1} \sum_{j=0}^{d-1} \sum_{\substack{n=1 \\ (f(n),N)=1}}^{N} \sum_{\chi_2 \in \mathcal{H}^*} \overline{\chi}_2(x^j)\chi_2(g(n))$$

$$+ \frac{1}{d^2} \sum_{\substack{i=0 \\ i\not\equiv j \,(\mathrm{mod}\, k)}}^{d-1} \sum_{j=0}^{d-1} \sum_{n=1}^{N} \sum_{\chi_1 \in \mathcal{H}^*} \overline{\chi}_1(x^i)\chi_1(f(n)) \sum_{\chi_2 \in \mathcal{H}^*} \overline{\chi}_2(x^j)\chi_2(g(n)).$$

It is not hard to show that

$$\frac{1}{d^2} \sum_{\substack{i=0 \\ i\not\equiv j \,(\mathrm{mod}\, k)}}^{d-1} \sum_{j=0}^{d-1} \sum_{\substack{n=1 \\ (f(n)g(n),N)=1}}^{N} 1 + \sum_{\substack{n=1 \\ e_n^{(f)} \neq e_n^{(g)} \\ (f(n)g(n),N)>1}}^{N} 1 \tag{6.4}$$

$$= \frac{N}{d^2} \sum_{\substack{i=0 \\ i\not\equiv j \,(\mathrm{mod}\, k)}}^{d-1} \sum_{j=0}^{d-1} 1 - \frac{1}{d^2} \sum_{\substack{i=0 \\ i\not\equiv j \,(\mathrm{mod}\, k)}}^{d-1} \sum_{j=0}^{d-1} \sum_{\substack{n=1 \\ (f(n)g(n),N)>1}}^{N} 1 + \sum_{\substack{n=1 \\ e_n^{(f)} \neq e_n^{(g)} \\ (f(n)g(n),N)>1}}^{N} 1$$

$$\geq \frac{k-1}{k} N - 2D(p+q-1)\frac{k-1}{k} \geq \frac{k-1}{k}(N - 5DN^{1/2}).$$

On the other hand, from Theorem 3.1 we have

$$\frac{1}{d^2} \sum_{\substack{i=0 \\ i\not\equiv j \,(\mathrm{mod}\, k)}}^{d-1} \sum_{j=0}^{d-1} \sum_{\substack{n=1 \\ (g(n),N)=1}}^{N} \sum_{\chi_1 \in \mathcal{H}^*} \overline{\chi}_1(x^i)\chi_1(f(n)) \tag{6.5}$$

$$= \frac{1}{d}\left(1 - \frac{1}{k}\right) \sum_{\chi_1 \in \mathcal{H}^*} \sum_{i=0}^{d-1} \overline{\chi}_1(x^i) \sum_{\substack{n=1 \\ (g(n),N)=1}}^{N} \chi_1(f(n))$$

$$\ll \frac{1}{d}\left(1 - \frac{1}{k}\right) \sum_{\chi_1 \in \mathcal{H}^*} \left|\sum_{i=0}^{d-1} \overline{\chi}_1(x^i)\right| \cdot \left| \sum_{\substack{n=1 \\ (g(n),N)=1}}^{N} \chi_1(f(n))\right| = 0,$$

and

$$\frac{1}{d^2}\sum_{\substack{i=0\\ i\not\equiv j \,(\mathrm{mod}\, k)}}^{d-1}\sum_{j=0}^{d-1}\sum_{\substack{n=1\\ (f(n),N)=1}}^{N}\sum_{\chi_2\in\mathcal{H}^*}\overline{\chi}_2(x^j)\chi_2(g(n)) \tag{6.6}$$

$$= \frac{1}{d}\Big(1-\frac{1}{k}\Big)\sum_{\chi_2\in\mathcal{H}^*}\sum_{j=0}^{d-1}\overline{\chi}_2(x^j)\sum_{\substack{n=1\\ (f(n),N)=1}}^{N}\chi_2(g(n))$$

$$\ll \frac{1}{d}\Big(1-\frac{1}{k}\Big)\sum_{\chi_2\in\mathcal{H}^*}\Big|\sum_{j=0}^{d-1}\overline{\chi}_2(x^j)\Big|\cdot\Big|\sum_{\substack{n=1\\ (f(n),N)=1}}^{N}\chi_2(g(n))\Big| = 0.$$

Let $\chi'\in\mathcal{H}^*$ be a generator of $\mathcal{H}$. For $\chi_1,\chi_2\in\mathcal{H}^*$, write

$$\chi_1=(\chi')^{b_1},\quad \chi_2=(\chi')^{b_2},\quad 1\le b_1,b_2\le d-1.$$

Then

$$\sum_{n=1}^{N}\chi_1(f(n))\chi_2(g(n))=\sum_{n=1}^{N}\chi'\big(f(n)^{b_1}g(n)^{b_2}\big).$$

Write $\chi'=\chi_p\chi_q$ with χ_p a character modulo p and χ_q a character modulo q. From Theorem 3.1 we know that $\operatorname{ord}\chi_p=\operatorname{ord}\chi_q=\operatorname{ord}\chi'=d$. We have

$$\begin{aligned}\sum_{n=1}^{N}\chi_1(f(n))\chi_2(g(n)) &= \sum_{u=0}^{q-1}\sum_{v=0}^{p-1}\chi'\big(f(up+vq)^{b_1}g(up+vq)^{b_2}\big)\\ &= \sum_{u=0}^{q-1}\chi_q\big(f(up+vq)^{b_1}g(up+vq)^{b_2}\big)\sum_{v=0}^{p-1}\chi_p\big(f(up+vq)^{b_1}g(up+vq)^{b_2}\big)\\ &= \sum_{u=0}^{q-1}\chi_q\big(f(up)^{b_1}g(up)^{b_2}\big)\sum_{v=0}^{p-1}\chi_p\big(f(vq)^{b_1}g(vq)^{b_2}\big)\\ &= \sum_{u=0}^{q-1}\chi_q\big(f(u)^{b_1}g(u)^{b_2}\big)\sum_{v=0}^{p-1}\chi_p\big(f(v)^{b_1}g(v)^{b_2}\big).\end{aligned}$$

