Publ. Math. Debrecen
85/3-4 (2014), 257–271
DOI: 10.5486/PMD.2014.5746

A note on pseudorandom subsets formed by generalized cyclotomic classes

By HUANING LIU (Shaanxi) and ERPING SONG (Shaanxi)

Abstract. Recently Z. Chen has constructed a family of pseudorandom subsets by generalized cyclotomic classes, and studied the well-distribution and correlation measures. In this paper we further studied the correlation measures of the subsets.

§1. Introduction

Let subset $\mathcal{R} \subset \{1, 2, \dots, N\}$. Define the sequence

$$E_N = E_N(\mathcal{R}) = (e_1, e_2, \dots, e_N) \in \left\{1 - \frac{|\mathcal{R}|}{N}, -\frac{|\mathcal{R}|}{N}\right\}^N$$

by

$$e_n = \begin{cases} 1 - \dfrac{|\mathcal{R}|}{N} & \text{for} \quad n \in \mathcal{R}, \\ -\dfrac{|\mathcal{R}|}{N} & \text{for} \quad n \notin \mathcal{R}. \end{cases}$$

C. Dartyge and A. Sárközy [2] introduced the following measures of pseudorandomness: the *well-distribution measure* of the subset $\mathcal{R}$ is defined by

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

Mathematics Subject Classification: 11K45.
Key words and phrases: pseudorandom subset, cyclotomic class, character sum, correlation.
This work is supported by National Natural Science Foundation of China under Grant No.11201370, the Natural Science Foundation of Shaanxi Province of China under Grant No. 2013JM1017 and 2011JQ1010, and the Natural Science Foundation of the Education Department of Shaanxi Province of China under Grant No. 2013JK0558.

where the maximum is taken over all $a, b, t \in \mathbb{N}$ with $1 \le a \le a + (t-1)b \le N$. The *correlation measure of order* k of the subset $\mathcal{R}$ is defined by

$$C_k(\mathcal{R}, N) = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} \cdots e_{n+d_k} \right|,$$

where the maximum is taken over all $D = (d_1, \ldots, d_k)$ and M with $0 \le d_1 < \cdots < d_k \le N - M$.

Later many pseudorandom subsets were given and studied. For example, suppose that p, q are two distinct primes satisfying "RSA type" with $2 < p < q < 2p$. Let $N = pq$, $d = (p-1, q-1)$ and $e = [p-1, q-1] = (p-1)(q-1)/d$. There exists a common primitive root g of both p and q. There also exists an integer x satisfying

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

The generalized cyclotomic classes of order d are defined by

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

It is obvious that

$$D_i \cap D_j = \emptyset \quad \text{for } i \ne j, \qquad |D_i| = e \quad \text{for } 0 \le i \le d-1,$$

and

$$\bigcup_{i=0}^{d-1} D_i = \{ n : 0 \le n < pq,\ (n, pq) = 1 \}.$$

Z. Chen [1] presented a large family of subsets formed by generalized cyclotomic classes, and studied the pseudorandom measures.

Proposition 1.1 (Chen, 2010)**.** *Let $f(x) = a_l x^l + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ with $(a_l, N) = 1$ and $0 < l < p(< q)$. 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 $\overline{\mathbb{F}}_q$. Define*

$$\mathcal{R} = \{ n : 1 \le n \le N,\ [f(n)(\mathrm{mod} N)] \in D_u \}$$

for some fixed u with $1 \le u \le d-1$. Then we have

$$W(\mathcal{R}, N) \ll l^2 N^{1/2}(1 + \log N), \quad C_2(\mathcal{R}, N) \ll l^2 N^{3/4}(1 + \log N).$$

In this paper we further study the correlation measures of the subsets. The first purpose of this paper is to give sharper estimates for $C_2(\mathcal{R}, N)$ and $C_3(\mathcal{R}, N)$.

Theorem 1.1. *Define $\mathcal{R}$ as in Proposition 1.1. Then we have*

$$C_2(\mathcal{R}, N) \ll lN^{3/4}, \tag{1.1}$$

$$C_3(\mathcal{R}, N) \ll lN^{3/4}. \tag{1.2}$$

Since $C_2(\mathcal{R}, N) \ll lN^{3/4}$ and $C_3(\mathcal{R}, N) \ll lN^{3/4}$, it is natural to expect that

$$C_k(\mathcal{R}, N) \ll lN^{3/4} \quad \text{for } k \geq 4.$$

However, in Section 4 we shall prove that $C_4(\mathcal{R}, N)$ is very large if p, q are known.

Theorem 1.2. *Define $\mathcal{R}$ as in Proposition 1.1. Then we have*

$$C_4(\mathcal{R}, N) \gg \frac{1}{d^3} N. \tag{1.3}$$

§2. Some lemmas

To complete the proof of theorems, we need the following lemmas.

