PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 135, Number 5, May 2007, Pages 1309–1318
S 0002-9939(06)08630-8
Article electronically published on November 14, 2006

NEW PSEUDORANDOM SEQUENCES CONSTRUCTED BY QUADRATIC RESIDUES AND LEHMER NUMBERS

HUANING LIU

(Communicated by Wen-Ching Winnie Li)

Abstract. Let p be an odd prime. Define

$$e_n = \begin{cases} (-1)^{n+\overline{n}}, & \text{if } n \text{ is a quadratic residue mod } p, \\ (-1)^{n+\overline{n}+1}, & \text{if } n \text{ is a quadratic nonresidue mod } p, \end{cases}$$

where $\overline{n}$ is the multiplicative inverse of n modulo p such that $1 \leq \overline{n} \leq p-1$. This paper shows that the sequence $\{e_n\}$ is a "good" pseudorandom sequence, by using the properties of exponential sums, character sums, Kloosterman sums and mean value theorems of Dirichlet L-functions.

1. Introduction

Let p be an odd prime. For any integer n with $1 \leq n \leq p-1$, we define $\overline{n}$ to be the multiplicative inverse of n modulo p such that $1 \leq \overline{n} \leq p-1$. D. H. Lehmer [7] asked us to study the case that n and $\overline{n}$ are of opposite parity. In [13] and [14] W. Zhang proved that

$$\sum_{n=1}^{p-1} (-1)^{n+\overline{n}} \ll p^{\frac{1}{2}} \log^2 p.$$

Later he (partly with coauthors) gave a few generalizations on this subject (see [15]–[18] for details). Recently S. R. Louboutin, J. Rivat and A. Sárközy [8] showed that the sequence $\left\{(-1)^{n+\overline{n}}\right\}$ forms a "good" pseudorandom sequence.

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

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

In [9] Mauduit and Sárközy first introduced the following measures of pseudorandomness: the well-distribution measure of E_N is defined by

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

Received by the editors October 28, 2005 and, in revised form, December 23, 2005.
2000 *Mathematics Subject Classification.* Primary 11A07; 11K45.
Key words and phrases. Pseudorandom, binary sequence, inverse.
This work was supported by the NSF (10271093, 60472068) of P. R. China.

where the maximum is taken over all a, b, $t \in \mathcal{N}$ with $1 \le a \le a + (t-1)b \le N$. The correlation measure of order k of E_N is denoted as

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

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

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

is defined for all a, b, t, $D = (d_1, \cdots, d_k)$ with $1 \le a + jb + d_i \le N$ $(i = 1, 2, \cdots, k)$. In [10] the connection between the measures W and C_2 was studied.

The sequence is considered as a "good" pseudorandom sequence if both $W\left(E_N\right)$ and $C_k\left(E_N\right)$ (at least for small k) are "small" in terms of N. Later Cassaigne, Mauduit and Sárközy [4] proved that this terminology is justified since for almost all $E_N \in \{-1, +1\}^N$, both $W\left(E_N\right)$ and $C_k\left(E_N\right)$ are less than $N^{\frac{1}{2}} (\log N)^c$. Moreover, it was shown in [9] that the Legendre symbol forms a "good" pseudorandom sequence. In [2] and [3], Cassaigne and coauthors studied the pseudorandomness of the Liouville function, defined as $\lambda(n) = (-1)^{\Omega(n)}$ ($\Omega(n)$: number of prime factors of n counted with multiplicity) and also of $\gamma(n) = (-1)^{\omega(n)}$ ($\omega(n)$: number of distinct prime factors of n). Furthermore, let

$$K(m, n; p) = \sum_{a=1}^{p-1} \mathrm{e}\left(\frac{ma + n\overline{a}}{p}\right)$$

denote the Kloosterman sum, where $\mathrm{e}(y) = \mathrm{e}^{2\pi i y}$, and p is a prime. Fouvry (with other coauthors) [5] showed that the signs of $K(1, n; p)$ form a "good" pseudorandom binary sequence.

