# Pseudorandom subsets with composite moduli*

Hua Zhang    Huaning Liu

**Abstract**

In earlier papers C. Dartyge and A. Sárközy presented large families of pseudorandom subsets with prime moduli. In this paper we extend two large families of subsets to the case when the moduli is composite.

## 1 Introduction

The need for pseudorandom binary sequences arises in many cryptographic applications. Therefore it is interesting to give some binary sequences and study their pseudorandom properties theoretically. In 1997 C. Mauduit and A. Sárközy [5] initiated a comprehensive study of finite pseudorandom binary sequences

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

First they introduced the following pseudorandom measures: The *well-distribution measure* of $E_N$ is defined by

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

*This work is supported by National Natural Science Foundation of China under Grant No.11201370, the Science and Technology Program of Shaanxi Province of China under Grant No. 2013JM1017, 2014JM1007 and 2014KJXX-61, and the Natural Science Foundation of the Education Department of Shaanxi Province of China under Grant No. 2013JK0558.

Received by the editors in January 2013.

Communicated by M. Van den Bergh.

2010 *Mathematics Subject Classification* : 11K45.

*Key words and phrases* : pseudorandom subset; composite moduli; exponential sum.

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

$$C_l\left(E_N\right) = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} \cdots e_{n+d_l} \right|,$$

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

Many pseudorandom binary sequences were given and studied. For example, C. Mauduit, J. Rivat and A. Sárközy [4] presented the following family of pseudorandom binary sequences.

**Proposition 1.1.** *Let $p$ be an odd prime number, $f(x) \in \mathbb{F}_p[x]$ of degree $k$, and define $E_p = (e_1, \cdots, e_p)$ by*

$$e_n = \begin{cases} +1, & \textit{if } 0 \leq r_p(f(n)) < p/2, \\ -1, & \textit{if } p/2 \leq r_p(f(n)) < p, \end{cases}$$

*where $r_p(n)$ denotes the unique $r \in \{0, 1, \cdots, p-1\}$ such that $n \equiv r (\mathrm{mod}\ p)$. Then we have*

$$W(E_p) \ll kp^{1/2}(\log p)^2,$$

*and for $2 \leq l \leq k-1$, we also have*

$$C_l(E_p) \ll kp^{1/2}(\log p)^{l+1}.$$

Another construction was given by C. Mauduit and A. Sárközy in [6].

**Proposition 1.2.** *Assume that $p$ is a prime number, $f(x) \in \mathbb{F}_p[x]$ has degree $k$ $(1 < k < p)$ and no multiple zero in $\overline{\mathbb{F}}_p$. For $(a, p) = 1$, denote the multiplicative inverse of $a$ by $a^{-1}$ such that $aa^{-1} \equiv 1 (\mathrm{mod} p)$. Define the binary sequence $E_p = (e_1, \cdots, e_p)$ by*

$$e_n = \begin{cases} +1, & \textit{if } (f(n), p) = 1, r_p(f(n)^{-1}) < p/2, \\ -1, & \textit{if either } (f(n), p) = 1, r_p(f(n)^{-1}) \geq p/2 \textit{ or } p \mid f(n). \end{cases}$$

*Then we have*

$$W(E_p) \ll kp^{1/2}(\log p)^2.$$

*Moreover assume that $l \in \mathbb{N}$, and one of the following conditions holds:*

$$\text{(i) } l = 2, \qquad \text{(ii) } (4k)^l < p.$$

*Then we have*

$$C_l(E_p) \ll klp^{1/2}(\log p)^{l+1}.$$

The above constructions are with a prime moduli $p$. One might like to look for constructions with composite moduli $m$. Let $m$ be a modulus of "RSA type", i.e., it is the product of two primes not far apart, say,

$$m = pq, \quad p, q \text{ are primes}, \quad p < q < 2p. \tag{1.1}$$

J. Rivat and A. Sárközy [7] tried to extend the above two constructions to the case of composite moduli $m$ defined by (1.1). Their main results on these constructions are the following.

**Proposition 1.3.** *Assume that* $m \in \mathbb{N}$ *is of the form* (1.1), $f(x) = a_k x^k + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, $(a_k, pq) = 1$, *and* $2 \le k < p(< q)$. *Define the binary sequence* $E_m = (e_1, \cdots, e_m)$ *by*

$$e_n = \begin{cases} +1, & \text{if } 0 \le r_m(f(n)) < m/2, \\ -1, & \text{if } m/2 \le r_m(f(n)) < m, \end{cases}$$

*where* $r_m(n)$ *denotes the unique* $r \in \{0, 1, \cdots, m-1\}$ *with* $n \equiv r (\bmod m)$. *Then we have*

$$W(E_m) \ll k^2 m^{1/2} (\log m)^2.$$

*Assume that* $k \ge 3$. *Then we also have*

$$C_2(E_m) \ll k m^{3/4} (\log m)^3.$$

**Definition 1.1.** *For* $a \in \mathbb{Z}$ *and* $m \in \mathbb{N}$ *such that* $(a, m) = 1$, *let* $i_m(a)$ *denote the unique integer* $b$ *such that* $0 \le b \le m-1$ *and* $ab \equiv 1 (\bmod m)$.

**Proposition 1.4.** *Assume that* $m \in \mathbb{N}$ *is of the form* (1.1), $f(x) = a_k x^k + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, $(a_k, pq) = 1$, *and* $1 \le k < p(< q)$. *Define the binary sequence* $E_m = (e_1, \cdots, e_m)$ *by*

$$e_n = \begin{cases} +1, & \text{if } (f(n), m) = 1, r_m(i_m(f(n))) < m/2, \\ -1, & \text{if either } (f(n), m) = 1, r_m(i_m(f(n))) \ge m/2, \text{ or } (f(n), m) > 1. \end{cases}$$

*Then we have*

$$W(E_m) \ll k^2 m^{1/2} (\log m)^2,$$

*and*

$$C_2(E_m) \ll k^2 m^{3/4} (\log m)^3.$$

H. Liu, T. Zhan and X. Wang [3] studied the correlation measure of order greater than 2 of the sequences defined in Proposition 1.3 and Proposition 1.4.

**Proposition 1.5.** *Define* $m$, $k$, $f(x)$ *and* $E_m$ *as in Proposition 1.3. Assume that* $k \ge 4$. *Then*

$$C_3(E_m) \ll k m^{3/4} (\log m)^4.$$

*Assume that the prime factors* $p, q$ *of* $m$ *are made known, and* $1 \le l \le \min((k-1)/2, q - p + 1)$. *Then we have*

$$C_{4l}(E_m) \gg \left(\frac{2}{\pi}\right)^{4l} m.$$

**Proposition 1.6.** *Define* $m$, $k$, $f(x)$ *and* $E_m$ *as in Proposition 1.4. Assume that* $(4k)^3 < p(< q)$. *Then*

$$C_3(E_m) \ll k^3 m^{3/4} (\log m)^4.$$

*Assume that the prime factors $p$, $q$ of $m$ are made known, and $(4k)^{2l} < p$. Then we have*

$$C_{4l}(E_m) \gg \left(\frac{2}{\pi}\right)^{4l} m.$$

In a series of papers C. Dartyge and A. Sárközy (partly with other coauthors) studied pseudorandom subsets. Let $\mathcal{R} \subset \{1, 2, \cdots, N\}$ and define the sequence

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

by

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

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

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

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 $l$* of the subset $\mathcal{R}$ is defined by

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

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

Later many pseudorandom subsets were given and studied. For example, C. Dartyge, E. Mosaki and A. Sárközy [1] proved the following:

**Proposition 1.7.** *Assume that $p$ is an odd prime number, $f(x) \in \mathbb{F}_p[x]$ is of degree $k \ge 2$. Let $r \in \mathbb{Z}, s \in \mathbb{N}, s < p/2$. Define $\mathcal{R} \subset \{1, \cdots, p\}$ by*

$$\mathcal{R} = \{n : 1 \le n \le p, \exists h \in \{r, r+1, \cdots, r+s-1\} \textit{ with } f(n) \equiv h (\text{mod } p)\}.$$

*Writing $\alpha = |\mathcal{R}|/p$ and $\beta = s/p$, we have*

$$|\alpha - \beta| < \frac{1}{p} + \frac{k(1 + \log p)}{\sqrt{p}}, \qquad W(\mathcal{R}, p) < 2k\sqrt{p}(\log p)^2.$$