Lemma 2.1. *Let $k, d \in \mathbb{N}$ and let p be a prime number with $d \mid p-1$. Let $r \leq k$, $0 \leq d_1 < \cdots < d_r < p$, $1 \leq D_1, \ldots, D_r < d$ and $(D_1, \ldots, D_r) = 1$. Suppose that $f \in \mathbb{F}_p[x]$ is a polynomial of degree l with no multiple roots in $\overline{\mathbb{F}}_p$. Define*

$$F(n) = f(n+d_1)^{D_1} \cdots f(n+d_r)^{D_r}$$

and write

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

in $\overline{\mathbb{F}}_p$, where $x_i \neq x_j$ for $i \neq j$. If 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 we have

$$(d, u_1, \ldots, u_s) = 1.$$

Proof. See [3]. □

Lemma 2.2. *Let p be a prime number, and let χ be a non-principal character modulo p of order d. Suppose that $f(x) \in \mathbb{F}_p[x]$ is not the constant multiple of the d-th power of a polynomial over $\mathbb{F}_p$. Then for all $a \in \mathbb{Z}$ we have*

$$\left| \sum_{n \in \mathbb{F}_p} \chi(f(n)) e\left(\frac{an}{p}\right) \right| \leq sp^{1/2},$$

where s denotes the number of distinct zeros of $f(x)$ in $\overline{\mathbb{F}}_p$.

Proof. See Lemma 2 of [5]. □

§3. Proof of Theorem 1.1

Let $\widehat{Z_N^*}$ be the set of all Dirichlet characters modulo N. For any $\chi \in \widehat{Z_N^*}$ we write $\overline{\chi}$ the inverse of χ. By the definition of $\mathcal{R}$ we have

$$n \in \mathcal{R} \Longleftrightarrow [f(n)(\mathrm{mod} N)] \in D_u \Longleftrightarrow \frac{1}{\phi(N)} \sum_{s=0}^{e-1} \sum_{\chi \bmod N} \chi(f(n))\overline{\chi}\left(g^s x^u\right) = 1$$

$$\Longleftrightarrow \frac{1}{d} \sum_{\substack{\chi \bmod N \\ \chi(g)=1}} \chi(f(n))\overline{\chi}\left(x^u\right) = 1.$$

Define

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

Then $\mathcal{H}$ is the annihilator of G in $\widehat{Z_N^*}$. By Theorem 5.6 of [4] we know that the order of $\mathcal{H}$ is $\frac{|\widehat{Z_N^*}|}{|G|} = d$. Denote $\mathcal{H}^* = \mathcal{H} \backslash \{\chi_0\}$. It is easy to show that any $\chi \in \mathcal{H}^*$ can be expressed as $\chi = \chi_p \chi_q$, where χ_p is a primitive character modulo p, and χ_q is a primitive character modulo q.

Let

$$\alpha = \frac{|\mathcal{R}|}{N}, \quad \beta = \frac{1}{d} - \alpha.$$

From [1] we know that

$$\alpha = 1/d + O\left(l^2 N^{-1/2}\right), \quad \beta = O\left(l^2 N^{-1/2}\right),$$

and

$$e_n = \begin{cases} \dfrac{1}{d} \displaystyle\sum_{\chi \in \mathcal{H}^*} \overline{\chi}(x^u)\chi(f(n)) + O\left(l^2 N^{-1/2}\right), & \text{if } (f(n), N) = 1, \\ -\dfrac{1}{d} + O\left(l^2 N^{-1/2}\right), & \text{if } (f(n), N) > 1. \end{cases} \tag{3.1}$$

For $M \in \mathbb{N}$, $d_1, d_2 \in \mathbb{Z}$ with $0 \le d_1 < d_2 \le N - M$, by (3.1) we have

$$\begin{aligned}
&\sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \\
&= \sum_{\substack{n=1 \\ (f(n+d_1)f(n+d_2),N)=1}}^{M} \left(\frac{1}{d} \sum_{\chi_1 \in \mathcal{H}^*} \overline{\chi}_1(x^u) \chi_1(f(n+d_1)) + O\left(l^2 N^{-1/2}\right) \right) \\
&\quad \times \left(\frac{1}{d} \sum_{\chi_2 \in \mathcal{H}^*} \overline{\chi}_2(x^u) \chi_2(f(n+d_2)) + O\big(l^2 N^{-1/2}\big) \right) \\
&\quad + O\Bigg(\sum_{\substack{n=1 \\ (f(n+d_1)f(n+d_2),N)>1}}^{M} 1 \Bigg) \\
&= \frac{1}{d^2} \sum_{\chi_1 \in \mathcal{H}^*} \overline{\chi}_1(x^u) \sum_{\chi_2 \in \mathcal{H}^*} \overline{\chi}_2(x^u) \sum_{n=1}^{M} \chi_1(f(n+d_1)) \chi_2(f(n+d_2)) \\
&\quad + O\Bigg(\sum_{n=1}^{M} \frac{1}{d} \sum_{\chi \in \mathcal{H}^*} l^2 N^{-1/2} \Bigg) + O\left(l^4 N^{-1}\right) \\
&\quad + O\Bigg(\sum_{\substack{n=1 \\ (f(n+d_1)f(n+d_2),N)>1}}^{M} 1 \Bigg) \\
&= \frac{1}{d^2} \sum_{\chi_1 \in \mathcal{H}^*} \overline{\chi}_1(x^u) \sum_{\chi_2 \in \mathcal{H}^*} \overline{\chi}_2(x^u) \sum_{n=1}^{M} \chi_1(f(n+d_1)) \chi_2(f(n+d_2)) \\
&\quad + O\left(l^2 N^{1/2}\right). \qquad (3.2)
\end{aligned}$$