As was said in [9], the search for new approaches and new constructions should be continued. The purpose of this paper is to give some new examples of pseudorandom sequences. Let

$$\begin{aligned} e_n &= \begin{cases} (-1)^{n+\overline{n}}, & \text{if } n \text{ is a quadratic residue mod } p, \\ (-1)^{n+\overline{n}+1}, & \text{if } n \text{ is a quadratic nonresidue mod } p, \end{cases} \\ &= (-1)^{n+\overline{n}} \chi_2(n), \end{aligned} \tag{1.1}$$

where χ_2 is the Legendre symbol. We shall prove that the sequence $\{e_n\}$ is a "good" pseudorandom sequence, that is, the following:

Theorem 1.1. *Let p be an odd prime, and let $E_{p-1} = \{e_1, \cdots, e_{p-1}\}$ be defined by* (1.1). *Then we have*

$$\begin{aligned} W\left(E_{p-1}\right) &\ll p^{\frac{1}{2}} \log^2 p; \\ C_2\left(E_{p-1}\right) &\ll p^{\frac{1}{2}} \log^3 p; \\ Q_2\left(E_{p-1}\right) &\ll p^{\frac{1}{2}} \log^3 p. \end{aligned}$$

2. Some lemmas

We need the following lemmas.

Lemma 2.1. *Let p be a prime and let χ be a Dirichlet character modulo p. Define the generalized Kloosterman sum $K(m,n,\chi;p)$ by*

$$K(m,n,\chi;p)=\sum_{a=1}^{p-1}\chi(a)e\left(\frac{ma+n\overline{a}}{p}\right).$$

If $(m,n,p)=1$, then we have

$$|K(m,n,\chi;p)|\le 2p^{\frac{1}{2}}.$$

Proof. See reference [11]. □

Lemma 2.2. *Let p be a prime, let χ be a Dirichlet character modulo p, and let m and n be integers with $(n,p)=1$. Then we have*

$$\sum_{a=1}^{p-1}(-1)^a\chi(a)e\left(\frac{ma+n\overline{a}}{p}\right)\ll\sqrt{p}\log p.$$

Proof. From the trigonometric identity

$$\sum_{u=1}^{p}\mathrm{e}\left(\frac{un}{p}\right)=\begin{cases} p, & \text{if } p\mid n,\\ 0, & \text{if } p\nmid n,\end{cases} \tag{2.1}$$

we have

$$\begin{aligned}&\sum_{a=1}^{p-1}(-1)^a\chi(a)\mathrm{e}\left(\frac{ma+n\overline{a}}{p}\right)\\ &=\frac{1}{p}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{u=1}^{p}\mathrm{e}\left(\frac{u(a-b)}{p}\right)(-1)^b\chi(a)\mathrm{e}\left(\frac{ma+n\overline{a}}{p}\right)\\ &=\frac{1}{p}\sum_{u=1}^{p}\sum_{b=1}^{p-1}(-1)^b\mathrm{e}\left(-\frac{ub}{p}\right)\sum_{a=1}^{p-1}\chi(a)\mathrm{e}\left(\frac{(m+u)a+n\overline{a}}{p}\right).\end{aligned}$$

Noting that

$$\sum_{b=1}^{p-1}(-1)^b\mathrm{e}\left(-\frac{ub}{p}\right)\ll\frac{1}{\left|\sin\left(\frac{\pi}{2}-\frac{\pi u}{p}\right)\right|}, \tag{2.2}$$

then by Lemma 2.1 we get

$$\sum_{a=1}^{p-1}(-1)^a\chi(a)\mathrm{e}\left(\frac{ma+n\overline{a}}{p}\right)\ll\frac{1}{\sqrt{p}}\sum_{u=1}^{p}\frac{1}{\left|\sin\left(\frac{\pi}{2}-\frac{\pi u}{p}\right)\right|}\ll\sqrt{p}\log p.$$

This proves Lemma 2.2. □

Lemma 2.3. *Let Ψ be a nontrivial additive character, let χ be a multiplicative character on a finite field $\mathcal{F}_q$ of characteristic p, let f, g be rational functions in $\mathcal{F}_q(x)$ and let*

$$K(\Psi, f; \chi, g) = \sum_{x \in \mathcal{F}_q \setminus s} \chi(g(x))\Psi(f(x)),$$

where s denotes the set of poles of f and g. For $f = f_1/f_2$ we define $\deg(f) = \deg(f_1) - \deg(f_2)$. If $K(\Psi, f; \chi, g)$ is a nondegenerate sum with polynomial f and rational g, we have

$$|K(\Psi, f; \chi, g)| \leq (\deg(f) + l - 1)\, q^{\frac{1}{2}},$$

where l is the number of distinct zeros and (non-infinite) poles of g in $\overline{\mathcal{F}}_p$.

