Publ. Math. Debrecen
74/1-2 (2009), 195–214

On the correlation of pseudorandom binary sequences with composite moduli

By HUANING LIU (Jinan), TAO ZHAN (Jinan) and XIAOYUN WANG (Jinan)

Abstract. Recently J. Rivat and A. Sárközy extended two large families of pseudorandom binary sequences to the case of composite moduli m, where m is the product of two different primes not far apart. In this paper we study the correlation measure of these sequences. Our results show that these sequences are "bad" if either m is "not large" or m is "large" but its prime factors are known.

§1. Introduction

In a series of papers C. Mauduit, J. Rivat and A. Sárközy (partly with other coauthors) studied finite pseudorandom binary sequences

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

In particular in [8] C. Mauduit and A. Sárközy first introduced the following measures of pseudorandomness: the *well-distribution measure* of E_N is defined by

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

Mathematics Subject Classification: 11K45, 11L07.
Key words and phrases: pseudorandom binary sequence, composite moduli, correlation.
Research supported by the National Grand Fundamental Research 973 Programs of China under Grant 2007CB807902 and 2007CB807903, the China Postdoctoral Science Foundation funded project under Grant 20070421084, and the Specialized Research Fund for the Post Doctorate of Shandong Province under Grant 200702036.

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 E_N is defined as

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

where the maximum is taken over all $D = (d_1, \ldots, d_k)$ and M with $0 \le d_1 < \cdots < d_k \le N - M$, and the *combined (well-distribution-correlation) PR- measure of order k*

$$Q_k(E_N) = \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \cdots e_{a+jb+d_k} \right|$$

is defined for all a, b, t, $D = (d_1, \ldots, d_k)$ with $1 \le a + jb + d_i \le N (i = 1, 2, \ldots, k)$.

Many pseudorandom binary sequences were given and studied, see [1], [2], [3], [4], [5], [6], [7], [9], [10] for details. For example, two large families of pseudorandom binary sequences have been given. The first construction was given by C. Mauduit, J. Rivat and A. Sárközy in [7].

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

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

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

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

and for $2 \le l \le d - 1$, we also have

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

The other construction was given by C. Mauduit and A. Sárközy in [9].

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 $E_p = (e_1, \ldots, e_p)$ by*

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

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

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

Note that the above constructions are with a prime moduli p. One might like to look for constructions with composite moduli m, since this type of constructions are more important in cryptography. 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 [11] tried to extend the above two constructions to the case of composite moduli m defined by (1.1). They wrote that,"...we will show that a partial extension of the construction above is possible, but we also run into, perhaps, unexpected difficulties." Indeed, in [11] first they study the extension of the Legendre symbol construction [2] to Jacobi symbol with modulus of form (1.1). Then they study the pseudorandom properties of two further constructions with moduli of form (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), $f(x) = a_d x^d + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, $(a_d, pq) = 1$, *and* $2 \le d < p(< q)$. *Define the binary sequence* $E'_m = (e'_1, \ldots, e'_m)$ *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* $r \in \{0, 1, \ldots, m-1\}$ *with* $n \equiv r (\mathrm{mod}\, m)$. *Then we have*

$$W(E'_m) \ll d^2 m^{1/2}(\log m)^2.$$

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

$$C_2(E'_m) \ll dm^{3/4}(\log m)^3.$$

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 $ab \equiv 1 (\mathrm{mod} m)$.

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 $E''_m = (e''_1, \ldots, e''_m)$ 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

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

In this paper we shall study the correlation measure of order greater than 2 of the sequences defined in Proposition 1.3 and Proposition 1.4. In Section 3 we shall prove the following.

Theorem 1.1. *Define m, d, $f(x)$ and E'_m as in Proposition 1.3. Assume that $d \ge 4$. Then we have*

$$C_3(E'_m) \ll d m^{3/4} (\log m)^4.$$

Theorem 1.2. *Define m, k, $f(x)$ and E''_m as in Proposition 1.4. Assume that $(4k)^3 < p(< q)$. Then we have*

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

Since

$$C_2(E'_m) \ll d m^{3/4} (\log m)^3, \qquad C_3(E'_m) \ll d m^{3/4} (\log m)^4,$$
$$C_2(E''_m) \ll k^2 m^{3/4} (\log m)^3, \qquad C_3(E''_m) \ll k^3 m^{3/4} (\log m)^4,$$

it is natural to expect that

$$C_l(E'_m) \ll d m^{3/4} (\log m)^{l+1} \quad \text{and} \quad C_l(E''_m) \ll k^l m^{3/4} (\log m)^{l+1}$$

for $l \ge 4$. However, in Section 4 we shall prove that $C_{4l}(E'_m)$ and $C_{4l}(E''_m)$ are large for $l \in \mathbb{N}$.

Theorem 1.3. *Define m, d, $f(x)$ and E'_m as in Proposition 1.3. Assume that the prime factors p, q of m are made known, and*

$$1 \le l \le \min\left((d-1)/2, q-p+1\right).$$

Then we have

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

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

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

§2. Some lemmas

To prove the theorems, we need the following lemmas.

Lemma 2.1. *If $n \in \mathbb{Z}$ and m is an odd integer, then we have*

$$\frac{1}{m}\sum_{|a|<m/2} v_m(a)\mathrm{e}\left(\frac{an}{m}\right) = \begin{cases} +1, & \text{if } 0 \le R_m(n) < m/2, \\ -1, & \text{if } m/2 \le R_m(n) < m, \end{cases}$$

where $v_m(a)$ is a function of period m such that

$$v_m(0) = 1, \quad v_m(a) = 1 + i\frac{(-1)^a - \cos(\pi a/m)}{\sin(\pi a/m)} \quad (1 \le |a| < m/2).$$

Furthermore, $v_m(a)$ satisfies

$$v_m(a) = \begin{cases} O(1), & \text{if } a \text{ is even}, \\ -\dfrac{2im}{\pi a} + O(1), & \text{if } a \text{ is odd}. \end{cases}$$

Proof. This is Lemma 2 in [7]. □

Lemma 2.2. *Let p be a prime number, $k \in \mathbb{N}$, $1 \le k < p$, $f(x) \in \mathbb{F}_p[x]$ a polynomial of degree $d \ge k$, and let $d_1, \ldots, d_k$ be k different elements of $\mathbb{F}_p$. Then for all $(h_1, \ldots, h_k) \in \mathbb{F}_p^k \backslash (0, \ldots, 0)$, the polynomial*

$$g(x) = h_1 f(x + d_1) + \cdots + h_k f(x + d_k)$$

is of degree $\ge d - k + 1$.