Noting that $\mathcal{H}$ is cyclic. For $\chi_1, \chi_2 \in \mathcal{H}^*$, there exists $\chi' \in \mathcal{H}^*$ such that

$$\chi_1 = (\chi')^{a_1}, \quad \chi_2 = (\chi')^{a_2}, \quad 1 \le a_1,\ a_2 \le d-1.$$

Define

$$\chi^* = (\chi')^{(a_1,a_2)}, \quad \delta_1 = \frac{a_1}{(a_1,a_2)}, \quad \delta_2 = \frac{a_2}{(a_1,a_2)}.$$

Then

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

and the order of χ^* is a divisor of d. Therefore the last sum of (3.2) can be reduced that

$$\sum_{n=1}^{M} \chi_1(f(n+d_1)) \chi_2(f(n+d_2)) = \sum_{n=1}^{M} \chi^*\big(f(n+d_1)^{\delta_1} f(n+d_2)^{\delta_2}\big)$$

$$= \frac{1}{N} \sum_{n=1}^{N} \chi^*\big(f(n+d_1)^{\delta_1} f(n+d_2)^{\delta_2}\big) \sum_{u=1}^{M} \sum_{|a|<\frac{N}{2}} \mathrm{e}\bigg(\frac{a(n-u)}{N}\bigg)$$

$$= \frac{1}{N} \sum_{|a|<\frac{N}{2}} \sum_{u=1}^{M} \mathrm{e}\bigg(-\frac{au}{N}\bigg) \sum_{n=1}^{N} \chi^*\big(f(n+d_1)^{\delta_1} f(n+d_2)^{\delta_2}\big) \mathrm{e}\bigg(\frac{an}{N}\bigg). \qquad (3.3)$$

Definition 3.1. 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 $ab \equiv 1 \pmod q$.

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

$$\sum_{n=1}^{N} \chi^*\big(f(n+d_1)^{\delta_1} f(n+d_2)^{\delta_2}\big) \mathrm{e}\bigg(\frac{an}{N}\bigg)$$

$$= \sum_{u=0}^{q-1} \sum_{v=0}^{p-1} \chi^*\big(f(up+vq+d_1)^{\delta_1} f(up+vq+d_2)^{\delta_2}\big) \mathrm{e}\bigg(\frac{a(up+vq)}{N}\bigg)$$

$$= \sum_{u=0}^{q-1} \chi_q\big(f(up+d_1)^{\delta_1} f(up+d_2)^{\delta_2}\big) \mathrm{e}\bigg(\frac{au}{q}\bigg)$$

$$\times \sum_{v=0}^{p-1} \chi_p\big(f(vq+d_1)^{\delta_1} f(vq+d_2)^{\delta_2}\big) \mathrm{e}\bigg(\frac{av}{p}\bigg)$$

$$= \sum_{u=0}^{q-1} \chi_q\big(f(u+d_1)^{\delta_1} f(u+d_2)^{\delta_2}\big) \mathrm{e}\bigg(\frac{a i_q(p) u}{q}\bigg)$$

$$\times \sum_{v=0}^{p-1} \chi_p\big(f(v+d_1)^{\delta_1} f(v+d_2)^{\delta_2}\big) \mathrm{e}\bigg(\frac{a i_p(q) v}{p}\bigg).$$

We consider d_1, d_2 in three cases.