Proof. See reference [12]. □

Lemma 2.4. *Let p be an odd prime, let χ_2 be the Legendre symbol, and let r and s be integers with $(rs, p) = 1$. Then for $1 \leq a + tb + d_2 \leq p - 1$, $0 \leq d_1 < d_2$ and $1 \leq a + d_1$, we have*

$$\Lambda = \sum_{j=0}^{t} \chi_2(a + jb + d_1)\chi_2(a + jb + d_2)\mathrm{e}\left(\frac{r\overline{a + jb + d_1} + s\overline{a + jb + d_2}}{p}\right) \ll p^{\frac{1}{2}} \log p.$$

Proof. By (2.1) we get

$$\begin{aligned}
\Lambda &= \frac{1}{p} \sum_{\substack{j=0 \\ p \nmid a+jb+d_1 \\ p \nmid a+jb+d_2}}^{p-1} \sum_{l=0}^{t} \sum_{u=1}^{p} \mathrm{e}\left(\frac{u(j-l)}{p}\right) \chi_2(a + jb + d_1)\chi_2(a + jb + d_2) \\
&\qquad \times \mathrm{e}\left(\frac{r\overline{a + jb + d_1} + s\overline{a + jb + d_2}}{p}\right) \\
&= \frac{1}{p} \sum_{u=1}^{p} \sum_{l=0}^{t} \mathrm{e}\left(-\frac{ul}{p}\right) \sum_{\substack{j=0 \\ p \nmid a+jb+d_1 \\ p \nmid a+jb+d_2}}^{p-1} \chi_2(a + jb + d_1)\chi_2(a + jb + d_2) \\
&\qquad \times \mathrm{e}\left(\frac{r\overline{a + jb + d_1} + s\overline{a + jb + d_2} + uj}{p}\right).
\end{aligned}$$

Let $g(j) = (a + jb + d_1)(a + jb + d_2)$ and

$$f(j) = \frac{r(a + jb + d_2) + s(a + jb + d_1) + uj(a + jb + d_1)(a + jb + d_2)}{(a + jb + d_1)(a + jb + d_2)}.$$

Then the sum

$$\begin{aligned}
&\sum_{\substack{j=0 \\ p \nmid a+jb+d_1 \\ p \nmid a+jb+d_2}}^{p-1} \chi_2(a + jb + d_1)\chi_2(a + jb + d_2)\mathrm{e}\left(\frac{r\overline{a + jb + d_1} + s\overline{a + jb + d_2} + uj}{p}\right) \\
&\quad = \sum_{\substack{j=0 \\ p \nmid a+jb+d_1 \\ p \nmid a+jb+d_2}}^{p-1} \chi_2(g(x))\mathrm{e}\left(\frac{f(x)}{p}\right)
\end{aligned}$$

is nondegenerate since $(rs, p) = 1$ and $d_1 \neq d_2$. Noting that

$$\sum_{l=0}^{t} \mathrm{e}\left(-\frac{ul}{p}\right) \ll \frac{1}{\left|\sin\left(\frac{\pi u}{p}\right)\right|}, \qquad \text{for } \ p \nmid u, \tag{2.3}$$

then from Lemma 2.3 we have

$$\Lambda \ll \frac{t}{\sqrt{p}} + \frac{1}{\sqrt{p}} \sum_{u=1}^{p-1} \frac{1}{\left|\sin\left(\frac{\pi u}{p}\right)\right|} \ll p^{\frac{1}{2}} \log p.$$

This completes the proof of Lemma 2.4. □

Lemma 2.5. *Let p be an odd prime and let k_1 and k_2 be nonnegative integers. Then for $1 \leq a + tb + d_2 \leq p - 1$, $0 \leq d_1 < d_2$ and $1 \leq a + d_1$, we have*

$$\begin{aligned}
\Upsilon &= \sum_{j=0}^{t} \chi_2(a + jb + d_1)\chi_2(a + jb + d_2) \sum_{\substack{\chi'(-1)=-1 \\ \chi' \bmod p}} \sum_{\substack{\chi''(-1)=-1 \\ \chi'' \bmod p}} \chi'\left(2^{k_1}\right)\chi''\left(2^{k_2}\right) \\
&\qquad \times \chi'(a + jb + d_1)\chi''(a + jb + d_2)\tau(\chi')\tau(\chi'')L(1, \overline{\chi}')L(1, \overline{\chi}'') \\
&\ll p^{\frac{5}{2}} \log^3 p,
\end{aligned}$$

where χ_2 is the Legendre symbol, $\tau(\chi) = \sum_{a=1}^{p-1} \chi(a) e\left(\frac{a}{p}\right)$ is the Gauss sum, and $L(1, \chi)$ denotes the Dirichlet L-function.