PROOF. This is Lemma 3 in [7]. □

Lemma 2.3. *Let p, q be distinct prime numbers and $f(x) = a_l x^l + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ with $2 \le l < \min(p, q)$, $pq \nmid a_l$ and X, Y real numbers with $0 < Y \le pq$. Then*

$$\left| \sum_{X < n \le X+Y} \mathrm{e}\left(\frac{f(n)}{pq}\right) \right| \ll l^2 p^{1/2} q^{1/2} \log(pq) \qquad \text{for } (a_l, pq) = 1,$$

$$\left| \sum_{X < n \le X+Y} \mathrm{e}\left(\frac{f(n)}{pq}\right) \right| \ll lpq^{1/2} \log(pq) \qquad \text{for } (a_l, q) = 1,$$

$$\left| \sum_{X < n \le X+Y} \mathrm{e}\left(\frac{f(n)}{pq}\right) \right| \ll lp^{1/2} q \log(pq) \qquad \text{for } (a_l, p) = 1.$$

PROOF. This is Lemma 10 in [11]. □

Lemma 2.4. *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 $2 \le l \le p$, and one of the following conditions holds:*

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

Let $d_1, \ldots, d_l$ be l different elements of $\mathbb{F}_p$. Then for all

$$(h_1, \ldots, h_l) \in \mathbb{F}_p^l \backslash (0, \ldots, 0),$$

the polynomial

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

is not the 0 polynomial.

PROOF. This is Lemma 5 in [9]. □

Lemma 2.5. *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 $0 < Y \le pq$. Then we have*

$$\left| \sum_{\substack{X < n \le X+Y \\ (R(n), pq) = 1}} \mathrm{e}\left(\frac{Q(n) i_{pq}(R(n))}{pq}\right) \right| \ll D^2 p^{1/2} q^{1/2} \log(pq),$$

if Q_p/R_p and Q_q/R_q are not constants or linear polynomials,

$$\left| \sum_{\substack{X<n\le X+Y\\(R(n),pq)=1}} \mathrm{e}\left(\frac{Q(n)i_{pq}(R(n))}{pq}\right) \right| \ll Dpq^{1/2}\log(pq),$$

if Q_q/R_q is not a constant or linear polynomial,

$$\left| \sum_{\substack{X<n\le X+Y\\(R(n),pq)=1}} \mathrm{e}\left(\frac{Q(n)i_{pq}(R(n))}{pq}\right) \right| \ll Dp^{1/2}q\log(pq),$$

if Q_p/R_p is not a constant or linear polynomial.

PROOF. This Lemma can be proved from Lemmas 1, 11 and 13 in [11]. □

Lemma 2.6. *Let p, q be distinct prime numbers. Then for any polynomial $f(x) \in \mathbb{Z}[x]$, we have*

$$\sum_{n=1}^{pq} \mathrm{e}\left(\frac{f(n)}{pq}\right) = \mathrm{e}\left(\frac{f(0)}{pq}\right)\left[\mathrm{e}\left(-\frac{i_q(p)f(0)}{q}\right)\sum_{u=1}^{q}\mathrm{e}\left(\frac{i_q(p)f(u)}{q}\right)\right] \times \left[\mathrm{e}\left(-\frac{i_p(q)f(0)}{p}\right)\sum_{v=1}^{p}\mathrm{e}\left(\frac{i_p(q)f(v)}{p}\right)\right].$$

PROOF. This is formula (19) in [11]. □

Lemma 2.7. *Suppose that p is a prime number and $f(x) = a_l x^l + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ is a polynomial with $0 < l < p$ and $(a_l, p) = 1$. Then*

$$\left| \sum_{n=0}^{p-1} \mathrm{e}\left(\frac{f(n)}{p}\right) \right| \le (l-1)\,p^{1/2}.$$

PROOF. This is Corollary 2F in [12]. □

Lemma 2.8. *Assume that $m \in \mathbb{N}$ is of the form (1.1). Then we have*

$$\sum_{\substack{|r_1|<m/2\\ p|r_1+r_2\\ r_1+r_2\neq 0}} \sum_{|r_2|<m/2} \sum_{|r_3|<m/2} \cdots \sum_{|r_l|<m/2} v_m(r_1)v_m(r_2)v_m(r_3)\ldots v_m(r_l)$$

$$\ll m^{l-1/2}\,(\log m)^l\,.$$

PROOF. From Lemma 2.1 we have

$$\sum_{\substack{|r_1|<m/2\\ p|r_1+r_2\\ r_1+r_2\neq 0}} \sum_{|r_2|<m/2} \sum_{|r_3|<m/2} \cdots \sum_{|r_l|<m/2} v_m(r_1)v_m(r_2)v_m(r_3)\ldots v_m(r_l)$$

$$\ll \sum_{\substack{-q<l<q\\ l\neq 0}} \sum_{|r_1|<m/2} \sum_{\substack{|r_1|<m/2\\ r_1+r_2=lp}} |v_m(r_1)||v_m(r_2)| \Big(\sum_{|r|<m/2} |v_m(r)| \Big)^{l-2}$$

$$\ll m^l (\log m)^{l-2} \sum_{\substack{-q<l<q\\ l\neq 0}} \sum_{\substack{|r_1|<m/2\\ r_1\neq 0\\ r_1+r_2=lp}} \sum_{\substack{|r_2|<m/2\\ r_2\neq 0}} \frac{1}{|r_1 r_2|}$$