*And for $2 \le l \le k-1$, we have*

$$C_l(\mathcal{R}, p) < 2k\sqrt{p}(1 + \log p)^{l+1}.$$

**Proposition 1.8.** *Assume that $p$ is an odd prime number, $k \in \mathbb{N}$, $k < p$, $r \in \mathbb{Z}$, $s \in \mathbb{N}$, $s < p$, $f(x) \in \mathbb{F}_p[x]$ has no multiple root and* $\deg(f(x)) = k$. *Define $\mathcal{R} \subset \{1, \cdots, p\}$ by*

$$\mathcal{R} = \{n : 1 \le n \le p, (f(n), p) = 1, \exists h \in \{r, r+1, \cdots, r+s-1\} \\ \text{with } hf(n) \equiv 1 (\text{mod } p)\}.$$

*Writing $\alpha = |\mathcal{R}|/p$ and $\beta = s/p$, we have*

$$|\alpha - \beta| \ll \frac{k \log p}{\sqrt{p}}, \qquad W(\mathcal{R}, p) \ll k\sqrt{p}(\log p)^2.$$

*Moreover, assume that $l \in \mathbb{N}$, $l \ge 2$ and one of the following conditions holds:*

$$\text{(i) } l = 2, \qquad \text{(ii) } (4k)^l < p.$$

*Then we have*

$$C_l(\mathcal{R}, p) \ll kl\sqrt{p}(\log p)^{l+1}.$$

Note that the above constructions are with a prime moduli $p$. In this paper we extend the constructions in Proposition 1.7 and Proposition 1.8 to the case when the moduli $m$ is of the form (1.1), and study the pseudorandom properties.

**Theorem 1.1.** *Assume that $m \in \mathbb{N}$ is of the form* (1.1), *$f(x) = a_k x^k + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, $(a_k, pq) = 1$, and $2 \le k < p(< q)$. Let $r \in \mathbb{Z}, s \in \mathbb{N}, s < m/2$. Define $\mathcal{R} \subset \{1, \cdots, m\}$ by*

$$\mathcal{R} = \{n : 1 \le n \le m, \exists h \in \{r, r+1, \cdots, r+s-1\} \text{ with } f(n) \equiv h (\text{mod } m)\}.$$

*Writing $\alpha = |\mathcal{R}|/m$ and $\beta = s/m$, we have*

$$|\alpha - \beta| \ll (k-1)^2 m^{-1/2} \log m, \qquad W(\mathcal{R}, m) \ll k^2 m^{1/2} (\log m)^2.$$

*Assume that $k \ge 3$. Then*

$$C_2(\mathcal{R}, m) \ll km^{3/4}.$$

*If $k \ge 4$, then we also have*

$$C_3(\mathcal{R}, m) \ll km^{3/4} \log m.$$

**Theorem 1.2.** *Assume that $m \in \mathbb{N}$ is of the form* (1.1), *$f(x) = a_k x^k + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, $(a_k, pq) = 1$, and $1 \le k < p(< q)$. Let $r \in \mathbb{Z}, s \in \mathbb{N}, s < m/2$. Define $\mathcal{R} \subset \{1, \cdots, m\}$ by*

$$\mathcal{R} = \{n : 1 \le n \le m, (f(n), m) = 1, \exists h \in \{r, r+1, \cdots, r+s-1\} \\ \text{with } hf(n) \equiv 1 (\text{mod } m)\}.$$

*Writing $\alpha = |\mathcal{R}|/m$ and $\beta = s/m$, we have*

$$|\alpha - \beta| \ll k^2 m^{-1/2} \log m, \qquad W(\mathcal{R}, m) \ll k^2 m^{1/2} (\log m)^2,$$

*and*

$$C_2(\mathcal{R}, m) \ll km^{3/4}.$$

*If* $(4k)^3 < p(< q)$, *then we also have*

$$C_3(\mathcal{R}, m) \ll km^{3/4} \log m.$$

The correlations of order 2 and 3 are small as in the binary sequence case. In Section 5 we shall prove that the correlation of order 4 is also large.

**Theorem 1.3.** *Define* $m$, $k$, $f(x)$ *and* $\mathcal{R}$ *as in Theorem 1.1. Assume that the prime factors* $p$, $q$ *of* $m$ *are made known, and* $1 \leq l \leq \min\left((k-1)/2, q-p+1\right)$. *Then we have*

$$C_{4l}(\mathcal{R}, m) \gg \left(\frac{2}{3} - \beta\right)^l \beta^{3l} m.$$

**Theorem 1.4.** *Define* $m$, $k$, $f(x)$ *and* $\mathcal{R}$ *as in Theorem 1.2. Assume that the prime factors* $p$, $q$ *of* $m$ *are made known, and* $(4k)^{2l} < p$. *Then we have*

$$C_{4l}(\mathcal{R}, m) \gg \left(\frac{2}{3} - \beta\right)^l \beta^{3l} m.$$

**Remark 1.1.** *These results show that in general it is not enough to estimate correlations of small (2, or 2 and 3) order, one also has to estimate correlations of higher order.*

**Notations.** *Throughout this paper,* $r_m(x)$ *denotes the unique* $y \in \{0, 1, \cdots, m-1\}$ *such that* $x \equiv y (\bmod\ m)$, $e_m(x) = e^{2\pi i x/m}$. *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* $0 \leq b \leq q-1$ *and* $ab \equiv 1 (\bmod\ q)$.

## 2 Some lemmas

We need the following lemmas.

**Lemma 2.1.** *Let* $m \in \mathbb{N}$. *For* $0 \leq \beta < 1$, $x \in \mathbb{Z}$ *we write*

$$g_\beta(x) = \begin{cases} 1-\beta, & \text{if } 0 \leq r_m(x) < \beta m, \\ -\beta, & \text{if } \beta m \leq r_m(x) < m, \end{cases}$$

*and the complex numbers* $a_h$ *with* $h \in \mathbb{Z}$, $|h| < \frac{m}{2}$ *are uniquely defined by*

$$g_\beta(x) = \sum_{|h| < \frac{m}{2}} a_h e_m(hx) \quad (\forall x \in \mathbb{Z}).$$

*Then uniformly for all* $0 \leq \beta < 1$, *we have*

$$|a_0| < \frac{1}{m} \text{ and } |a_h| \leq \frac{1}{2|h|} \text{ for } 0 < |h| < \frac{m}{2}.$$

*Proof.* This lemma can be easily proved by using the methods of Lemma 2 in [1]. ∎

**Lemma 2.2.** *Let $p$, $q$ be distinct prime numbers and $f(x) = a_k x^k + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ with $2 \le k < \min(p,q)$ and $(a_k, pq) = 1$. Let $X$, $Y$ be real numbers with $0 < Y \le pq$. Then*

$$\left|\sum_{n=0}^{pq-1} e_{pq}(f(n))\right| \le (k-1)^2\sqrt{pq},$$

$$\left|\sum_{X<n\le X+Y} e_{pq}(f(n))\right| \ll k^2\sqrt{pq}\log(pq).$$

*Proof.* See Lemma 9 and Lemma 10 of [7]. ∎

**Lemma 2.3.** *Let $p$, $q$ be distinct prime numbers. Then for any polynomial $f(x) \in \mathbb{Z}[x]$, we have*

$$\left|\sum_{n=1}^{pq} e_{pq}(f(n))\right| = \left|\sum_{u=1}^{q} e_q(i_q(p)f(u))\right| \times \left|\sum_{v=1}^{p} e_p(i_p(q)f(v))\right|.$$

*Proof.* This is Lemma 8 in [7]. ∎

**Lemma 2.4.** *Let $p$ be a prime numbers, $l \in \mathbb{N}$, $1 \le l < p$, $f(x) \in \mathbb{F}_p[x]$ a polynomial of degree $k \ge l$, and let $d_1, \cdots, d_l$ be $l$ different elements of $\mathbb{F}_p$. Then for all $(h_1, \cdots, h_l) \in \mathbb{F}_p^l \setminus (0, \cdots, 0)$, the polynomial*

$$g(x) = h_1 f(x + d_1) + \cdots + h_l f(x + d_l)$$

*is of degree $\ge k - l + 1$.*

*Proof.* This is Lemma 3 in [4]. ∎

**Lemma 2.5.** *Suppose that $p$ is a prime number and $f(x) = a_k x^k + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ is a polynomial with $0 < k < p$ and $(a_k, p) = 1$. Then*

$$\left|\sum_{n=0}^{p-1} e_p(f(n))\right| \le (k-1)\sqrt{p}.$$

*Proof.* This is Corollary 2F in [8]. ∎

**Lemma 2.6.** *Let $p$ and $q$ be two distinct prime numbers. Let $Q, R \in \mathbb{Z}[x]$ be polynomials such that reducing them modulo $p$ the polynomials $Q_p$ and $R_p$ obtained in this way determine a rational function $Q_p/R_p$ over $\mathbb{F}_p$, and reducing them modulo $q$ the polynomials $Q_q$ and $R_q$ obtained in this way determine a rational function $Q_q/R_q$ over*