Proof. For any nonprincipal character χ modulo p, and parameter $N \geq p$, by Abel's identity we get

$$\begin{aligned}
L(1, \chi) &= \sum_{n=1}^{+\infty} \frac{\chi(n)}{n} = \sum_{1 \leq n \leq N} \frac{\chi(n)}{n} + \int_N^{+\infty} \frac{\sum_{N < n \leq y} \chi(n)}{y^2} \mathrm{d}y \\
&= \sum_{1 \leq n \leq N} \frac{\chi(n)}{n} + O\left(\frac{\sqrt{p} \log p}{N}\right).
\end{aligned}$$

Then we have

$$\begin{aligned}
\Upsilon = &\sum_{j=0}^{t} \chi_2(a+jb+d_1)\chi_2(a+jb+d_2) \sum_{\substack{\chi'(-1)=-1\\ \chi' \bmod p}} \sum_{\substack{\chi''(-1)=-1\\ \chi'' \bmod p}} \chi'\left(2^{k_1}\right)\chi''\left(2^{k_2}\right) \\
&\times \chi'(a+jb+d_1)\chi''(a+jb+d_2)\sum_{r=1}^{p-1}\chi'(r)\mathrm{e}\left(\frac{r}{p}\right)\sum_{s=1}^{p-1}\chi''(s)\mathrm{e}\left(\frac{s}{p}\right) \\
&\times \sum_{1\le n\le N}\frac{\overline{\chi}'(n)}{n}\sum_{1\le m\le N}\frac{\overline{\chi}''(m)}{m} + O\left(\frac{tp^{\frac{7}{2}}\log p\log N}{N}\right) \\
= &\sum_{j=0}^{t} \chi_2(a+jb+d_1)\chi_2(a+jb+d_2) \sum_{1\le n\le N}\frac{1}{n}\sum_{1\le m\le N}\frac{1}{m}\sum_{r=1}^{p-1}\mathrm{e}\left(\frac{r}{p}\right)\sum_{s=1}^{p-1}\mathrm{e}\left(\frac{s}{p}\right) \\
&\times \sum_{\substack{\chi'(-1)=-1\\ \chi' \bmod p}} \chi'\left(2^{k_1}\right)\chi'(a+jb+d_1)\chi'(r)\overline{\chi}'(n) \\
&\times \sum_{\substack{\chi''(-1)=-1\\ \chi'' \bmod p}} \chi''\left(2^{k_2}\right)\chi''(a+jb+d_2)\chi''(s)\overline{\chi}''(m) + O\left(\frac{tp^{\frac{7}{2}}\log p\log N}{N}\right) \\
= &\ \Omega + O\left(\frac{tp^{\frac{7}{2}}\log p\log N}{N}\right). \qquad (2.4)
\end{aligned}$$

For $(ab,p)=1$, from the orthogonality relation for character sums,

$$\sum_{\chi \bmod p}\chi(a)\overline{\chi}(b) = \begin{cases} p-1, & \text{if } a\equiv b \bmod p, \\ 0, & \text{otherwise,} \end{cases} \qquad (2.5)$$

we get

$$\sum_{\substack{\chi(-1)=-1\\ \chi \bmod p}}\chi(a)\overline{\chi}(b) = \begin{cases} \frac{1}{2}(p-1), & \text{if } a\equiv b \bmod p, \\ -\frac{1}{2}(p-1), & \text{if } a\equiv -b \bmod p, \\ 0, & \text{otherwise.} \end{cases}$$

Therefore

$$\begin{aligned}
\Omega = &\frac{(p-1)^2}{4}\sum_{j=0}^{t}\chi_2(a+jb+d_1)\chi_2(a+jb+d_2)\sum_{\substack{1\le n\le N\\ (n,p)=1}}\frac{1}{n}\sum_{\substack{1\le m\le N\\ (m,p)=1}}\frac{1}{m} \qquad (2.6)\\
&\times \sum_{\substack{r=1\\ 2^{k_1}(a+jb+d_1)r\equiv n \bmod p}}^{p-1}\mathrm{e}\left(\frac{r}{p}\right)\sum_{\substack{s=1\\ 2^{k_2}(a+jb+d_2)s\equiv m \bmod p}}^{p-1}\mathrm{e}\left(\frac{s}{p}\right)
\end{aligned}$$