$$= m^l (\log m)^{l-2} \sum_{\substack{-q<l<q\\ l\neq 0}} \sum_{\substack{|r_1|<m/2\\ r_1\neq 0\\ r_1+r_2=lp}} \sum_{\substack{|r_2|<m/2\\ r_2\neq 0}} \left| \frac{1}{(r_1+r_2)} \left(\frac{1}{r_1} + \frac{1}{r_2} \right) \right|$$

$$\ll m^l (\log m)^{l-2} \sum_{\substack{-q<l<q\\ l\neq 0}} \frac{1}{|l|p} \left[\sum_{\substack{|r_1|<m/2\\ r_1\neq 0}} \frac{1}{|r_1|} + \sum_{\substack{|r_2|<m/2\\ r_2\neq 0}} \frac{1}{|r_2|} \right]$$

$$\ll m^{l-1/2} (\log m)^l . \qquad \square$$

Lemma 2.9. *Let $p, q \in \mathbb{N}$ with $(p,q)=1$ and $Q(x), R(x) \in \mathbb{Z}[x]$. Then*

$$\sum_{\substack{1\le n\le pq\\ (R(n),pq)=1}} \mathrm{e}\left(\frac{Q(n) i_{pq}(R(n))}{pq} \right) = \sum_{\substack{1\le u\le q\\ (R(u),q)=1}} \mathrm{e}\left(\frac{Q(u) i_q(pR(u))}{q} \right) \sum_{\substack{1\le v\le p\\ (R(v),p)=1}} \mathrm{e}\left(\frac{Q(v) i_p(qR(v))}{p} \right).$$

Proof. This is Lemma 11 in [11]. $\square$

Lemma 2.10. *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 ψ is a non-trivial additive character of $\mathbb{F}_p$, then*

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

Proof. This is Lemma 13 in [11]. $\square$

§3. Proof of Theorem 1.1 and Theorem 1.2

First we prove Theorem 1.1. Let $M \in \mathbb{N}$, $d_1, d_2, d_3 \in \mathbb{Z}$ such that $0 \le d_1 < d_2 < d_3 \le m - M$. By Lemma 2.1 we get

$$\begin{aligned}
\sum_{n=1}^{M} e'_{n+d_1} e'_{n+d_2} e'_{n+d_3} &= \frac{1}{m^3} \sum_{n=1}^{M} \sum_{|r_1|<m/2} v_m(r_1) \mathrm{e}\left(\frac{r_1 f(n+d_1)}{m}\right) \\
&\quad \times \sum_{|r_2|<m/2} v_m(r_2) \mathrm{e}\left(\frac{r_2 f(n+d_2)}{m}\right) \sum_{|r_3|<m/2} v_m(r_3) \mathrm{e}\left(\frac{r_3 f(n+d_3)}{m}\right) \\
&= \frac{1}{m^3} \sum_{|r_1|<m/2} \sum_{|r_2|<m/2} \sum_{|r_3|<m/2} v_m(r_1) v_m(r_2) v_m(r_3) \\
&\quad \times \sum_{n=1}^{M} \mathrm{e}\left(\frac{r_1 f(n+d_1) + r_2 f(n+d_2) + r_3 f(n+d_3)}{m}\right) \\
&= \frac{1}{m^3} \sum_{i=1}^{3} \binom{3}{i} \sum_{\substack{|r_1|<m/2 \\ (r_{j_1},m)>1,\dots,(r_{j_i},m)>1}} \sum_{|r_2|<m/2} \sum_{|r_3|<m/2} v_m(r_1) v_m(r_2) v_m(r_3) \\
&\quad \times \sum_{n=1}^{M} \mathrm{e}\left(\frac{r_1 f(n+d_1) + r_2 f(n+d_2) + r_3 f(n+d_3)}{m}\right) \\
&\quad + \frac{1}{m^3} \sum_{\substack{|r_1|<m/2 \\ (r_1,m)=1}} \sum_{\substack{|r_2|<m/2 \\ (r_2,m)=1}} \sum_{\substack{|r_3|<m/2 \\ (r_3,m)=1}} v_m(r_1) v_m(r_2) v_m(r_3) \\
&\quad \times \sum_{n=1}^{M} \mathrm{e}\left(\frac{r_1 f(n+d_1) + r_2 f(n+d_2) + r_3 f(n+d_3)}{m}\right).
\end{aligned}$$

From Lemma 2.1 we easily have

$$\begin{aligned}
&\frac{1}{m^3} \sum_{i=1}^{3} \binom{3}{i} \sum_{\substack{|r_1|<m/2 \\ (r_{j_1},m)>1,\dots,(r_{j_i},m)>1}} \sum_{|r_2|<m/2} \sum_{|r_3|<m/2} v_m(r_1) v_m(r_2) v_m(r_3) \\
&\qquad \times \sum_{n=1}^{M} \mathrm{e}\left(\frac{r_1 f(n+d_1) + r_2 f(n+d_2) + r_3 f(n+d_3)}{m}\right) \\
&\ll \frac{M}{m^3} \sum_{i=1}^{3} \binom{3}{i} \left(\sum_{\substack{|r|<m/2 \\ (r,m)=1}} |v_m(r)| \right)^{3-i} \left(\sum_{\substack{|s|<m/2 \\ (s,m)>1}} |v_m(s)| \right)^{i}
\end{aligned}$$

$$\ll \frac{M}{m^3}\sum_{i=1}^{3}\binom{3}{i}\Bigg(\sum_{\substack{|r|<m/2\\(r,m)=1}}\frac{m}{r}\Bigg)^{3-i}\Bigg(\sum_{\substack{|s|<m/2\\(s,m)>1\\s\neq 0}}\frac{m}{s}+1\Bigg)^{i}$$

$$\ll \frac{M}{m^3}\sum_{i=1}^{3}\binom{3}{i}m^{3-i}(\log m)^{3-i}\Bigg(\sum_{\substack{|s|<m/2\\p|s\\s\neq 0}}\frac{m}{s}+\sum_{\substack{|s|<m/2\\q|s\\s\neq 0}}\frac{m}{s}+1\Bigg)^{i}$$

$$\ll \frac{M}{m^3}\sum_{i=1}^{3}\binom{3}{i}m^{3-i}(\log m)^{3-i}m^{i/2}(\log m)^{i} \ll m^{1/2}(\log m)^3.$$