*$\mathbb{F}_q$. Write $D = \max(\deg(R), \deg(Q))$ and let $X$, $Y$ be real numbers with $0 < Y \leq pq$. Then we have*

$$\left| \sum_{\substack{n=0 \\ (R(n),pq)=1}}^{pq-1} e_{pq}\left(Q(n) i_{pq}(R(n))\right) \right| \ll D^2 \sqrt{pq},$$

*if $Q_p/R_p$ and $Q_q/R_q$ are not constants.*

$$\left| \sum_{\substack{X<n\leq X+Y \\ (R(n),pq)=1}} e_{pq}\left(Q(n) i_{pq}(R(n))\right) \right| \ll D^2 \sqrt{pq} \log(pq),$$

*if $Q_p/R_p$ and $Q_q/R_q$ are not constants or linear polynomials.*

*Proof.* See Lemma 14 and Lemma 15 in [7]. ■

**Lemma 2.7.** *Let $p, q \in \mathbb{N}$ with $(p,q) = 1$ and $Q(x), R(x) \in \mathbb{Z}[x]$. Then*

$$\sum_{\substack{1\leq n\leq pq \\ (R(n),pq)=1}} e_{pq}\left(Q(n) i_{pq}(R(n))\right) =$$

$$\sum_{\substack{1\leq u\leq q \\ (R(u),q)=1}} e_q\left(Q(u) i_q(pR(u))\right) \sum_{\substack{1\leq v\leq p \\ (R(v),p)=1}} e_p\left(Q(v) i_p(qR(v))\right).$$

*Proof.* This is Lemma 11 in [7]. ■

**Lemma 2.8.** *Assume that $p$ is a prime number, $f(x) \in \mathbb{F}_p[x]$ has degree $(0 <) k (< p)$ and no multiple zero in $\overline{\mathbb{F}_p}$. Assume that $l \in \mathbb{N}$ with $2 \leq l \leq p$, and one of the following conditions holds*

$$\text{(i) } l = 2, \qquad \text{(ii) } (4k)^l < p.$$

*Let $d_1, \cdots, d_l$ be $l$ different elements of $\mathbb{F}_p$. Then for all $(h_1, \cdots, h_l) \in \mathbb{F}_p^l \backslash (0, \cdots, 0)$, the polynomial*

$$g(n) = \sum_{i=1}^{l} h_i \prod_{\substack{1\leq j\leq l \\ j\neq i}} f(n + d_j)$$

*is not the $0$ polynomial.*

*Proof.* This is Lemma 5 in [6]. ■

**Lemma 2.9.** *Let $p$ be a prime number and $Q/R$ a rational function over $\mathbb{F}_p$, which is not constant. Let $s$ be the number of distinct roots of the polynomial $R$ in $\overline{\mathbb{F}}_p$. If $\psi$ is a non-trivial additive character of $\mathbb{F}_p$, then*

$$\left|\sum_{\substack{n\in\mathbb{F}_p\\ R(n)\neq 0}} \psi\left(\frac{Q(n)}{R(n)}\right)\right| \leq (\max(\deg(Q),\deg(R))+s-1)\sqrt{p}.$$

*Proof.* This is Lemma 13 in [7]. ■

**Lemma 2.10.** *Assume that $m\in\mathbb{N}$ is of the form (1.1). Then we have*

$$\sum_{|h_1|<m/2}\ \sum_{\substack{|h_2|<m/2\\ p|h_1+h_2\\ h_1+h_2\neq 0}}\ \sum_{|h_3|<m/2}\cdots\sum_{|h_l|<m/2} a_{h_1}e_m(-h_1r)a_{h_2}e_m(-h_2r)\cdots a_{h_l}e_m(-h_lr)$$
$$\ll m^{-1/2}(\log m)^l.$$

*Proof.* By using Lemma 2.1 and the methods in Lemma 2.8 of [3] we can easily get the lemma. ■

## 3 The proof of Theorem 1.1

Write $\alpha=|\mathcal{R}|/m$ and $\beta=s/m$, by Lemma 2.1 we get

$$\begin{aligned}\alpha m &= |\mathcal{R}| = \sum_{\substack{1\leq n\leq m\\ 0\leq r_m(f(n)-r)<s}} 1 = \sum_{\substack{1\leq n\leq m\\ 0\leq r_m(f(n)-r)<\beta m}} 1 = \sum_{1\leq n\leq m}(g_\beta(f(n)-r)+\beta)\\ &= \sum_{1\leq n\leq m}\sum_{|h|<m/2} a_h e_m(h(f(n)-r))+\beta m\\ &= \sum_{|h|<m/2} a_h e_m(-hr)\sum_{1\leq n\leq m} e_m(hf(n))+\beta m.\end{aligned}$$

From Lemma 2.1 we know that

$$\sum_{\substack{|h|<m/2\\ (h,m)>1}} a_h e_m(-hr) \ll \frac{1}{m}+\sum_{\substack{0<|h|<m/2\\ (h,m)>1}}\frac{1}{|h|} \ll m^{-1/2}\log m. \tag{3.1}$$

Then from Lemma 2.2 we have

$$|\alpha-\beta| \ll \frac{1}{m}\sum_{\substack{|h|<m/2\\ (h,m)=1}}\frac{1}{|h|}\left|\sum_{1\leq n\leq m} e_m(hf(n))\right| + m^{-1/2}\log m$$

$$\ll \quad (k-1)^2 m^{-1/2}\log m. \tag{3.2}$$

Furthermore, noting that

$$e_n = \begin{cases} 1-\frac{|R|}{m}, & \text{for } n\in R,\\ -\frac{|R|}{m}, & \text{for } n\notin R. \end{cases}$$

Then from Lemma 2.1 we get

$$e_n = g_\beta(f(n)-r)+\beta-\alpha. \tag{3.3}$$

For $a,b,t\in\mathbb{N}$ with $1\le a\le a+(t-1)b\le m$, we assume that $(b,m)=1$ since otherwise we have

$$\left|\sum_{j=0}^{t-1} e_{a+jb}\right| \le t\le \frac{m}{b}+1\ll m^{1/2}.$$

By (3.1)-(3.3), Lemma 2.1 and Lemma 2.2 we get

$$\begin{aligned}
\sum_{j=0}^{t-1} e_{a+jb} &= \sum_{j=0}^{t-1}(g_\beta(f(a+jb)-r)+\beta-\alpha)\\
&= \sum_{|h|<m/2} a_h e_m(-hr)\sum_{j=0}^{t-1} e_m(hf(a+jb))+t(\beta-\alpha)\\
&= \sum_{\substack{|h|<m/2\\(h,m)=1}} a_h e_m(-hr)\sum_{j=0}^{t-1} e_m(hf(a+jb))+O\left((k-1)^2 m^{1/2}\log m\right)\\
&\ll k^2 m^{1/2}(\log m)^2.
\end{aligned}$$

Therefore

$$W(\mathcal{R},m)=\max_{a,b,t}\left|\sum_{j=0}^{t-1} e_{a+jb}\right| \ll k^2 m^{1/2}(\log m)^2.$$

For $M,d_1,d_2\in\mathbb{N}$ with $0\le d_1<d_2\le m-M$, by (3.1)-(3.3) and Lemma 2.1 we have

$$\begin{aligned}
&\sum_{n=1}^{M} e_{n+d_1}e_{n+d_2} = \sum_{n=1}^{M}\left(g_\beta(f(n+d_1)-r)+\beta-\alpha\right)\left(g_\beta(f(n+d_2)-r)+\beta-\alpha\right)\\
&= \sum_{n=1}^{M} g_\beta(f(n+d_1)-r)g_\beta(f(n+d_2)-r)+O\left((k-1)^2 m^{1/2}\log m\right)\\
&= \frac{1}{m}\sum_{|z|<m/2}\sum_{j=1}^{M} e_m(-zj)\sum_{n=1}^{m} g_\beta(f(n+d_1)-r)g_\beta(f(n+d_2)-r)e_m(zn)\\
&\quad +O\left((k-1)^2 m^{1/2}\log m\right)\\
&= \frac{1}{m}\sum_{|z|<m/2}\sum_{j=1}^{M} e_m(-zj)\sum_{|h_1|<m/2} a_{h_1}e_m(-h_1 r)\sum_{|h_2|<m/2} a_{h_2}e_m(-h_2 r)
\end{aligned}$$

$$
\begin{aligned}
&\times \sum_{n=1}^{m} e_m(h_1 f(n+d_1) + h_2 f(n+d_2) + zn) + O\left((k-1)^2 m^{1/2} \log m\right) \\
&= \frac{1}{m} \sum_{|z|<m/2} \sum_{j=1}^{M} e_m(-zj) \sum_{\substack{|h_1|<m/2 \\ (h_1,m)=1}} a_{h_1} e_m(-h_1 r) \sum_{\substack{|h_2|<m/2 \\ (h_2,m)=1}} a_{h_2} e_m(-h_2 r) \\
&\times \sum_{n=1}^{m} e_m\left(h_1 f(n+d_1) + h_2 f(n+d_2) + zn\right) \\
&+ O\left((k-1)^2 m^{1/2} \log m\right) + O\left(m^{1/2} (\log m)^3\right). \qquad (3.4)
\end{aligned}
$$