$$
\begin{aligned}
&- \frac{(p-1)^2}{4} \sum_{j=0}^{t} \chi_2(a+jb+d_1)\chi_2(a+jb+d_2) \sum_{\substack{1\le n\le N\\(n,p)=1}} \frac{1}{n} \sum_{\substack{1\le m\le N\\(m,p)=1}} \frac{1}{m} \\
&\qquad \times \sum_{\substack{r=1\\ 2^{k_1}(a+jb+d_1)r\equiv n \bmod p}}^{p-1} \mathrm{e}\left(\frac{r}{p}\right) \sum_{\substack{s=1\\ 2^{k_2}(a+jb+d_2)s\equiv -m \bmod p}}^{p-1} \mathrm{e}\left(\frac{s}{p}\right) \\
&- \frac{(p-1)^2}{4} \sum_{j=0}^{t} \chi_2(a+jb+d_1)\chi_2(a+jb+d_2) \sum_{\substack{1\le n\le N\\(n,p)=1}} \frac{1}{n} \sum_{\substack{1\le m\le N\\(m,p)=1}} \frac{1}{m} \\
&\qquad \times \sum_{\substack{r=1\\ 2^{k_1}(a+jb+d_1)r\equiv -n \bmod p}}^{p-1} \mathrm{e}\left(\frac{r}{p}\right) \sum_{\substack{s=1\\ 2^{k_2}(a+jb+d_2)s\equiv m \bmod p}}^{p-1} \mathrm{e}\left(\frac{s}{p}\right) \\
&+ \frac{(p-1)^2}{4} \sum_{j=0}^{t} \chi_2(a+jb+d_1)\chi_2(a+jb+d_2) \sum_{\substack{1\le n\le N\\(n,p)=1}} \frac{1}{n} \sum_{\substack{1\le m\le N\\(m,p)=1}} \frac{1}{m} \\
&\qquad \times \sum_{\substack{r=1\\ 2^{k_1}(a+jb+d_1)r\equiv -n \bmod p}}^{p-1} \mathrm{e}\left(\frac{r}{p}\right) \sum_{\substack{s=1\\ 2^{k_2}(a+jb+d_2)s\equiv -m \bmod p}}^{p-1} \mathrm{e}\left(\frac{s}{p}\right) \\
&= \Omega_1 + \Omega_2 + \Omega_3 + \Omega_4.
\end{aligned}
$$

By Lemma 2.4 we have

$$
\begin{aligned}
\Omega_1 \quad &= \quad \frac{(p-1)^2}{4} \sum_{\substack{1\le n\le N\\(n,p)=1}} \frac{1}{n} \sum_{\substack{1\le m\le N\\(m,p)=1}} \frac{1}{m} \sum_{j=0}^{t} \chi_2(a+jb+d_1)\chi_2(a+jb+d_2) \\
&\qquad \times \mathrm{e}\left(\frac{n\overline{2^{k_1}a+jb+d_1} + m\overline{2^{k_2}a+jb+d_2}}{p}\right) \\
&\ll \quad p^{\frac{5}{2}} \log p \log^2 N. \qquad (2.7)
\end{aligned}
$$

Similarly we get

$$
\Omega_2, \Omega_3, \Omega_4 \ll p^{\frac{5}{2}} \log p \log^2 N. \qquad (2.8)
$$