Since $f,g\in\mathcal{T}$ are distinct, $f^{b_1}g^{b_2}$ has at least one zero of order b_1 or b_2. Thus by Lemma 2.1 we get

$$\Big|\sum_{n=1}^{N}\chi_1(f(n))\chi_2(g(n))\Big|\le 4D^2N^{1/2}.$$

Then from Theorem 3.1 we have

$$(6.7)\quad \Bigg|\frac{1}{d^2}\sum_{\substack{i=0\\ i\not\equiv j\,(\mathrm{mod}\,k)}}^{d-1}\sum_{j=0}^{d-1}\sum_{n=1}^{N}\sum_{\chi_1\in\mathcal{H}^*}\overline{\chi}_1(x^i)\chi_1(f(n))\sum_{\chi_2\in\mathcal{H}^*}\overline{\chi}_2(x^j)\chi_2(g(n))\Bigg|$$

$$\le \frac{1}{d^2}\sum_{\chi_1\in\mathcal{H}^*}\sum_{\chi_2\in\mathcal{H}^*}\Bigg|\sum_{i=0}^{d-1}\overline{\chi}_1(x^i)\sum_{\substack{j=0\\ j\not\equiv i\,(\mathrm{mod}\,k)}}^{d-1}\overline{\chi}_2(x^j)\Bigg|\cdot\Bigg|\sum_{n=1}^{N}\chi_1(f(n))\chi_2(g(n))\Bigg|$$

$$\le 4D^2N^{1/2}\frac{k-1}{k}.$$

Now combining (6.3)–(6.7) we immediately get

$$d(E_N(f),E_N(g))\ge\frac{k-1}{k}(N-(5D+4D^2)N^{1/2}).$$

Therefore

$$m(\mathcal{F})=\min_{\substack{f,g\in\mathcal{T}\\ f\ne g}}d(E_N(f),E_N(g))\ge\frac{k-1}{k}(N-(5D+4D^2)N^{1/2}).$$

This proves Theorem 6.1.

Acknowledgements. The authors express their gratitude to the referee for helpful and detailed comments.

This research was supported by the National Natural Science Foundation of China (grant no. 11571277), and the Science and Technology Program of Shaanxi Province of China (grant nos. 2014KJXX-61, 2016GY-080 and 2016GY-077).

References

[1] R. Ahlswede, C. Mauduit and Sárközy, *Large families of pseudorandom sequences of k symbols and their complexity. I*, in: General Theory of Information Transfer and Combinatorics, Lecture Notes in Comput. Sci. 4123, Springer, Berlin, 2006, 293–307.

[2] R. Ahlswede, C. Mauduit and Sárközy, *Large families of pseudorandom sequences of k symbols and their complexity. II*, in: General Theory of Information Transfer and Combinatorics, Lecture Notes in Comput. Sci. 4123, Springer, Berlin, 2006, 308–325.

[3] N. Brandstätter and A. Winterhof, *Some notes on the two-prime generator of order 2*, IEEE Trans. Inform. Theory 51 (2005), 3654–3657.

[4] Z. Chen, *Large families of pseudo-random subsets formed by generalized cyclotomic classes*, Monatsh. Math. 161 (2010), 161–172.

[5] Z. Chen, X. Du and C. Wu, *Pseudorandomness of certain sequences of k symbols with length pq*, J. Comput. Sci. Tech. 26 (2011), 276–282.

[6] Z. Chen and S. Li, *Some notes on generalized cyclotomic sequences of length pq*, J. Comput. Sci. Tech. 23 (2008), 843–850.

[7] C. Dartyge and A. Sárközy, *Large families of pseudorandom subsets formed by power residues*, Unif. Distrib. Theory 2 (2007), no. 2, 73–88.
[8] C. Ding, *Linear complexity of generalized cyclotomic binary sequences of order 2*, Finite Fields Appl. 3 (1997), 159–174.
[9] D. Gomez and A. Winterhof, *Multiplicative character sums of Fermat quotients and pseudorandom sequences*, Period. Math. Hungar. 64 (2012), 161–168.
[10] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983.
[11] H. Liu and E. Song, *A note on pseudorandom subsets formed by generalized cyclotomic classes*, Publ. Math. Debrecen 85 (2014), 257–271.
[12] K. Mak, *More constructions of pseudorandom sequences of k symbols*, Finite Fields Appl. 25 (2014), 222–233.
[13] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol*, Acta Arith. 82 (1997), 365–377.
[14] C. Mauduit and A. Sárközy, *On finite pseudorandom sequences of k symbols*, Indag. Math. (N.S.) 13 (2002), 89–101.
[15] V. Tóth, *Extension of the notion of collision and avalanche effect to sequences of k symbols*, Period. Math. Hungar. 65 (2012), 229–238.
[16] A. L. Whiteman, *A family of difference sets*, Illinois J. Math. 6 (1962), 107–121.

Huaning Liu, Bo Gao
School of Mathematics
Northwest University
Xi'an 710127, Shaanxi, China
E-mail: hnliumath@hotmail.com
bogaomath@163.com