Therefore

$$\sum_{n=1}^{M} e'_{n+d_1}e'_{n+d_2}e'_{n+d_3} = \frac{1}{m^3}\sum_{\substack{|r_1|<m/2\\(r_1,m)=1}}\sum_{\substack{|r_2|<m/2\\(r_2,m)=1}}\sum_{\substack{|r_3|<m/2\\(r_3,m)=1}} v_m(r_1)v_m(r_2)v_m(r_3)$$
$$\times\sum_{n=1}^{M}\mathrm{e}\left(\frac{r_1f(n+d_1)+r_2f(n+d_2)+r_3f(n+d_3)}{m}\right)+O\big(m^{1/2}(\log m)^3\big).$$

Since $0\le d_1<d_2<d_3\le m-M$, there exists at least one d_i such that $d_i\not\equiv d_j(\mathrm{mod}p)$ or $d_i\not\equiv d_j(\mathrm{mod}q)$ for $j\in\{1,2,3\}\backslash\{i\}$. Without loss of generality, we suppose that $d_3\not\equiv d_1(\mathrm{mod}p)$, $d_3\not\equiv d_2(\mathrm{mod}p)$. Note that $\deg(f)\ge 4$ and $(r_3,m)=1$, from Lemma 2.2 we know that the polynomial

$$r_1f(n+d_1)+r_2f(n+d_2)+r_3f(n+d_3)$$

is of degree ≥ 2 in $\mathbb{F}_p$. Then from Lemma 2.3 we have

$$\left|\sum_{n=1}^{M}\mathrm{e}\left(\frac{r_1f(n+d_1)+r_2f(n+d_2)+r_3f(n+d_3)}{m}\right)\right| \ll dp^{1/2}q\log(pq)\ll dm^{3/4}\log m.$$

Then by Lemma 2.1 we get

$$\sum_{n=1}^{M}e'_{n+d_1}e'_{n+d_2}e'_{n+d_3}\ll\frac{1}{m^3}\Bigg(\sum_{\substack{|r|<m/2\\(r,m)=1}}|v_m(r)|\Bigg)^3\cdot dm^{3/4}\log m+m^{1/2}(\log m)^3$$

$$\ll \frac{1}{m^3}\Bigg(\sum_{\substack{|r|<m/2\\(r,m)=1}}\frac{m}{r}\Bigg)^3 \cdot dm^{3/4}\log m + m^{1/2}(\log m)^3 \ll dm^{3/4}(\log m)^4.$$

Therefore

$$C_3(E'_m) \ll dm^{3/4}(\log m)^4.$$

Now we prove Theorem 1.2. 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 Lemma 2.1 and the methods of proving Theorem 1.1 we get

$$\begin{aligned}
\sum_{n=1}^{M} e''_{n+d_1}e''_{n+d_2}e''_{n+d_3} &= \frac{1}{m^3}\sum_{\substack{n=1\\(f(n+d_1)f(n+d_2)f(n+d_3),m)=1}}^{M}\\
&\quad\times\sum_{|r_1|<m/2} v_m(r_1)\mathrm{e}\left(\frac{r_1 i_m(f(n+d_1))}{m}\right)\\
&\quad\times\sum_{|r_2|<m/2} v_m(r_2)\mathrm{e}\left(\frac{r_2 i_m(f(n+d_2))}{m}\right)\sum_{|r_3|<m/2} v_m(r_3)\mathrm{e}\left(\frac{r_3 i_m(f(n+d_3))}{m}\right)+O(k)\\
&= \frac{1}{m^3}\sum_{|r_1|<m/2}\sum_{|r_2|<m/2}\sum_{|r_3|<m/2} v_m(r_1)v_m(r_2)v_m(r_3)\sum_{\substack{n=1\\(f(n+d_1)f(n+d_2)f(n+d_3),m)=1}}^{M}\\
&\quad\times \mathrm{e}\left(\frac{r_1 i_m(f(n+d_1)) + r_2 i_m(f(n+d_2)) + r_3 i_m(f(n+d_3))}{m}\right)+O(k)\\
&= \frac{1}{m^3}\sum_{i=1}^{3}\binom{3}{i}\sum_{\substack{|r_1|<m/2\\(r_{j_1},m)>1,\dots,(r_{j_i},m)>1}}\sum_{|r_2|<m/2}\sum_{|r_3|<m/2} v_m(r_1)v_m(r_2)v_m(r_3)\sum_{\substack{n=1\\(f(n+d_1)f(n+d_2)f(n+d_3),m)=1}}^{M}\\
&\quad\times \mathrm{e}\left(\frac{r_1 i_m(f(n+d_1)) + r_2 i_m(f(n+d_2)) + r_3 i_m(f(n+d_3))}{m}\right)\\
&\quad+\frac{1}{m^3}\sum_{\substack{|r_1|<m/2\\(r_1,m)=1}}\sum_{\substack{|r_2|<m/2\\(r_2,m)=1}}\sum_{|r_3|<m/2\ (r_3,m)=1} v_m(r_1)v_m(r_2)v_m(r_3)\sum_{\substack{n=1\\(f(n+d_1)f(n+d_2)f(n+d_3),m)=1}}^{M}\\
&\quad\times \mathrm{e}\left(\frac{r_1 i_m(f(n+d_1)) + r_2 i_m(f(n+d_2)) + r_3 i_m(f(n+d_3))}{m}\right)+O(k)\\
&= \frac{1}{m^3}\sum_{\substack{|r_1|<m/2\\(r_1,m)=1}}\sum_{\substack{|r_2|<m/2\\(r_2,m)=1}}\sum_{\substack{|r_3|<m/2\\(r_3,m)=1}} v_m(r_1)v_m(r_2)v_m(r_3)\sum_{\substack{n=1\\(f(n+d_1)f(n+d_2)f(n+d_3),m)=1}}^{M}
\end{aligned}$$

$$\times \mathrm{e}\left(\frac{r_1 i_m(f(n+d_1)) + r_2 i_m(f(n+d_2)) + r_3 i_m(f(n+d_3))}{m}\right)$$
$$+ O\left(m^{1/2}(\log m)^3\right).$$