Define $F_1(n) = h_1 f(n+d_1) + h_2 f(n+d_2) + zn$. From Lemma 2.3 we get

$$
\begin{aligned}
&\left| \sum_{n=1}^{m} e_m\left(h_1 f(n+d_1) + h_2 f(n+d_2) + zn\right) \right| \\
&= \left| \sum_{n=1}^{m} e_m\left(F_1(n)\right) \right| = \left| \sum_{u=1}^{q} e_q\left(i_q(p)(F_1(u))\right) \right| \cdot \left| \sum_{v=1}^{p} e_p\left(i_p(q)(F_1(v))\right) \right|.
\end{aligned}
$$

If $d_1 \not\equiv d_2 (\bmod\ p)$, by Lemma 2.4 and Lemma 2.5 we have

$$
\sum_{v=1}^{p} e_p\left(i_p(q)(F_1(v))\right) \ll k p^{1/2}.
$$

While if $d_1 \equiv d_2 (\bmod\ p)$, by Lemma 2.4 and Lemma 2.5 we also have

$$
\begin{aligned}
\sum_{v=1}^{p} e_p\left(i_p(q)(F_1(v))\right) &= \begin{cases} O\left(k p^{1/2}\right), & \text{if } p \nmid h_1 + h_2, \\ O(p), & \text{if } p \mid h_1 + h_2 \text{ and } p \mid z, \\ 0, & \text{if } p \mid h_1 + h_2 \text{ and } p \nmid z, \end{cases} \\
&= \begin{cases} O(p), & \text{if } p \mid h_1 + h_2 \text{ and } p \mid z, \\ O\left(k p^{1/2}\right), & \text{otherwise.} \end{cases}
\end{aligned}
$$

Therefore

$$
\begin{aligned}
&\left| \sum_{n=1}^{m} e_m\left(h_1 f(n+d_1) + h_2 f(n+d_2) + zn\right) \right| \\
&= \begin{cases} O(k m^{3/4}), & \text{if } p \mid h_1 + h_2, p \mid z, \text{ or } q \mid h_1 + h_2, q \mid z, \\ O\left(k^2 m^{1/2}\right), & \text{otherwise.} \end{cases} \qquad (3.5)
\end{aligned}
$$

Now from (3.4), (3.5) and Lemma 2.1 we get

$$
\begin{aligned}
&\sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \\
&\ll \frac{1}{m} \sum_{\substack{|z|<m/2 \\ p \mid z}} \left| \sum_{j=1}^{M} e_m(-zj) \right| \sum_{\substack{|h_1|<m/2 \\ (h_1,m)=1}} \sum_{\substack{|h_2|<m/2 \\ (h_2,m)=1 \\ p \mid h_1 + h_2}} \frac{1}{|h_1 h_2|} \cdot k m^{3/4}
\end{aligned}
$$

$$
\begin{aligned}
&+\frac{1}{m}\sum_{\substack{|z|<m/2\\ q|z}}\left|\sum_{j=1}^{M}e_m(-zj)\right|\sum_{\substack{|h_1|<m/2\\ (h_1,m)=1}}\sum_{\substack{|h_2|<m/2\\ (h_2,m)=1\\ q|h_1+h_2}}\frac{1}{|h_1h_2|}\cdot km^{3/4}\\
&+\frac{1}{m}\sum_{|z|<m/2}\left|\sum_{j=1}^{M}e_m(-zj)\right|\sum_{\substack{|h_1|<m/2\\ (h_1,m)=1}}\sum_{\substack{|h_2|<m/2\\ (h_2,m)=1}}\frac{1}{|h_1h_2|}\cdot k^2m^{1/2}\\
&+(k-1)^2m^{1/2}\log m+m^{1/2}(\log m)^3\\
\ll\ & km^{3/4}.
\end{aligned}
$$

Therefore

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

Now let $M\in\mathbb{N}$, $d_1,d_2,d_3\in\mathbb{Z}$ such that $0\le d_1<d_2<d_3\le m-M$. By (3.1)-(3.3) and Lemma 2.1 we have

$$
\begin{aligned}
\sum_{n=1}^{M}e_{n+d_1}e_{n+d_2}e_{n+d_3}&=\sum_{n=1}^{M}\left(g_\beta(f(n+d_1)-r)+\beta-\alpha\right)\left(g_\beta(f(n+d_2)-r)+\beta-\alpha\right)\\
&\qquad\times\left(g_\beta(f(n+d_3)-r)+\beta-\alpha\right)\\
&=\sum_{n=1}^{M}g_\beta(f(n+d_1)-r)g_\beta(f(n+d_2)-r)g_\beta(f(n+d_3)-r)+O\left((k-1)^2m^{1/2}\log m\right)\\
&=\frac{1}{m}\sum_{|z|<m/2}\sum_{j=1}^{M}e_m(-zj)\sum_{n=1}^{m}g_\beta(f(n+d_1)-r)g_\beta(f(n+d_2)-r)g_\beta(f(n+d_3)-r)e_m(zn)\\
&\qquad+O\left((k-1)^2m^{1/2}\log m\right)\\
&=\frac{1}{m}\sum_{|z|<m/2}\sum_{j=1}^{M}e_m(-zj)\sum_{|h_1|<m/2}a_{h_1}e_m(-h_1r)\sum_{|h_2|<m/2}a_{h_2}e_m(-h_2r)\sum_{|h_3|<m/2}a_{h_3}e_m(-h_3r)\\
&\qquad\times\sum_{n=1}^{m}e_m(h_1f(n+d_1)+h_2f(n+d_2)+h_3f(n+d_3)+zn)+O\left((k-1)^2m^{1/2}\log m\right)\\
&=\frac{1}{m}\sum_{|z|<m/2}\sum_{j=1}^{M}e_m(-zj)\sum_{\substack{|h_1|<m/2\\ (h_1,m)=1}}a_{h_1}e_m(-h_1r)\sum_{\substack{|h_2|<m/2\\ (h_2,m)=1}}a_{h_2}e_m(-h_2r)\sum_{\substack{|h_3|<m/2\\ (h_3,m)=1}}a_{h_3}e_m(-h_3r)\\
&\qquad\times\sum_{n=1}^{m}e_m\left(h_1f(n+d_1)+h_2f(n+d_2)+h_3f(n+d_3)+zn\right)\\
&\qquad+O\left((k-1)^2m^{1/2}\log m\right)+O\left(m^{1/2}(\log m)^4\right).
\end{aligned}
\tag{3.6}
$$

Define $F_2(n)=h_1f(n+d_1)+h_2f(n+d_2)+h_3f(n+d_3)+zn$. From Lemma 2.3 we get

$$
\left|\sum_{n=1}^{m}e_m\left(h_1f(n+d_1)+h_2f(n+d_2)+h_3f(n+d_3)+zn\right)\right|
$$

$$= \left| \sum_{n=1}^{m} e_m\left(F_2(n)\right) \right| = \left| \sum_{u=1}^{q} e_q\left(i_q(p)(F_2(u))\right) \right| \cdot \left| \sum_{v=1}^{p} e_p\left(i_p(q)(F_2(v))\right) \right|.$$