Case I: $d_1 \not\equiv d_2 \pmod p$ and $d_1 \not\equiv d_2 \pmod q$. By Lemma 2.1 and Lemma 2.2 we have

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

$$\sum_{v=0}^{p-1} \chi_p\big(f(v+d_1)^{\delta_1} f(v+d_2)^{\delta_2}\big) \mathrm{e}\bigg(\frac{a i_p(q) v}{p}\bigg) \ll l p^{1/2}.$$

Then

$$\sum_{n=1}^{N} \chi^*\big(f(n+d_1)^{\delta_1} f(n+d_2)^{\delta_2}\big) \mathrm{e}\bigg(\frac{an}{N}\bigg) \ll l^2 N^{1/2}. \qquad (3.4)$$

Combining (3.2), (3.3) and (3.4) we immediately get

$$\begin{aligned}
&\sum_{n=1}^{M} e_{n+d_1}e_{n+d_2}\\
&\quad\ll \frac{1}{d^2}\sum_{\chi_1\in\mathcal{H}^*}\sum_{\chi_2\in\mathcal{H}^*}\frac{1}{N}\sum_{|a|<\frac{N}{2}}\left|\sum_{u=1}^{M}\mathrm{e}\Big(-\frac{au}{N}\Big)\right|\cdot l^2N^{1/2}+l^2N^{1/2}\\
&\quad\ll \frac{l^2N^{1/2}}{N}\Bigg(M+\sum_{1\le a<\frac{N}{2}}\frac{N}{a}\Bigg)+l^2N^{1/2}\ll l^2N^{1/2}\log N. \qquad (3.5)
\end{aligned}$$

Case II: $d_1\equiv d_2 \pmod p$ and $d_1\not\equiv d_2 \pmod q$. According to Lemma 2.1 and Lemma 2.2 we have

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

On the other hand, we get

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

Then we can have

$$\begin{aligned}
&\sum_{n=1}^{N}\chi^*\big(f(n+d_1)^{\delta_1}f(n+d_2)^{\delta_2}\big)\mathrm{e}\Big(\frac{an}{N}\Big)\\
&\qquad\qquad=\begin{cases} O\big(lq^{1/2}p\big), & \text{if } t_p\mid \delta_1+\delta_2 \text{ and } p\mid a,\\ O\big(l^2N^{1/2}\big), & \text{otherwise.}\end{cases} \qquad (3.6)
\end{aligned}$$

Now from (3.2), (3.3) and (3.6) we have

$$\begin{aligned}\sum_{n=1}^{M} e_{n+d_1}e_{n+d_2} &\ll \frac{1}{d^2}\sum_{\chi_1\in\mathcal{H}^*}\sum_{\chi_2\in\mathcal{H}^*}\frac{1}{N}\sum_{\substack{|a|<\frac{N}{2}\\ p|a}}\left|\sum_{u=1}^{M}\mathrm{e}\Big(-\frac{au}{N}\Big)\right|\cdot lq^{1/2}p\\ &\quad+\frac{1}{d^2}\sum_{\chi_1\in\mathcal{H}^*}\sum_{\chi_2\in\mathcal{H}^*}\frac{1}{N}\sum_{|a|<\frac{N}{2}}\left|\sum_{u=1}^{M}\mathrm{e}\Big(-\frac{au}{N}\Big)\right|\cdot l^2N^{1/2}+l^2N^{1/2}\\ &\ll \frac{lq^{1/2}p}{N}\Bigg(M+\sum_{\substack{1\le a<\frac{N}{2}\\ p|a}}\frac{N}{a}\Bigg)+\frac{l^2N^{1/2}}{N}\Bigg(M+\sum_{1\le a<\frac{N}{2}}\frac{N}{a}\Bigg)+l^2N^{1/2}\\ &\ll lN^{3/4}. \qquad (3.7)\end{aligned}$$

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

$$\sum_{n=1}^{M} e_{n+d_1}e_{n+d_2}\ll lN^{3/4}. \qquad (3.8)$$

Now combining (3.5), (3.7) and (3.8) we immediately get

$$C_2(\mathcal{R},N)=\max_{M,D}\left|\sum_{n=1}^{M}e_{n+d_1}e_{n+d_2}\right|\ll lN^{3/4}.$$

This proves (1.1).

Let $M\in\mathbb{N}$, $d_1,d_2,d_3\in\mathbb{Z}$ such that $0\le d_1<d_2<d_3<N-M$. From (3.1) we can deduce that

$$\begin{aligned}&\sum_{n=1}^{M}e_{n+d_1}e_{n+d_2}e_{n+d_3}\\ &=\sum_{\substack{n=1\\ (\prod_{j=1}^{3}f(n+d_j),N)=1}}^{M}\prod_{j=1}^{3}\Bigg(\frac{1}{d}\sum_{\chi_j\in\mathcal{H}^*}\overline{\chi}_j(x^u)\chi_j(f(n+d_j))+O\big(l^2N^{-1/2}\big)\Bigg)+O(lN^{1/2})\\ &=\frac{1}{d^3}\sum_{\chi_1\in\mathcal{H}^*}\overline{\chi}_1(x^u)\sum_{\chi_2\in\mathcal{H}^*}\overline{\chi}_2(x^u)\sum_{\chi_3\in\mathcal{H}^*}\overline{\chi}_3(x^u)\\ &\quad\times\sum_{n=1}^{M}\chi_1(f(n+d_1))\chi_2(f(n+d_2))\chi_3(f(n+d_3))\end{aligned}$$