Define

$$Q(n) = r_1 f(n+d_2)f(n+d_3) + r_2 f(n+d_1)f(n+d_3) + r_3 f(n+d_1)f(n+d_2),$$
$$R(n) = f(n+d_1)f(n+d_2)f(n+d_3),$$

then we have

$$\sum_{\substack{n=1\\(f(n+d_1)f(n+d_2)f(n+d_3),m)=1}}^{M} \left(\mathrm{e}\frac{r_1 i_m(f(n+d_1)) + r_2 i_m(f(n+d_2)) + r_3 i_m(f(n+d_3))}{m}\right)$$
$$= \sum_{\substack{n=1\\(R(n),m)=1}}^{M} \mathrm{e}\left(\frac{Q(n) i_m(R(n))}{m}\right).$$

Since $0 \le d_1 < d_2 < d_3 \le m - M$, there exists at least one d_i such that $d_i \not\equiv d_j (\mathrm{mod} p)$ or $d_i \not\equiv d_j (\mathrm{mod} q)$ for $j \in \{1,2,3\}\backslash\{i\}$. Without loss of generality, we suppose that $d_3 \not\equiv d_1 (\mathrm{mod} p)$, $d_3 \not\equiv d_2 (\mathrm{mod} p)$. Reducing $Q(n)$ and $R(n)$ modulo p we get $Q_p(n)$ and $R_p(n)$ respectively, where

$$Q_p(n) = \begin{cases} r_1 f(n+d_2)f(n+d_3) + r_2 f(n+d_1)f(n+d_3) + r_3 f(n+d_1)f(n+d_2), \\ \qquad \text{if } \ d_1 \not\equiv d_2 (\mathrm{mod} p), \\ f(n+d_1)\left((r_1+r_2)f(n+d_3) + r_3 f(n+d_1)\right), \\ \qquad \text{if } \ d_1 \equiv d_2 (\mathrm{mod} p), \end{cases}$$

$$R_p(n) = \begin{cases} f(n+d_1)f(n+d_2)f(n+d_3), & \text{if } \ d_1 \not\equiv d_2 (\mathrm{mod} p), \\ \left(f(n+d_1)\right)^2 f(n+d_3), & \text{if } \ d_1 \equiv d_2 (\mathrm{mod} p). \end{cases}$$

Note that $(r_3, m) = 1$ and $(4k)^3 < p$, by Lemma 2.4 we know that $Q_p(n)$ is not the 0 polynomial in $\mathbb{F}_p$. Since $\deg(Q_p) < \deg(R_p)$, then Q_p/R_p is not a constant or linear polynomial. So from Lemma 2.5 we have

$$\left| \sum_{\substack{n=1\\(f(n+d_1)f(n+d_2)f(n+d_3),m)=1}}^{M} \mathrm{e}\left(\frac{r_1 i_m(f(n+d_1)) + r_2 i_m(f(n+d_2)) + r_3 i_m(f(n+d_3))}{m}\right) \right|$$
$$\ll k^3 p^{1/2} q \log(pq) \ll k^3 m^{3/4} \log m.$$

Then by Lemma 2.1 we get

$$\sum_{n=1}^{M} e''_{n+d_1}e''_{n+d_2}e''_{n+d_3} \ll \frac{1}{m^3}\left(\sum_{\substack{|r|<m/2\\(r,m)=1}}|v_m(r)|\right)^3 \cdot k^3m^{3/4}\log m + m^{1/2}(\log m)^3$$

$$\ll \frac{1}{m^3}\left(\sum_{\substack{|r|<m/2\\(r,m)=1}}\frac{m}{r}\right)^3 \cdot k^3m^{3/4}\log m + m^{1/2}(\log m)^3 \ll k^3m^{3/4}(\log m)^4.$$

Therefore

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

This completes the proof of Theorem 1.2.

§4. 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

$$1 \le l \le \min\left((d-1)/2, q-p+1\right),$$

$d_1, \dots, d_{4l} \in \mathbb{Z}$ such that

$$0 \le d_1 < \cdots < d_{4l} \le m - M \tag{4.1}$$

and

$$\begin{cases} d_i \equiv d_j (\mathrm{mod} p), & \text{if } 2 \nmid i \text{ and } j = i+1,\\ d_i \not\equiv d_j (\mathrm{mod} p), & \text{otherwise.}\end{cases} \tag{4.2}$$

$$\begin{cases} d_i \equiv d_j (\mathrm{mod} q), & \text{if either } (i,j) = (4k+1, 4k+3) \text{ or } (i,j) = (4k+2, 4k+4),\\ d_i \not\equiv d_j (\mathrm{mod} q), & \text{otherwise.}\end{cases} \tag{4.3}$$

By Lemma 2.1 we get

$$\sum_{n=1}^{M} e'_{n+d_1}\cdots e'_{n+d_{4l}}$$

$$= \frac{1}{m^{4l}}\sum_{n=1}^{M}\sum_{|r_1|<m/2} v_m(r_1)\mathrm{e}\left(\frac{r_1 f(n+d_1)}{m}\right)\cdots\sum_{|r_{4l}|<m/2} v_m(r_{4l})\mathrm{e}\left(\frac{r_{4l} f(n+d_{4l})}{m}\right)$$

$$= \frac{1}{m^{4l}} \sum_{|r_1|<m/2} \cdots \sum_{|r_{4l}|<m/2} v_m(r_1)\dots v_m(r_{4l}) \times \sum_{n=1}^{M} \mathrm{e}\left(\frac{r_1 f(n+d_1)+\cdots+r_{4l}f(n+d_{4l})}{m}\right). \tag{4.4}$$