If $d_1, d_2, d_3$ are different in $\mathbb{F}_p$, by Lemma 2.4 and Lemma 2.5 we have

$$\sum_{v=1}^{p} e_p\left(i_p(q)(F_2(v))\right) \ll kp^{1/2}.$$

If $d_1 \equiv d_2 \not\equiv d_3 (\bmod\ p)$, by Lemma 2.4 and Lemma 2.5 we get

$$\sum_{v=1}^{p} e_p\left(i_p(q)(F_2(v))\right) \ll kp^{1/2}.$$

While if $d_1 \equiv d_2 \equiv d_3 (\bmod\ p)$, by Lemma 2.4 and Lemma 2.5 we also get

$$\begin{aligned}\sum_{v=1}^{p} e_p\left(i_p(q)(F_2(v))\right) &= \begin{cases} O\left(kp^{1/2}\right), & \text{if } p \nmid h_1+h_2+h_3, \\ O(p), & \text{if } p \mid h_1+h_2+h_3 \text{ and } p \mid z, \\ 0, & \text{if } p \mid h_1+h_2+h_3 \text{ and } p \nmid z, \end{cases} \\ &= \begin{cases} O(p), & \text{if } p \mid h_1+h_2+h_3 \text{ and } p \mid z, \\ O\left(kp^{1/2}\right), & \text{otherwise.} \end{cases}\end{aligned}$$

Therefore

$$\begin{aligned}&\left| \sum_{n=1}^{m} e_m\left(h_1 f(n+d_1) + h_2 f(n+d_2) + h_3 f(n+d_3) + zn\right) \right| \\ &= \begin{cases} O(km^{3/4}), & \text{if } p \mid h_1+h_2+h_3, p \mid z, \text{ or } q \mid h_1+h_2+h_3, q \mid z, \\ O\left(k^2 m^{1/2}\right), & \text{otherwise.} \end{cases}\end{aligned} \tag{3.7}$$

Now from (3.6), (3.7) and Lemma 2.1 we get

$$\begin{aligned}&\sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} e_{n+d_3} \\ &\ll \frac{1}{m} \sum_{\substack{|z|<m/2 \\ p|z}} \left| \sum_{j=1}^{M} e_m(-zj) \right| \sum_{\substack{|h_1|<m/2 \\ (h_1,m)=1}} \sum_{\substack{|h_2|<m/2 \\ (h_2,m)=1 \\ p|h_1+h_2+h_3}} \sum_{\substack{|h_3|<m/2 \\ (h_3,m)=1}} \frac{1}{|h_1 h_2 h_3|} \cdot km^{3/4} \\ &\quad + \frac{1}{m} \sum_{\substack{|z|<m/2 \\ q|z}} \left| \sum_{j=1}^{M} e_m(-zj) \right| \sum_{\substack{|h_1|<m/2 \\ (h_1,m)=1}} \sum_{\substack{|h_2|<m/2 \\ (h_2,m)=1 \\ q|h_1+h_2+h_3}} \sum_{\substack{|h_3|<m/2 \\ (h_3,m)=1}} \frac{1}{|h_1 h_2 h_3|} \cdot km^{3/4} \\ &\quad + \frac{1}{m} \sum_{|z|<m/2} \left| \sum_{j=1}^{M} e_m(-zj) \right| \sum_{\substack{|h_1|<m/2 \\ (h_1,m)=1}} \sum_{\substack{|h_2|<m/2 \\ (h_2,m)=1}} \sum_{\substack{|h_3|<m/2 \\ (h_3,m)=1}} \frac{1}{|h_1 h_2 h_3|} \cdot k^2 m^{1/2}\end{aligned}$$

$$\begin{aligned} &+(k-1)^2 m^{1/2}\log m + m^{1/2}(\log m)^4 \\ \ll\ & km^{3/4}\log m. \end{aligned}$$

Therefore

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

This proves Theorem 1.1.

## 4 The proof of Theorem 1.2

Write $\alpha = |\mathcal{R}|/m$ and $\beta = s/m$. By (3.1), Lemma 2.1 and Lemma 2.6 we get

$$\begin{aligned} \alpha m &= |\mathcal{R}| = \sum_{\substack{n=1 \\ (f(n),m)=1 \\ 0\le r_m(i_m(f(n))-r)<s}}^{m} 1 = \sum_{\substack{n=1 \\ (f(n),m)=1}}^{m} \left(g_\beta(i_m(f(n))-r)+\beta\right) \\ &= \sum_{|h|<m/2} a_h e_m(-hr) \sum_{\substack{n=1 \\ (f(n),m)=1}}^{m} e_m(hi_m(f(n))) + \beta m + O\left(km^{1/2}\right) \\ &= \sum_{\substack{|h|<m/2 \\ (h,m)=1}} a_h e_m(-hr) \sum_{\substack{n=1 \\ (f(n),m)=1}}^{m} e_m(hi_m(f(n))) + \beta m + O\left(km^{1/2}\right) \\ &\qquad + O\left(m^{1/2}\log m\right) \\ &= \beta m + O\left(k^2 m^{1/2}\log m\right). \end{aligned}$$

That is to say,

$$|\alpha-\beta| \ll k^2 m^{-1/2}\log m. \tag{4.1}$$

Furthermore, from Lemma 2.1 we can get

$$e_n = g_\beta(i_m(f(n))-r)+\beta-\alpha \quad \text{for} \quad (f(n),m)=1. \tag{4.2}$$

For $a, b, t \in \mathbb{N}$ with $1 \le a \le a+(t-1)b \le m$, we assume that $(b,m)=1$ since otherwise we have

$$\left|\sum_{j=0}^{t-1} e_{a+jb}\right| \le t \le \frac{m}{b}+1 \ll m^{1/2}.$$

By (3.1), (4.1), (4.2), Lemma 2.1 and Lemma 2.6 we get

$$\begin{aligned}\sum_{j=0}^{t-1} e_{a+jb} &= \sum_{\substack{j=0\\(f(a+jb),m)=1}}^{t-1} \left(g_\beta(i_m(f(a+jb))-r)+\beta-\alpha\right)+O\left(km^{1/2}\right)\\
&= \sum_{|h|<m/2} a_h e_m(-hr) \sum_{\substack{j=0\\(f(a+jb),m)=1}}^{t-1} e_m(hi_m(f(a+jb)))+t(\beta-\alpha)\\
&\qquad +O\left(km^{1/2}\right)\\
&= \sum_{\substack{|h|<m/2\\(h,m)=1}} a_h e_m(-hr) \sum_{\substack{j=0\\(f(a+jb),m)=1}}^{t-1} e_m(hi_m(f(a+jb)))\\
&\qquad +O\left(k^2m^{1/2}\log m\right)\\
&\ll k^2m^{1/2}(\log m)^2.\end{aligned}$$

Therefore

$$W(\mathcal{R},m)=\max_{a,b,t}\left|\sum_{j=0}^{t-1} e_{a+jb}\right| \ll k^2m^{1/2}(\log m)^2.$$

For $M, d_1, d_2 \in \mathbb{N}$ with $0 \le d_1 < d_2 \le m-M$, by (3.1), (4.1), (4.2) and Lemma 2.1 we have

$$\begin{aligned}\sum_{n=1}^{M} e_{n+d_1}e_{n+d_2} &= \sum_{\substack{n=1\\(f(n+d_1)f(n+d_2),m)=1}}^{M} \left(g_\beta(i_m(f(n+d_1))-r)+\beta-\alpha\right)\\
&\quad\times\left(g_\beta(i_m(f(n+d_2))-r)+\beta-\alpha\right)+O\left(km^{1/2}\right)\\
&= \sum_{\substack{n=1\\(f(n+d_1)f(n+d_2),m)=1}}^{M} g_\beta(i_m(f(n+d_1))-r)g_\beta(i_m(f(n+d_2))-r)\\
&\qquad +O\left(k^2m^{1/2}\log m\right)\\
&= \frac{1}{m}\sum_{|z|<m/2}\sum_{j=1}^{M} e_m(-zj) \sum_{\substack{n=1\\(f(n+d_1)f(n+d_2),m)=1}}^{m} g_\beta(i_m(f(n+d_1))-r)\\
&\quad\times g_\beta(i_m(f(n+d_2))-r)e_m(zn)+O\left(k^2m^{1/2}\log m\right)\\
&= \frac{1}{m}\sum_{|z|<m/2}\sum_{j=1}^{M} e_m(-zj)\sum_{|h_1|<m/2} a_{h_1}e_m(-h_1r)\sum_{|h_2|<m/2} a_{h_2}e_m(-h_2r)\\
&\quad\times \sum_{\substack{n=1\\(f(n+d_1)f(n+d_2),m)=1}}^{m} e_m(h_1i_m(f(n+d_1))+h_2i_m(f(n+d_2))+zn)\\
&\qquad +O\left(k^2m^{1/2}\log m\right)\end{aligned}$$

$$= \frac{1}{m} \sum_{|z|<m/2} \sum_{j=1}^{M} e_m(-zj) \sum_{\substack{|h_1|<m/2 \\ (h_1,m)=1}} a_{h_1} e_m(-h_1 r) \sum_{\substack{|h_2|<m/2 \\ (h_2,m)=1}} a_{h_2} e_m(-h_2 r)$$
$$\times \sum_{\substack{n=1 \\ (f(n+d_1)f(n+d_2),m)=1}}^{m} e_m\left(h_1 i_m(f(n+d_1)) + h_2 i_m(f(n+d_2)) + zn\right)$$
$$+O\left(k^2 m^{1/2} \log m\right) + O\left(m^{1/2} (\log m)^3\right). \tag{4.3}$$