$$+ O\left(\sum_{n=1}^{M}\frac{1}{d^2}\sum_{\chi_1\in\mathcal{H}^*}\sum_{\chi_2\in\mathcal{H}^*} l^2N^{-1/2}\right) + O\left(\sum_{n=1}^{M}\frac{1}{d}\sum_{\chi\in\mathcal{H}^*} l^4N^{-1}\right)$$

$$+ O(l^6N^{-3/2}) + O(l^2N^{1/2}) = \frac{1}{d^3}\sum_{\chi_1\in\mathcal{H}^*}\overline{\chi}_1(x^u)\sum_{\chi_2\in\mathcal{H}^*}\overline{\chi}_2(x^u)\sum_{\chi_3\in\mathcal{H}^*}\overline{\chi}_3(x^u)$$

$$\times\sum_{n=1}^{M}\chi_1(f(n+d_1))\chi_2(f(n+d_2))\chi_3(f(n+d_3)) + O(l^2N^{1/2}). \tag{3.9}$$

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

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

Then

$$\sum_{n=1}^{M}\chi_1(f(n+d_1))\chi_2(f(n+d_2))\chi_3(f(n+d_3))$$
$$= \sum_{n=1}^{M}\chi^*\big(f(n+d_1)^{\delta_1}f(n+d_2)^{\delta_2}f(n+d_3)^{\delta_3}\big) = \frac{1}{N}\sum_{|a|<\frac{N}{2}}\sum_{u=1}^{M}\mathrm{e}\bigg(-\frac{au}{N}\bigg)$$
$$\times\sum_{n=1}^{N}\chi^*\big(f(n+d_1)^{\delta_1}f(n+d_2)^{\delta_2}f(n+d_3)^{\delta_3}\big)\mathrm{e}\bigg(\frac{an}{N}\bigg). \tag{3.10}$$

Write $\chi^* = \chi_p\chi_q$. We have

$$\sum_{n=1}^{N}\chi^*\big(f(n+d_1)^{\delta_1}f(n+d_2)^{\delta_2}f(n+d_3)^{\delta_3}\big)\mathrm{e}\bigg(\frac{an}{N}\bigg)$$
$$= \sum_{u=0}^{q-1}\chi_q\big(f(u+d_1)^{\delta_1}f(u+d_2)^{\delta_2}f(u+d_3)^{\delta_3}\big)\mathrm{e}\bigg(\frac{ai_q(p)u}{q}\bigg)$$
$$\times\sum_{v=0}^{p-1}\chi_p\big(f(v+d_1)^{\delta_1}f(v+d_2)^{\delta_2}f(v+d_3)^{\delta_3}\big)\mathrm{e}\bigg(\frac{ai_p(q)v}{p}\bigg).$$

We consider d_1, d_2, d_3 in several cases.

I. Suppose that $d_i \not\equiv d_j$ for $1 \le i < j \le 3$. By Lemma 2.1 and Lemma 2.2 we easily get

$$\sum_{v=0}^{p-1}\chi_p\big(f(v+d_1)^{\delta_1}f(v+d_2)^{\delta_2}f(v+d_3)^{\delta_3}\big)\mathrm{e}\bigg(\frac{ai_p(q)v}{p}\bigg) \ll lp^{1/2}.$$

II. Assume that $d_1 \equiv d_2 \not\equiv d_3 \pmod p$. Then from Lemma 2.1 and Lemma 2.2 we have

$$\sum_{v=0}^{p-1} \chi_p\big(f(v+d_1)^{\delta_1} f(v+d_2)^{\delta_2} f(v+d_3)^{\delta_3}\big) \mathrm{e}\left(\frac{ai_p(q)v}{p}\right) \ll lp^{1/2}.$$

III. If $d_1 \equiv d_2 \equiv d_3 \pmod p$, we get the following results

$$\begin{aligned}
&\sum_{v=0}^{p-1} \chi_p\big(f(v+d_1)^{\delta_1} f(v+d_2)^{\delta_2} f(v+d_3)^{\delta_3}\big) \mathrm{e}\left(\frac{ai_p(q)v}{p}\right) \\
&\quad = \sum_{v=0}^{p-1} \chi_p^{\delta_1+\delta_2+\delta_3}\big(f(v+d_1)\big) \mathrm{e}\left(\frac{ai_p(q)v}{p}\right) \\
&\quad = \begin{cases} O\big(lp^{1/2}\big), & \text{if } \ t_p \nmid \delta_1+\delta_2+\delta_3, \\ O(l), & \text{if } \ t_p \mid \delta_1+\delta_2+\delta_3 \text{ and } \ p \nmid a, \\ p + O(l), & \text{if } \ t_p \mid \delta_1+\delta_2+\delta_3 \text{ and } \ p \mid a. \end{cases} \\
&\quad = \begin{cases} O(p), & \text{if } \ t_p \mid \delta_1+\delta_2+\delta_3 \text{ and } \ p \mid a, \\ O\big(lp^{1/2}\big), & \text{otherwise.} \end{cases}
\end{aligned}$$