Write $F(n) = r_1 f(n+d_1)+\cdots+r_{4l}f(n+d_{4l})$. By Lemma 2.6 we have

$$\begin{aligned}
&\sum_{n=1}^{M} \mathrm{e}\left(\frac{r_1 f(n+d_1)+\cdots+r_{4l}f(n+d_{4l})}{m}\right)\\
&= \frac{1}{m}\sum_{n=1}^{m} \mathrm{e}\left(\frac{F(n)}{m}\right)\sum_{s=1}^{M}\sum_{z=1}^{m}\mathrm{e}\left(\frac{z(n-s)}{m}\right) = \frac{1}{m}\sum_{z=1}^{m}\sum_{s=1}^{M}\mathrm{e}\left(-\frac{zs}{m}\right)\sum_{n=1}^{m}\mathrm{e}\left(\frac{F(n)+zn}{m}\right)\\
&= \frac{1}{m}\sum_{z=1}^{m}\sum_{s=1}^{M}\mathrm{e}\left(-\frac{zs}{m}\right)\mathrm{e}\left(\frac{F(0)}{m}\right)\left[\mathrm{e}\left(-\frac{i_q(p)F(0)}{q}\right)\sum_{u=1}^{q}\mathrm{e}\left(\frac{i_q(p)\,(F(u)+zu)}{q}\right)\right]\\
&\quad\times\left[\mathrm{e}\left(-\frac{i_p(q)F(0)}{p}\right)\sum_{v=1}^{p}\mathrm{e}\left(\frac{i_p(q)\,(F(v)+zv)}{p}\right)\right].
\end{aligned}$$

Then from (4.3) we get

$$\begin{aligned}
&\sum_{u=1}^{q}\mathrm{e}\left(\frac{i_q(p)\,(F(u)+zu)}{q}\right)\\
&= \sum_{u=1}^{q}\mathrm{e}\left(\frac{i_q(p)\,(r_1 f(u+d_1)+\cdots+r_{4l}f(u+d_{4l})+zu)}{q}\right)\\
&= \sum_{u=1}^{q}\mathrm{e}\left(\frac{i_q(p)\left[\sum_{k=0}^{l-1}((r_{4k+1}+r_{4k+3})f(u+d_{4k+1})+(r_{4k+2}+r_{4k+4})f(u+d_{4k+2}))+zu\right]}{q}\right).
\end{aligned}$$

If $q \mid r_{4k+1}+r_{4k+3}$, $q \mid r_{4k+2}+r_{4k+4}$, for $k = 0,\dots,l-1$, then

$$\sum_{u=1}^{q}\mathrm{e}\left(\frac{i_q(p)\,(F(u)+zu)}{q}\right) = \sum_{u=1}^{q}\mathrm{e}\left(\frac{i_q(p)\cdot zu}{q}\right) = \begin{cases} q, & \text{if } q \mid z,\\ 0, & \text{if } q \nmid z.\end{cases}$$

Otherwise by Lemma 2.2 we know that $F(u)$ is of degree $\geq d-2l+1 \geq 2$, then from Lemma 2.7 we have

$$\left|\sum_{u=1}^{q}\mathrm{e}\left(\frac{i_q(p)\,(F(u)+zu)}{q}\right)\right| \leq dq^{1/2}.$$

That is to say,

$$\sum_{u=1}^{q} \mathrm{e}\left(\frac{i_q(p)\,(F(u)+zu)}{q}\right) = \begin{cases} q, & \text{if } q \mid r_{4k+1}+r_{4k+3},\ q \mid r_{4k+2}+r_{4k+4},\\ & \quad \text{for } k=0,\dots,l-1,\ \text{and } q \mid z,\\ 0, & \text{if } q \mid r_{4k+1}+r_{4k+3},\ q \mid r_{4k+2}+r_{4k+4},\\ & \quad \text{for } k=0,\dots,l-1,\ \text{and } q \nmid z,\\ O\left(dq^{1/2}\right), & \text{otherwise.} \end{cases}$$

Similarly we get

$$\sum_{v=1}^{p} \mathrm{e}\left(\frac{i_p(q)\,(F(v)+zv)}{p}\right) = \begin{cases} p, & \text{if } p \mid r_{2j-1}+r_{2j},\ \text{for } j=1,\dots,2l,\ \text{and } p \mid z,\\ 0, & \text{if } p \mid r_{2j-1}+r_{2j},\ \text{for } j=1,\dots,2l,\ \text{and } p \nmid z,\\ O\left(dp^{1/2}\right), & \text{otherwise.} \end{cases}$$

Therefore

$$\sum_{n=1}^{M} \mathrm{e}\left(\frac{r_1 f(n+d_1)+\dots+r_{4l} f(n+d_{4l})}{m}\right) = \begin{cases} M, & \text{if } \ p \mid r_{2j-1}+r_{2j}, j=1,\dots,2l,\\ & \quad q \mid r_{4k+1}+r_{4k+3},\ q \mid r_{4k+2}+r_{4k+4},\\ & \quad k=0,\dots,l-1,\\ O\left(dm^{3/4}\log m\right), & \text{otherwise.} \end{cases} \tag{4.5}$$

Then from (4.4), (4.5) and Lemma 2.1 we have

$$\sum_{n=1}^{M} e'_{n+d_1}\dots e'_{n+d_{4l}} = \frac{M}{m^{4l}} \sum_{\substack{|r_1|<m/2\\ p \mid r_{2j-1}+r_{2j},\ j=1,\dots,2l\\ q \mid r_{4k+1}+r_{4k+3},\ q \mid r_{4k+2}+r_{4k+4},\ k=0,\dots,l-1}} \cdots \sum_{|r_{4l}|<m/2} v_m(r_1)\dots v_m(r_{4l}) + O\left(\frac{1}{m^{4l}}\left(\sum_{|r|<m/2}|v_m(r)|\right)^{4l} dm^{3/4}\log m\right)$$

$$= \frac{M}{m^{4l}} \sum_{\substack{|r_1|<m/2 \\ p|r_{2j-1}+r_{2j},\ j=1,\dots,2l \\ q|r_{4k+1}+r_{4k+3},\ q|r_{4k+2}+r_{4k+4},\ k=0,\dots,l-1}} \cdots \sum_{|r_{4l}|<m/2} v_m(r_1)\dots v_m(r_{4l}) + O\left(dm^{3/4}(\log m)^{4l+1}\right).$$