Define

$$Q_1(n) = h_1 f(n+d_2) + h_2 f(n+d_1) + znf(n+d_1)f(n+d_2),$$

and $R_1(n) = f(n+d_1)f(n+d_2)$. From Lemma 2.7 we get

$$\left| \sum_{\substack{n=1 \\ (f(n+d_1)f(n+d_2),m)=1}}^{m} e_m\left(h_1 i_m(f(n+d_1)) + h_2 i_m(f(n+d_2)) + zn\right) \right|$$
$$= \left| \sum_{\substack{n=1 \\ (R_1(n),m)=1}}^{m} e_m\left(Q_1(n) i_m(R_1(n))\right) \right|$$
$$= \left| \sum_{\substack{u=1 \\ (R_1(u),q)=1}}^{q} e_q\left(Q_1(u) i_q(pR_1(u))\right) \right| \cdot \left| \sum_{\substack{v=1 \\ (R_1(v),p)=1}}^{p} e_p\left(Q_1(v) i_p(qR_1(v))\right) \right|.$$

If $d_1 \not\equiv d_2 (\bmod\ p)$, by Lemma 2.8 and Lemma 2.9 we have

$$\sum_{\substack{v=1 \\ (R_1(v),p)=1}}^{p} e_p\left(Q_1(v) i_p(qR_1(v))\right) \ll dp^{1/2}.$$

While if $d_1 \equiv d_2 (\bmod\ p)$, by Lemma 2.8 and Lemma 2.9 we also have

$$\sum_{\substack{v=1 \\ (R_1(v),p)=1}}^{p} e_p\left(Q_1(v) i_p(qR_1(v))\right) = \begin{cases} O\left(kp^{1/2}\right), & \text{if } p \nmid h_1 + h_2, \\ O(p), & \text{if } p \mid h_1 + h_2 \text{ and } p \mid z, \\ O(k), & \text{if } p \mid h_1 + h_2 \text{ and } p \nmid z, \end{cases}$$
$$= \begin{cases} O(p), & \text{if } p \mid h_1 + h_2 \text{ and } p \mid z, \\ O\left(kp^{1/2}\right), & \text{otherwise.} \end{cases}$$

Therefore

$$\left| \sum_{\substack{n=1 \\ (f(n+d_1)f(n+d_2),m)=1}}^{m} e_m\left(h_1 i_m(f(n+d_1)) + h_2 i_m(f(n+d_2)) + zn\right) \right|$$

$$= \begin{cases} O(km^{3/4}), & \text{if } p \mid h_1+h_2, p \mid z, \text{ or } q \mid h_1+h_2, q \mid z, \\ O\left(k^2 m^{1/2}\right), & \text{otherwise.} \end{cases} \tag{4.4}$$

Now from (4.3), (4.4) and Lemma 2.1 we get

$$\begin{aligned}
&\sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \\
&\ll \frac{1}{m} \sum_{\substack{|z|<m/2 \\ p|z}} \left| \sum_{j=1}^{M} e_m(-zj) \right| \sum_{\substack{|h_1|<m/2 \\ (h_1,m)=1}} \sum_{\substack{|h_2|<m/2 \\ (h_2,m)=1 \\ p|h_1+h_2}} \frac{1}{|h_1 h_2|} \cdot km^{3/4} \\
&\quad + \frac{1}{m} \sum_{\substack{|z|<m/2 \\ q|z}} \left| \sum_{j=1}^{M} e_m(-zj) \right| \sum_{\substack{|h_1|<m/2 \\ (h_1,m)=1}} \sum_{\substack{|h_2|<m/2 \\ (h_2,m)=1 \\ q|h_1+h_2}} \frac{1}{|h_1 h_2|} \cdot km^{3/4} \\
&\quad + \frac{1}{m} \sum_{|z|<m/2} \left| \sum_{j=1}^{M} e_m(-zj) \right| \sum_{\substack{|h_1|<m/2 \\ (h_1,m)=1}} \sum_{\substack{|h_2|<m/2 \\ (h_2,m)=1}} \frac{1}{|h_1 h_2|} \cdot k^2 m^{1/2} \\
&\quad + k^2 m^{1/2} \log m + m^{1/2} (\log m)^3 \\
&\ll km^{3/4}.
\end{aligned}$$

Therefore

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

For $M, d_1, d_2, d_3 \in \mathbb{N}$ with $0 \le d_1 < d_2 < d_3 \le m - M$, by (3.1), (4.1), (4.2) and Lemma 2.1 we have

$$\begin{aligned}
\sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} e_{n+d_3} &= \sum_{\substack{n=1 \\ (f(n+d_1)f(n+d_2)f(n+d_3),m)=1}}^{M} \left( g_\beta(i_m(f(n+d_1))-r) + \beta - \alpha \right) \\
&\quad \times \left( g_\beta(i_m(f(n+d_2))-r) + \beta - \alpha \right) \left( g_\beta(i_m(f(n+d_3))-r) + \beta - \alpha \right) + O\left(km^{1/2}\right) \\
&= \sum_{\substack{n=1 \\ (f(n+d_1)f(n+d_2)f(n+d_3),m)=1}}^{M} g_\beta(i_m(f(n+d_1))-r) g_\beta(i_m(f(n+d_2))-r) \\
&\quad \times g_\beta(i_m(f(n+d_3))-r) + O\left(k^2 m^{1/2} \log m\right) \\
&= \frac{1}{m} \sum_{|z|<m/2} \sum_{j=1}^{M} e_m(-zj) \sum_{\substack{n=1 \\ (f(n+d_1)f(n+d_2)f(n+d_3),m)=1}}^{m} g_\beta(i_m(f(n+d_1))-r) \\
&\quad \times g_\beta(i_m(f(n+d_2))-r) g_\beta(i_m(f(n+d_3))-r) e_m(zn) + O\left(k^2 m^{1/2} \log m\right) \\
&= \frac{1}{m} \sum_{|z|<m/2} \sum_{j=1}^{M} e_m(-zj) \sum_{|h_1|<m/2} a_{h_1} e_m(-h_1 r) \sum_{|h_2|<m/2} a_{h_2} e_m(-h_2 r) \sum_{|h_3|<m/2} a_{h_3} e_m(-h_3 r)
\end{aligned}$$

$$
\begin{aligned}
&\times \sum_{\substack{n=1\\(f(n+d_1)f(n+d_2)f(n+d_3),m)=1}}^{m} e_m(h_1 i_m(f(n+d_1))+h_2 i_m(f(n+d_2)))\\
&\times e_m(h_3 i_m(f(n+d_3))+zn)+O\left(k^2 m^{1/2}\log m\right)\\
=&\ \frac{1}{m}\sum_{|z|<m/2}\sum_{j=1}^{M} e_m(-zj)\sum_{\substack{|h_1|<m/2\\(h_1,m)=1}} a_{h_1}e_m(-h_1 r)\sum_{\substack{|h_2|<m/2\\(h_2,m)=1}} a_{h_2}e_m(-h_2 r)\sum_{\substack{|h_3|<m/2\\(h_3,m)=1}} a_{h_3}e_m(-h_3 r)\\
&\times \sum_{\substack{n=1\\(f(n+d_1)f(n+d_2)f(n+d_3),m)=1}}^{m} e_m(h_1 i_m(f(n+d_1))+h_2 i_m(f(n+d_2)))\\
&\times e_m(h_3 i_m(f(n+d_3))+zn)+O\left(k^2 m^{1/2}\log m\right)+O\left(m^{1/2}(\log m)^4\right). \qquad (4.5)
\end{aligned}
$$