Noting that $d_i \not\equiv d_j \pmod N$ for all $1 \le i < j \le 3$. We have

$$\begin{aligned}
&\sum_{n=1}^{N} \chi^*\big(f(n+d_1)^{\delta_1} f(n+d_2)^{\delta_2} f(n+d_3)^{\delta_3}\big) \mathrm{e}\left(\frac{an}{N}\right) \\
&\qquad = \begin{cases} O\left(lN^{3/4}\right), & \text{if } \ t_p \mid \delta_1+\delta_2+\delta_3, p \mid a, \\ & \text{or } \ t_q \mid \delta_1+\delta_2+\delta_3, q \mid a, \\ O\left(l^2N^{1/2}\right), & \text{otherwise.} \end{cases}
\end{aligned} \tag{3.11}$$

Then from (3.9), (3.10) and (3.11) we get

$$\begin{aligned}
\sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} e_{n+d_3} &\ll \frac{1}{d^3} \sum_{\chi_1 \in \mathcal{H}^*} \sum_{\chi_2 \in \mathcal{H}^*} \sum_{\chi_3 \in \mathcal{H}^*} \frac{1}{N} \sum_{\substack{|a| < \frac{N}{2} \\ p \mid a}} \left| \sum_{u=1}^{M} \mathrm{e}\left(-\frac{au}{N}\right) \right| \cdot lN^{3/4} \\
&+ \frac{1}{d^3} \sum_{\chi_1 \in \mathcal{H}^*} \sum_{\chi_2 \in \mathcal{H}^*} \sum_{\chi_3 \in \mathcal{H}^*} \frac{1}{N} \sum_{\substack{|a| < \frac{N}{2} \\ q \mid a}} \left| \sum_{u=1}^{M} \mathrm{e}\left(-\frac{au}{N}\right) \right| \cdot lN^{3/4}
\end{aligned}$$

$$+\frac{1}{d^3}\sum_{\chi_1\in\mathcal{H}^*}\sum_{\chi_2\in\mathcal{H}^*}\sum_{\chi_3\in\mathcal{H}^*}\frac{1}{N}\sum_{|a|<\frac{N}{2}}\left|\sum_{u=1}^{M}\mathrm{e}\Big(-\frac{au}{N}\Big)\right|\cdot l^2N^{1/2}+l^2N^{1/2}$$

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

$$+\frac{l^2N^{1/2}}{N}\Bigg(M+\sum_{1\le a<\frac{N}{2}}\frac{N}{a}\Bigg)+l^2N^{1/2}\ll lN^{3/4}.$$

Therefore

$$C_3(\mathcal{R},N)=\max_{M,D}\left|\sum_{n=1}^{M}e_{n+d_1}e_{n+d_2}e_{n+d_3}\right|\ll lN^{3/4}.$$

This proves (1.2).

§4. Proof of Theorem 1.2

Let $M\in\mathbb{N}$, $d_1,d_2,d_3,d_4\in\mathbb{Z}$ such that $0\le d_1<d_2<d_3<d_4<N-M$. Suppose that

$$d_1\equiv d_2\pmod p,\quad d_3\equiv d_4\pmod p,\quad d_1\not\equiv d_3\pmod p,\tag{4.1}$$

$$d_1\equiv d_3\pmod q,\quad d_2\equiv d_4\pmod q,\quad d_1\not\equiv d_2\pmod q.\tag{4.2}$$

From (3.1) we can get

$$\sum_{n=1}^{M}e_{n+d_1}e_{n+d_2}e_{n+d_3}e_{n+d_4}$$

$$=\sum_{\substack{n=1\\ (\prod_{j=1}^4 f(n+d_j),N)=1}}^{M}\prod_{j=0}^{4}\left(\frac{1}{d}\sum_{\chi_j\in\mathcal{H}^*}\overline{\chi}_j(x^u)\chi_j(f(n+d_j))+O\left(l^2N^{-1/2}\right)\right)$$

$$+O\Bigg(\sum_{\substack{n=1\\ (\prod_{j=1}^4 f(n+d_j),N)>1}}1\Bigg)$$

$$=\frac{1}{d^4}\sum_{\chi_1\in\mathcal{H}^*}\overline{\chi}_1(x^u)\sum_{\chi_2\in\mathcal{H}^*}\overline{\chi}_2(x^u)\sum_{\chi_3\in\mathcal{H}^*}\overline{\chi}_3(x^u)\sum_{\chi_4\in\mathcal{H}^*}\overline{\chi}_4(x^u)$$

$$\times \sum_{n=1}^{M} \chi_1(f(n+d_1))\chi_2(f(n+d_2))\chi_3(f(n+d_3))\chi_4(f(n+d_4))$$
$$+ O\big(l^2 N^{1/2}\big). \tag{4.3}$$