By Lemma 2.8 we easily get

$$\begin{aligned}\sum_{n=1}^{M} e'_{n+d_1}\dots e'_{n+d_{4l}} &= \frac{M}{m^{4l}} \sum_{\substack{|r_1|<m/2 \\ r_{2j-1}+r_{2j}=0,\ j=1,\dots,2l \\ r_{4k+1}+r_{4k+3}=r_{4k+2}+r_{4k+4}=0,\ k=0,\dots,l-1}} \cdots \sum_{|r_{4l}|<m/2} v_m(r_1)\dots v_m(r_{4l}) \\ &\quad + O\left(dm^{3/4}(\log m)^{4l+1}\right) \\ &= \frac{M}{m^{4l}} \left(\sum_{|r|<m/2} (v_m(r)v_m(-r))^2 \right)^l + O\left(dm^{3/4}(\log m)^{4l+1}\right).\end{aligned}$$

So from Lemma 2.1 we have

$$\begin{aligned}\sum_{n=1}^{M} e'_{n+d_1}\dots e'_{n+d_{4l}} &= \frac{M}{m^{4l}} \left(\sum_{\substack{|r|<m/2 \\ 2\nmid r}} (v_m(r)v_m(-r))^2 \right)^l + O\left(dm^{3/4}(\log m)^{4l+1}\right) \\ &= \frac{M}{m^{4l}} \left(\sum_{\substack{|r|<m/2 \\ 2\nmid r}} \left(\frac{16m^4}{\pi^4 r^4} + O\left(\frac{m^3}{r^3}\right) \right) \right)^l + O\left(dm^{3/4}(\log m)^{4l+1}\right) \\ &= \frac{2^{4l+1}}{\pi^{4l}} \left(1 - \frac{1}{2^{4l}}\right) \zeta(4l) M + O\left(dm^{3/4}(\log m)^{4l+1}\right), \qquad (4.6)\end{aligned}$$

where $\zeta(s)$ is the Riemann zeta function.

Now taking

$$\begin{cases} d_{4k+1} = 0 + k \\ d_{4k+2} = p + k \\ d_{4k+3} = q + k \\ d_{4k+4} = p + q + k, \end{cases} \qquad k = 0, \dots, l-1, \qquad M = m - 2q. \qquad (4.7)$$

Since $1 \le l \le q-p+1$, it is not hard to show that the integers $d_1, \dots, d_{4l}$, M satisfy (4.1), (4.2) and (4.3). Then from (4.6) we have

$$\left| \sum_{n=1}^{M} e'_{n+d_1} \dots e'_{n+d_{4l}} \right| \gg \left(\frac{2}{\pi}\right)^{4l} m.$$

Therefore

$$C_{4l}(E'_m) = \max_{M,D} \left| \sum_{n=1}^{M} e'_{n+d_1} \dots e'_{n+d_{4l}} \right| \gg \left(\frac{2}{\pi}\right)^{4l} m.$$

This proves Theorem 1.3.

Now we prove Theorem 1.4. Let $M \in \mathbb{N}$, $4l \in \mathbb{N}$ with $(4k)^{2l} < p$, $d_1, \dots, d_{4l} \in \mathbb{Z}$ satisfying (4.1), (4.2) and (4.3). Using Lemmas 2.1, 2.9, 2.4, 2.10, 2.8 and the methods of proving Theorem 1.3 we have

$$\begin{aligned}
&\sum_{n=1}^{M} e''_{n+d_1} \dots e''_{n+d_{4l}} = \frac{1}{m^{4l}} \sum_{\substack{n=1 \\ (f(n+d_1)\dots f(n+d_{4l}),m)=1}}^{M} \sum_{|r_1|<m/2} v_m(r_1) \\
&\times \mathrm{e}\left(\frac{r_1 i_m(f(n+d_1))}{m}\right) \times \dots \times \sum_{|r_{4l}|<m/2} v_m(r_{4l}) \mathrm{e}\left(\frac{r_{4l} i_m(f(n+d_{4l}))}{m}\right) + O(kl) \\
&= \frac{1}{m^{4l}} \sum_{|r_1|<m/2} \cdots \sum_{|r_{4l}|<m/2} v_m(r_1) \dots v_m(r_{4l}) \\
&\quad \times \sum_{\substack{n=1 \\ (f(n+d_1)\dots f(n+d_{4l}),m)=1}}^{M} \mathrm{e}\left(\frac{r_1 i_m(f(n+d_1)) + \dots + r_{4l} i_m(f(n+d_{4l}))}{m}\right) + O(kl) \\
&= \frac{M}{m^{4l}} \sum_{\substack{|r_1|<m/2 \\ p \mid r_{2j-1}+r_{2j},\ j=1,\dots,2l \\ q \mid r_{4k+1}+r_{4k+3},\ q \mid r_{4k+2}+r_{4k+4},\ k=0,\dots,l-1}} \cdots \sum_{|r_{4l}|<m/2} v_m(r_1) \dots v_m(r_{4l}) + O\big(klm^{3/4}(\log m)^{4l+1}\big) \\
&= \frac{M}{m^{4l}} \sum_{\substack{|r_1|<m/2 \\ r_{2j-1}+r_{2j}=0,\ j=1,\dots,2l \\ r_{4k+1}+r_{4k+3}=r_{4k+2}+r_{4k+4}=0,\ k=0,\dots,l-1}} \cdots \sum_{|r_{4l}|<m/2} v_m(r_1) \dots v_m(r_{4l}) + O\big(klm^{3/4}(\log m)^{4l+1}\big) \\
&= \frac{M}{m^{4l}} \left(\sum_{|r|<m/2} (v_m(r) v_m(-r))^2 \right)^l + O\big(klm^{3/4}(\log m)^{4l+1}\big) \\
&= \frac{2^{4l+1}}{\pi^{4l}} \left(1 - \frac{1}{2^{4l}}\right) \zeta(4l) M + O\big(klm^{3/4}(\log m)^{4l+1}\big). \qquad (4.8)
\end{aligned}$$