Define

$$
\begin{aligned}
Q_2(n) \;=\;& h_1 f(n+d_2)f(n+d_3)+h_2 f(n+d_1)f(n+d_3)+h_3 f(n+d_1)f(n+d_2)\\
&+znf(n+d_1)f(n+d_2)f(n+d_3),
\end{aligned}
$$

and $R_2(n)=f(n+d_1)f(n+d_2)f(n+d_3)$. From Lemma 2.7 we get

$$
\begin{aligned}
&\left|\sum_{\substack{n=1\\(f(n+d_1)f(n+d_2)f(n+d_3),m)=1}}^{m} e_m(h_1 i_m(f(n+d_1))+h_2 i_m(f(n+d_2)))\right.\\
&\qquad\left.\times e_m(h_3 i_m(f(n+d_3))+zn)\right|\\
=&\left|\sum_{\substack{n=1\\(R_2(n),m)=1}}^{m} e_m\left(Q_2(n)i_m(R_2(n))\right)\right|\\
=&\left|\sum_{\substack{u=1\\(R_2(u),q)=1}}^{q} e_q\left(Q_2(u)i_q(pR_2(u))\right)\right|\cdot\left|\sum_{\substack{v=1\\(R_2(v),p)=1}}^{p} e_p\left(Q_2(v)i_p(qR_2(v))\right)\right|.
\end{aligned}
$$

If $d_1, d_2, d_3$ are different in $\mathbb{F}_p$, by Lemma 2.8 and Lemma 2.9 we have

$$
\sum_{\substack{v=1\\(R_2(v),p)=1}}^{p} e_p\left(Q_2(v)i_p(qR_2(v))\right)\ll kp^{1/2}.
$$

If $d_1\equiv d_2\not\equiv d_3(\bmod\ p)$, by Lemma 2.8 and Lemma 2.9 we get

$$
\sum_{\substack{v=1\\(R_2(v),p)=1}}^{p} e_p\left(Q_2(v)i_p(qR_2(v))\right)\ll kp^{1/2}.
$$

While if $d_1 \equiv d_2 \equiv d_3 (\bmod\ p)$, from Lemma 2.8 and Lemma 2.9 we also get

$$\begin{aligned}\sum_{\substack{v=1\\(R_2(v),p)=1}}^{p} e_p\left(Q_2(v) i_p(q R_2(v))\right) &= \begin{cases} O\left(kp^{1/2}\right), & \text{if } p \nmid h_1+h_2+h_3,\\ O(p), & \text{if } p \mid h_1+h_2+h_3 \text{ and } p \mid z,\\ O\left(k\right), & \text{if } p \mid h_1+h_2+h_3 \text{ and } p \nmid z,\end{cases}\\ &= \begin{cases} O(p), & \text{if } p \mid h_1+h_2+h_3 \text{ and } p \mid z,\\ O\left(kp^{1/2}\right), & \text{otherwise.}\end{cases}\end{aligned}$$

Therefore

$$\begin{aligned}&\left|\sum_{\substack{n=1\\(f(n+d_1)f(n+d_2)f(n+d_3),m)=1}}^{m} e_m(h_1 i_m(f(n+d_1)) + h_2 i_m(f(n+d_2)))\right.\\ &\qquad \left.\times e_m(h_3 i_m(f(n+d_3)) + zn)\right|\\ &= \begin{cases} O(km^{3/4}), & \text{if } p \mid h_1+h_2+h_3, p \mid z, \text{ or } q \mid h_1+h_2+h_3, q \mid z,\\ O\left(k^2 m^{1/2}\right), & \text{otherwise.}\end{cases} \qquad (4.6)\end{aligned}$$

Now from (4.5), (4.6) and Lemma 2.1 we get

$$\begin{aligned}&\sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} e_{n+d_3}\\ &\ll \frac{1}{m} \sum_{\substack{|z|<m/2\\ p|z}} \left|\sum_{j=1}^{M} e_m(-zj)\right| \sum_{\substack{|h_1|<m/2\\(h_1,m)=1}} \sum_{\substack{|h_2|<m/2\\(h_2,m)=1\\p|h_1+h_2+h_3}} \sum_{\substack{|h_3|<m/2\\(h_3,m)=1}} \frac{1}{|h_1 h_2 h_3|} \cdot km^{3/4}\\ &\quad + \frac{1}{m} \sum_{\substack{|z|<m/2\\ q|z}} \left|\sum_{j=1}^{M} e_m(-zj)\right| \sum_{\substack{|h_1|<m/2\\(h_1,m)=1}} \sum_{\substack{|h_2|<m/2\\(h_2,m)=1\\q|h_1+h_2+h_3}} \sum_{\substack{|h_3|<m/2\\(h_3,m)=1}} \frac{1}{|h_1 h_2 h_3|} \cdot km^{3/4}\\ &\quad + \frac{1}{m} \sum_{|z|<m/2} \left|\sum_{j=1}^{M} e_m(-zj)\right| \sum_{\substack{|h_1|<m/2\\(h_1,m)=1}} \sum_{\substack{|h_2|<m/2\\(h_2,m)=1}} \sum_{\substack{|h_3|<m/2\\(h_3,m)=1}} \frac{1}{|h_1 h_2 h_3|} \cdot k^2 m^{1/2}\\ &\quad + k^2 m^{1/2} \log m + m^{1/2} (\log m)^4\\ &\ll km^{3/4} \log m.\end{aligned}$$

Therefore

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

This completes the proof of Theorem 1.2.

## 5 Proof of Theorem 1.3 and Theorem 1.4

First we prove Theorem 1.3. Let $M \in \mathbb{N}$, $4l \in \mathbb{N}$ with $1 \le l \le \min((k-1)/2, q-p+1)$. Choosing $d_1, \cdots, d_{4l} \in \mathbb{Z}$ such that $0 \le d_1 < \cdots < d_{4l} \le m - M$ and

$$\begin{cases} d_i \equiv d_j (\operatorname{mod} p), & \text{if } 2 \nmid i \text{ and } j = i+1, \\ d_i \not\equiv d_j (\operatorname{mod} p), & \text{otherwise.} \end{cases} \tag{5.1}$$

$$\begin{cases} d_i \equiv d_j (\operatorname{mod} q), & \text{if either } (i,j) = (4k+1, 4k+3) \text{ or } (i,j) = (4k+2, 4k+4), \\ d_i \not\equiv d_j (\operatorname{mod} q), & \text{otherwise.} \end{cases} \tag{5.2}$$

By (3.2), (3.3) and Lemma 2.1 we have

$$\begin{aligned} &\sum_{n=1}^{M} e_{n+d_1} \cdots e_{n+d_{4l}} \\ &= \sum_{n=1}^{M} \big(g_\beta(f(n+d_1) - r) + \beta - \alpha\big) \cdots \big(g_\beta(f(n+d_{4l}) - r) + \beta - \alpha\big) \\ &= \sum_{n=1}^{M} g_\beta(f(n+d_1) - r) \cdots g_\beta(f(n+d_{4l}) - r) + O\left((k-1)^2 m^{1/2} \log m\right) \\ &= \sum_{|h_1| < m/2} a_{h_1} e_m(-h_1 r) \cdots \sum_{|h_{4l}| < m/2} a_{h_{4l}} e_m(-h_{4l} r) \\ &\quad \times \sum_{n=1}^{M} e_m\left(h_1 f(n+d_1) + \cdots + h_{4l} f(n+d_{4l})\right) \\ &\qquad + O\left((k-1)^2 m^{1/2} \log m\right). \end{aligned} \tag{5.3}$$

Using the methods in proving Theorem 1.3 of [3] we have

$$\begin{aligned} &\sum_{n=1}^{M} e_m\left(h_1 f(n+d_1) + \cdots + h_{4l} f(n+d_{4l})\right) \\ &= \begin{cases} M, & \text{if } p \mid h_{2j-1} + h_{2j}, j = 1, \cdots, 2l, \\ & \quad q \mid h_{4k+1} + h_{4k+3}, q \mid h_{4k+2} + h_{4k+4}, \\ & \qquad k = 0, \cdots, l-1, \\ O\left(d m^{3/4} \log m\right), & \text{otherwise.} \end{cases} \end{aligned} \tag{5.4}$$