For $\chi_1, \chi_2, \chi_3, \chi_4 \in \mathcal{H}^*$, there exists $\chi' \in \mathcal{H}^*$ with

$$\chi_i = (\chi')^{a_i}, \quad 1 \le a_i \le d-1, \quad i = 1,2,3,4.$$

Define

$$\chi^* = (\chi')^{(a_1,a_2,a_3,a_4)}, \quad \delta_i = \frac{a_i}{(a_1,a_2,a_3,a_4)}, \quad i = 1,2,3,4.$$

Then

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

and

$$1 \le \delta_1, \delta_2, \delta_3, \delta_4 \le d-1, \quad (\delta_1, \delta_2, \delta_3, \delta_4) = 1.$$

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

$$\sum_{n=1}^{M} \chi_1(f(n+d_1))\chi_2(f(n+d_2))\chi_3(f(n+d_3))\chi_4(f(n+d_4))$$
$$= \sum_{n=1}^{M} \chi^*\big(f(n+d_1)^{\delta_1} f(n+d_2)^{\delta_2} f(n+d_3)^{\delta_3} f(n+d_4)^{\delta_4}\big)$$
$$= \frac{1}{N} \sum_{|a|<\frac{N}{2}} \sum_{u=1}^{M} \mathrm{e}\left(-\frac{au}{N}\right)$$
$$\times \sum_{n=1}^{N} \chi^*\big(f(n+d_1)^{\delta_1} f(n+d_2)^{\delta_2} f(n+d_3)^{\delta_3} f(n+d_4)^{\delta_4}\big) \mathrm{e}\left(\frac{an}{N}\right)$$
$$= \frac{1}{N} \sum_{|a|<\frac{N}{2}} \sum_{u=1}^{M} \mathrm{e}\left(-\frac{au}{N}\right)$$
$$\times \sum_{u=0}^{q-1} \chi_q\big(f(u+d_1)^{\delta_1} f(u+d_2)^{\delta_2} f(u+d_3)^{\delta_3} f(u+d_4)^{\delta_4}\big) \mathrm{e}\left(\frac{a i_q(p) u}{q}\right)$$
$$\times \sum_{v=0}^{p-1} \chi_p\big(f(v+d_1)^{\delta_1} f(v+d_2)^{\delta_2} f(v+d_3)^{\delta_3} f(v+d_4)^{\delta_4}\big) \mathrm{e}\left(\frac{a i_p(q) v}{p}\right)$$
$$= \frac{1}{N} \sum_{|a|<\frac{N}{2}} \sum_{u=1}^{M} \mathrm{e}\left(-\frac{au}{N}\right)$$

$$\times \sum_{u=0}^{q-1} \chi_q\big(f(u+d_1)^{\delta_1+\delta_3} f(u+d_2)^{\delta_2+\delta_4}\big) \mathrm{e}\bigg(\frac{ai_q(p)u}{q}\bigg)$$
$$\times \sum_{v=0}^{p-1} \chi_p\big(f(v+d_1)^{\delta_1+\delta_2} f(v+d_3)^{\delta_3+\delta_4}\big) \mathrm{e}\bigg(\frac{ai_p(q)v}{p}\bigg). \tag{4.4}$$

By Lemma 2.1 and Lemma 2.2 we easily have

$$\sum_{v=0}^{p-1} \chi_p\big(f(v+d_1)^{\delta_1+\delta_2} f(v+d_3)^{\delta_3+\delta_4}\big) \mathrm{e}\bigg(\frac{ai_p(q)v}{p}\bigg) = \begin{cases} p+O(l), & \text{if } \ t_p \mid \delta_1+\delta_2, \ t_p \mid \delta_3+\delta_4 \text{ and } \ p \mid a, \\ O\big(lp^{1/2}\big), & \text{otherwise,} \end{cases}$$

and

$$\sum_{u=0}^{q-1} \chi_q\big(f(u+d_1)^{\delta_1+\delta_3} f(u+d_2)^{\delta_2+\delta_4}\big) \mathrm{e}\bigg(\frac{ai_q(p)u}{q}\bigg) = \begin{cases} q+O(l), & \text{if } \ t_q \mid \delta_1+\delta_3, \ t_q \mid \delta_2+\delta_4 \text{ and } \ q \mid a, \\ O\big(lq^{1/2}\big), & \text{otherwise.} \end{cases}$$

Therefore

$$\sum_{n=1}^{N} \chi^*\big(f(n+d_1)^{\delta_1} f(n+d_2)^{\delta_2} f(n+d_3)^{\delta_3} f(n+d_4)^{\delta_4}\big) \mathrm{e}\bigg(\frac{an}{N}\bigg) = \begin{cases} N+O\left(lN^{1/2}\right), & \text{if } \ t_p \mid \delta_1+\delta_2, t_p \mid \delta_3+\delta_4, \\ & \qquad t_q \mid \delta_1+\delta_3, \ t_q \mid \delta_2+\delta_4, N|a, \\ O\left(lN^{3/4}\right), & \text{otherwise.} \end{cases} \tag{4.5}$$