Now taking $d_1, \ldots, d_{4l}$, M as in (4.7), then from (4.8) we have

$$\left| \sum_{n=1}^{M} e''_{n+d_1} \ldots e''_{n+d_{4l}} \right| \gg \left(\frac{2}{\pi}\right)^{4l} m.$$

Therefore

$$C_{4l}(E''_m) = \max_{M,D} \left| \sum_{n=1}^{M} e''_{n+d_1} \ldots e''_{n+d_{4l}} \right| \gg \left(\frac{2}{\pi}\right)^{4l} m.$$

This completes the proof of Theorem 1.4.

§5. Further discussions

In [11] J. Rivat and A. Sárközy proved the following.

Proposition 5.1. *Define p, q, m, d, $f(x)$ and $E'_m = (e'_1, \ldots, e'_m)$ as in Proposition 1.3. Assume that $2 \le l \le d-1$, and $d_1 < d_2 < \cdots < d_l$ and M are positive integers with*

$$d_i \not\equiv d_j (\mathrm{mod} p), \quad d_i \not\equiv d_j (\mathrm{mod} q), \quad \text{for} \quad 1 \le i < j \le l$$

and $M \le m - d_l$. Then we have

$$\left| \sum_{n=1}^{M} e'_{n+d_1} e'_{n+d_2} \ldots e'_{n+d_l} \right| \ll d^2 m^{1/2} (\log m)^{l+1}.$$

Proposition 5.2. *Define p, q, m, k, $f(x)$ and $E''_m = (e''_1, \ldots, e''_m)$ as in Proposition 1.4. Assume that $l \in \mathbb{N}$, and one of the following conditions holds:*

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

Then if $d_1 < d_2 < \cdots < d_l$ and M are positive integers with

$$d_i \not\equiv d_j (\mathrm{mod} p), \quad d_i \not\equiv d_j (\mathrm{mod} q), \quad \text{for} \quad 1 \le i < j \le l$$

and $M \le m - d_l$, we have

$$\left| \sum_{n=1}^{M} e''_{n+d_1} e''_{n+d_2} \ldots e''_{n+d_l} \right| \ll k^4 l^2 m^{1/2} (\log m)^{l+1}.$$

Our Theorem 1.3 and Theorem 1.4 show that E'_m and E''_m are "bad" binary sequences provided the prime factors p, q of m are known. However, if $m = pq$ is large and p, q are kept secret, from Proposition 5.1 and Proposition 5.2 we know that E'_m and E''_m can be considered as "good" sequences. Especially for positive integers $d_1, d_2, \ldots, d_l$ and M such that $d_1 < d_2 < \cdots < p(< q)$ and $M \le m - d_l$, we have

$$\left| \sum_{n=1}^{M} e'_{n+d_1} e'_{n+d_2} \ldots e'_{n+d_l} \right| \ll d^2 m^{1/2} (\log m)^{l+1}$$

and

$$\left| \sum_{n=1}^{M} e''_{n+d_1} e''_{n+d_2} \ldots e''_{n+d_l} \right| \ll k^4 l^2 m^{1/2} (\log m)^{l+1}.$$

This suggests that the high order "short range" correlations of E'_m and E''_m can be small.

Acknowledgments. The author expresses his gratitude to the referee for his helpful and detailed comments.

References

[1] J. Cassaigne, S. Ferenczi, C. Mauduit, J. Rivat and A. Sárközy, On finite pseudorandom binary sequencs III: the Liouville function, I, *Acta Arithmetica* **87** (1999), 367–390.

[2] L. Goubin, C. Mauduit and A. Sárközy, Construction of large families of pseudorandom binary sequences, *Journal of Number Theory* **106** (2004), 56–69.

[3] K. Gyarmati, On a family of pseudorandom binary sequences, *Periodica Mathematica Hungarica* **49** (2004), 45–63.

[4] P. Hubert, C. Mauduit and nd A. Sárközy, On pseudorandom binary lattices, *Acta Arithmetica* **125** (2006), 51–62.

[5] H. Liu, New pseudorandom sequences constructed by quadratic residues and Lehmer numbers, *Proceedings of the American Mathematical Society* **135** (2007), 1309–1318.

[6] H. Liu, A family of pseudorandom binary sequences constructed by the multiplicative inverse, *Acta Arithmetica* **130** (2007), 167–180.

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

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

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

[10] C. Mauduit and A. Sárközy, On large families of pseudorandom binary lattices, *Uniform Distribution Theory* **2** (2007), 23–37.

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

[12] W. Schmidt, Equations Over Finite Fields: An Elementary Approach, Vol. 536, Lecture Notes in Mathematics, *Springer-Verlag*, *Berlin*, 1976.

HUANING LIU
SCHOOL OF MATHEMATICS AND SYSTEM SCIENCES
SHANDONG UNIVERSITY
JINAN, SHANDONG
P. R. CHINA
DEPARTMENT OF MATHEMATICS
NORTHWEST UNIVERSITY
XI'AN, SHAANXI
P. R. CHINA

E-mail: hnliumath@hotmail.com

TAO ZHAN
SCHOOL OF MATHEMATICS AND SYSTEM SCIENCES
SHANDONG UNIVERSITY
JINAN, SHANDONG
P. R. CHINA

E-mail: zhantao@sdu.edu.cn

XIAOYUN WANG
SCHOOL OF MATHEMATICS AND SYSTEM SCIENCES
SHANDONG UNIVERSITY
JINAN, SHANDONG
P. R. CHINA

E-mail: xywang@sdu.edu.cn

(Received August 4, 2008; revised December 9, 2008)