Then from (5.3), (5.4), Lemma 2.1 and Lemma 2.10 we can get

$$\begin{aligned} &\sum_{n=1}^{M} e_{n+d_1} \cdots e_{n+d_{4l}} \\ &= M \sum_{\substack{|h_1| < m/2 \\ p \mid h_{2j-1} + h_{2j},\, j = 1, \cdots, 2l \\ q \mid h_{4k+1} + h_{4k+3},\, q \mid h_{4k+2} + h_{4k+4},\, k = 0, \cdots, l-1}} \cdots \sum_{|h_{4l}| < m/2} a_{h_1} e_m(-h_1 r) \cdots a_{h_{4l}} e_m(-h_{4l} r) \\ &\quad + O\left(\left(\sum_{|h| < m/2} |a_h e_m(-hr)|\right)^{4l} d m^{3/4} \log m\right) \end{aligned}$$

$$
\begin{aligned}
&= M \sum_{\substack{|h_1|<m/2 \\ p|h_{2j-1}+h_{2j},\ j=1,\cdots,2l \\ q|h_{4k+1}+h_{4k+3},\ q|h_{4k+2}+h_{4k+4},\ k=0,\cdots,l-1}} \cdots \sum_{|h_{4l}|<m/2} a_{h_1} e_m(-h_1 r) \cdots a_{h_{4l}} e_m(-h_{4l} r) \\
&\quad + O\left(dm^{3/4}(\log m)^{4l+1}\right) \\
&= M \sum_{\substack{|h_1|<m/2 \\ h_{2j-1}+h_{2j}=0,\ j=1,\cdots,2l \\ h_{4k+1}+h_{4k+3}=h_{4k+2}+h_{4k+4}=0,\ k=0,\cdots,l-1}} \cdots \sum_{|h_{4l}|<m/2} a_{h_1} e_m(-h_1 r) \cdots a_{h_{4l}} e_m(-h_{4l} r) \\
&\quad + O\left(dm^{3/4}(\log m)^{4l+1}\right) \\
&= M \left( \sum_{|h|<m/2} (a_h e_m(-hr) a_{-h} e_m(hr))^2 \right)^l + O\left(dm^{3/4}(\log m)^{4l+1}\right) \\
&= M \left( \sum_{|h|<m/2} a_h^2 a_{-h}^2 \right)^l + O\left(dm^{3/4}(\log m)^{4l+1}\right) \\
&= M \left( \sum_{\substack{|h|<m/2 \\ h\neq 0}} a_h^2 a_{-h}^2 \right)^l + O\left(dm^{3/4}(\log m)^{4l+1}\right). \qquad (5.5)
\end{aligned}
$$

For $|h| < m/2$ and $h \neq 0$, by Lemma 2.1 we have

$$
\begin{aligned}
\sum_{|x|<m/2} g_\beta(x) e_m(-hx) &= \sum_{|x|<m/2} \sum_{|k|<m/2} a_k e_m((k-h)x) \\
&= \sum_{|k|<m/2} a_k \sum_{|x|<m/2} e_m((k-h)x) = m a_h.
\end{aligned}
$$

Therefore

$$
\begin{aligned}
a_h &= \frac{1}{m} \sum_{|x|<m/2} g_\beta(x) e_m(-hx) = \frac{1}{m} \sum_{x=0}^{m-1} g_\beta(x) e_m(-hx) \\
&= \frac{1}{m} \sum_{0\le x<\beta m} (1-\beta) e_m(-hx) + \frac{1}{m} \sum_{\beta m \le x \le m-1} (-\beta) e_m(-hx) \\
&= \frac{1}{m} \sum_{0 \le x < \beta m} e_m(-hx).
\end{aligned}
$$

Write $A = \lceil \beta m \rceil$. Noting that $1 \le \beta m = s \le (m-1)/2$, we have $A \le (m+1)/2$. Then

$$
\sum_{\substack{|h|<m/2 \\ h\neq 0}} a_h^2 a_{-h}^2 = \frac{1}{m^4} \sum_{x_1=0}^{A-1} \sum_{x_2=0}^{A-1} \sum_{x_3=0}^{A-1} \sum_{x_4=0}^{A-1} \sum_{\substack{|h|<m/2 \\ h\neq 0}} e_m\left(h(x_3+x_4-x_1-x_2)\right)
$$

$$= \frac{1}{m^3}\sum_{\substack{x_1=0\\x_1+x_2\equiv x_3+x_4(\bmod m)}}^{A-1}\sum_{x_2=0}^{A-1}\sum_{x_3=0}^{A-1}\sum_{x_4=0}^{A-1} 1 - \frac{A^4}{m^4} = \frac{1}{m^3}\sum_{\substack{x_1=0\\x_1+x_2=x_3+x_4}}^{A-1}\sum_{x_2=0}^{A-1}\sum_{x_3=0}^{A-1}\sum_{x_4=0}^{A-1} 1 - \frac{A^4}{m^4}.$$

It is not hard to show that

$$\sum_{\substack{x_1=0\\x_1+x_2=x_3+x_4}}^{A-1}\sum_{x_2=0}^{A-1}\sum_{x_3=0}^{A-1}\sum_{x_4=0}^{A-1} 1 = \sum_{u=0}^{2A-2}\left(\sum_{\substack{x_1=0\\x_1+x_2=u}}^{A-1}\sum_{x_2=0}^{A-1}\right)^2 = \sum_{u=0}^{A-1}\left(\sum_{\substack{x_1=0\\x_1+x_2=u}}^{A-1}\sum_{x_2=0}^{A-1}\right)^2 + \sum_{u=A}^{2A-2}\left(\sum_{\substack{x_1=0\\x_1+x_2=u}}^{A-1}\sum_{x_2=0}^{A-1}\right)^2$$
$$= \sum_{u=0}^{A-1}\left(\sum_{x_1=0}^{u} 1\right)^2 + \sum_{u=A}^{2A-2}\left(\sum_{x_1=u-A+1}^{A-1} 1\right)^2 = \sum_{u=0}^{A-1}(u+1)^2 + \sum_{u=A}^{2A-2}(2A-1-u)^2$$
$$= \frac{2}{3}A^3 + O\left(A^2\right).$$

Therefore

$$\sum_{\substack{|h|<m/2\\h\neq 0}} a_h^2 a_{-h}^2 = \left(\frac{2}{3}-\beta\right)\beta^3 + O\left(\frac{1}{m}\right). \tag{5.6}$$

Combining (5.5) and (5.6) we have

$$\sum_{n=1}^{M} e_{n+d_1}\cdots e_{n+d_{4l}} = M\left(\frac{2}{3}-\beta\right)^l \beta^{3l} + O\left(dm^{3/4}(\log m)^{4l+1}\right). \tag{5.7}$$

Now taking

$$\begin{cases} d_{4k+1} = 0+k \\ d_{4k+2} = p+k \\ d_{4k+3} = q+k \\ d_{4k+4} = p+q+k \end{cases}, \qquad k = 0,\cdots,l-1, \qquad M = m-2q. \tag{5.8}$$

Since $1 \le l \le q-p+1$, it is easy to show that the integers $d_1,\cdots,d_{4l}$, $M$ satisfy (5.1) and (5.2). Then from (5.7) we have

$$\left|\sum_{n=1}^{M} e_{n+d_1}\cdots e_{n+d_{4l}}\right| \gg \left(\frac{2}{3}-\beta\right)^l \beta^{3l} m.$$

Therefore

$$C_{4l}(\mathcal{R},m) = \max_{M,D}\left|\sum_{n=1}^{M} e_{n+d_1}\cdots e_{n+d_{4l}}\right| \gg \left(\frac{2}{3}-\beta\right)^l \beta^{3l} m.$$

This proves Theorem 1.3. Using the same methods we can deduce Theorem 1.4.

## Acknowledgments

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

## References

[1] C. Dartyge, E. Mosaki and A. Sárközy, On large families of subsets of the set of the integers not exceeding $N$, *The Ramanujan Journal,* 18 (2009), pp. 209–229.

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

[3] H. Liu, T. Zhan and X. Wang, On the correlation of pseudorandom binary sequences with composite moduli, *Publicationes Mathematicae Debrecen,* 74 (2009), pp. 195–214.

[4] C. Mauduit, J. Rivat and A. Sárközy, Construction of pseudorandom binary sequences using additive characters, *Monatshefte für Mathematik,* 141 (2004), pp. 197–208.

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

[6] C. Mauduit and A. Sárközy, Construction of pseudorandom binary sequences by using the multiplicative inverse, *Acta Mathematica Hungarica,* 108 (2005), pp. 239–252.

[7] J. Rivat and A. Sárközy, Modular constructions of pseudorandom binary sequences with composite moduli, *Periodica Mathematica Hungarica,* 51 (2005), pp. 75–107.

[8] W. Schmidt, *Equations Over Finite Fields: An Elementary Approach,* Lecture Notes in. Mathematics, Springer, Berlin, vol. 536, 1976.

Department of Mathematics, Northwest University
Xi'an, Shaanxi, P. R. China
*E-mail: 420100981@qq.com, hnliumath@hotmail.com*