Combining (4.3)-(4.5) we get

$$\sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} e_{n+d_3} e_{n+d_4}$$
$$= \frac{1}{d^4} \sum_{\chi_1 \in \mathcal{H}^*} \sum_{\substack{\chi_2 \in \mathcal{H}^* \\ t_p|\delta_1+\delta_2, \\ t_q|\delta_1+\delta_3,}} \sum_{\substack{\chi_3 \in \mathcal{H}^* \\ t_p|\delta_3+\delta_4 \\ t_q|\delta_2+\delta_4}} \sum_{\chi_4 \in \mathcal{H}^*} \frac{1}{N} \cdot M\left(N + O(lN^{1/2})\right)$$
$$+ O\left(\frac{1}{d^4} \sum_{\chi_1 \in \mathcal{H}^*} \sum_{\chi_2 \in \mathcal{H}^*} \sum_{\chi_3 \in \mathcal{H}^*} \sum_{\chi_4 \in \mathcal{H}^*} \frac{1}{N} \sum_{|a|<\frac{N}{2}} \left|\sum_{u=1}^{M} \mathrm{e}\left(-\frac{au}{N}\right)\right| \cdot lN^{3/4}\right)$$

$$+ O\big(l^2 N^{1/2}\big)$$
$$= \frac{M}{d^4} \sum_{\chi_1\in\mathcal{H}^*} \sum_{\substack{\chi_2\in\mathcal{H}^* \\ t_p|\delta_1+\delta_2,\ \\ t_q|\delta_1+\delta_3,\ }} \sum_{\substack{\chi_3\in\mathcal{H}^* \\ t_p|\delta_3+\delta_4 \\ t_q|\delta_2+\delta_4}} \sum_{\chi_4\in\mathcal{H}^*} + O\left(lN^{3/4}\log N\right).$$

On the other hand, we have

$$\sum_{\chi_1\in\mathcal{H}^*} \sum_{\chi_2\in\mathcal{H}^*} \sum_{\substack{\chi_3\in\mathcal{H}^* \\ t_p|\delta_1+\delta_2,\ t_p|\delta_3+\delta_4 \\ t_q|\delta_1+\delta_3,\ t_q|\delta_2+\delta_4}} \sum_{\chi_4\in\mathcal{H}^*} 1 \geq \sum_{\alpha=1}^{d-1} \sum_{a_1=1}^{d-1} \sum_{a_2=1}^{d-1} \sum_{\substack{a_3=1 \\ (a_1,a_2,a_3,a_4)=\alpha \\ d|a_1+a_2,\ d|a_3+a_4 \\ d|a_1+a_3,\ d|a_2+a_4}}^{d-1} \sum_{a_4=1}^{d-1} 1$$
$$= \sum_{\alpha=1}^{d-1} \sum_{\substack{a_1=1 \\ (a_1,d-a_1)=\alpha}}^{d-1} 1 = \sum_{\alpha=1}^{d-1} \sum_{\substack{a=1 \\ (a,d)=\alpha}}^{d-1} 1 \gg d.$$

Therefore
$$\sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} e_{n+d_3} e_{n+d_4} \gg \frac{M}{d^3}.$$

Suppose that p, q are known, then we can take

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

It is obvious that d_1, d_2, d_3, d_4 satisfy (4.1) and (4.2). So we have

$$C_4(\mathcal{R}, N) \gg \frac{1}{d^3} N.$$

Acknowledgments. The authors express their gratitude to the referees for their helpful and detailed comments.

References

[1] Z. Chen, Large families of pseudo-random subsets formed by generalized cyclotomic classes, *Monatshefte für Mathematik* **161** (2010), 161–172.

[2] C. Dartyge and A. Sárközy, On pseudo-random subsets of the set of the integers not exceeding N, *Periodica Math. Hungar.* **54** (2007), 183–200.

[3] C. Dartyge and A. Sárközy, Large families of pseudorandom subsets formed by power residues, *Uniform Distribution Theory* **2** (2007), 73–88.

[4] R. Lidl and H. Niederreiter, Finite Fields (Encyclopedia of Mathematics and its Applications), *Addison-Wesley*, *Reading*, 1983.

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

HUANING LIU
DEPARTMENT OF MATHEMATICS
NORTHWEST UNIVERSITY
XI'AN, SHAANXI
P.R. CHINA

E-mail: hnliumath@hotmail.com

ERPING SONG
DEPARTMENT OF MATHEMATICS
NORTHWEST UNIVERSITY
XI'AN, SHAANXI
P.R. CHINA

E-mail: songerping@foxmail.com

(Received January 7, 2013; revised March 31, 2014)