Now taking $N = p^2$ in (2.4), (2.6), (2.7) and (2.8), we immediately have

$$
\Upsilon \ll p^{\frac{5}{2}} \log^3 p.
$$

This proves Lemma 2.5. □

3. Proof of the theorem

For a, b, t with $1 \le a \le a + (t-1)b \le p-1$, by (1.1) and (2.1) we have

$$\begin{aligned}
\sum_{j=0}^{t-1} e_{a+jb} &= \sum_{j=0}^{t-1} (-1)^{a+jb+\overline{a+jb}} \chi_2(a+jb) \\
&= \frac{1}{p^3} \sum_{\substack{j=0 \\ p\nmid a+jb}}^{p-1} \sum_{l=0}^{t-1} \sum_{u=1}^{p} \mathrm{e}\left(\frac{u(j-l)}{p}\right) \sum_{c=1}^{p-1} \sum_{r=1}^{p} \mathrm{e}\left(\frac{r(a+jb-c)}{p}\right) \\
&\quad \times \sum_{d=1}^{p-1} \sum_{s=1}^{p} \mathrm{e}\left(\frac{s(\overline{a+jb}-d)}{p}\right) (-1)^{c+d} \chi_2(c) \\
&= \frac{1}{p^3} \sum_{r=1}^{p} \sum_{s=1}^{p-1} \sum_{u=1}^{p} \sum_{l=0}^{t-1} \mathrm{e}\left(-\frac{ul}{p}\right) \sum_{c=1}^{p-1} (-1)^c \chi_2(c) \mathrm{e}\left(-\frac{rc}{p}\right) \sum_{d=1}^{p-1} (-1)^d \mathrm{e}\left(-\frac{sd}{p}\right) \\
&\quad \times \sum_{\substack{j=0 \\ p\nmid a+jb}}^{p-1} \mathrm{e}\left(\frac{r(a+jb)+s\overline{a+jb}+uj}{p}\right) \\
&= \frac{1}{p^3} \sum_{r=1}^{p} \sum_{s=1}^{p-1} \sum_{u=1}^{p} \sum_{l=0}^{t-1} \mathrm{e}\left(-\frac{ul}{p}\right) \sum_{c=1}^{p-1} (-1)^c \chi_2(c) \mathrm{e}\left(-\frac{rc}{p}\right) \sum_{d=1}^{p-1} (-1)^d \mathrm{e}\left(-\frac{sd}{p}\right) \\
&\quad \times \mathrm{e}\left(-\frac{ua\overline{b}}{p}\right) \sum_{t=1}^{p-1} \mathrm{e}\left(\frac{rt+s\overline{t}+u\overline{b}t}{p}\right) \\
&= \frac{1}{p^2} \sum_{s=1}^{p-1} \left(\sum_{d=1}^{p-1} (-1)^d \mathrm{e}\left(-\frac{sd}{p}\right)\right) \sum_{u=1}^{p} \left(\sum_{l=0}^{t-1} \mathrm{e}\left(-\frac{ul}{p}\right)\right) \mathrm{e}\left(-\frac{ua\overline{b}}{p}\right) \\
&\qquad \times \left(\sum_{t=1}^{p-1} (-1)^t \chi_2(t) \mathrm{e}\left(\frac{u\overline{b}t+s\overline{t}}{p}\right)\right).
\end{aligned}$$

Then by (2.2), (2.3) and Lemma 2.2 we get

$$\begin{aligned}
\sum_{j=0}^{t-1} e_{a+jb} &\ll \frac{tp^{\frac{1}{2}}}{p^2} \sum_{s=1}^{p-1} \frac{1}{\left|\sin\left(\frac{\pi}{2}-\frac{\pi s}{p}\right)\right|} + \frac{p^{\frac{1}{2}}}{p^2} \sum_{s=1}^{p-1} \frac{1}{\left|\sin\left(\frac{\pi}{2}-\frac{\pi s}{p}\right)\right|} \sum_{u=1}^{p-1} \frac{1}{\left|\sin\left(\frac{\pi u}{p}\right)\right|} \\
&\ll p^{\frac{1}{2}} \log^2 p.
\end{aligned}$$

Therefore

$$W\left(E_{p-1}\right) = \max_{a,b,t} \left|\sum_{j=0}^{t-1} e_{a+jb}\right| \ll p^{\frac{1}{2}} \log^2 p.$$

For $1 \le a + tb + d_2 \le p - 1$ and $0 \le d_1 < d_2$, by (1.1) and (2.5) we have

$$\begin{aligned}
&\sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \\
&= \sum_{j=0}^{t} (-1)^{a+jb+d_1+\overline{a+jb+d_1}} \chi_2(a+jb+d_1)(-1)^{a+jb+d_2+\overline{a+jb+d_2}} \chi_2(a+jb+d_2) \\
&= (-1)^{d_1+d_2} \sum_{j=0}^{t} (-1)^{\overline{a+jb+d_1}+\overline{a+jb+d_2}} \chi_2(a+jb+d_1)\chi_2(a+jb+d_2) \\
&= \frac{(-1)^{d_1+d_2}}{(p-1)^2} \sum_{j=0}^{t} \sum_{r=1}^{p-1} \sum_{s=1}^{p-1} \sum_{\chi' \bmod p} \chi'(r(a+jb+d_1)) \sum_{\chi'' \bmod p} \chi''(s(a+jb+d_2)) \\
&\qquad \times (-1)^{r+s} \chi_2(a+jb+d_1)\chi_2(a+jb+d_2) \\
&= \frac{(-1)^{d_1+d_2}}{(p-1)^2} \sum_{\chi' \bmod p} \sum_{\chi'' \bmod p} \sum_{j=0}^{t} (\chi'(a+jb+d_1)\chi_2(a+jb+d_1) \\
&\qquad\qquad\qquad\qquad \times \chi''(a+jb+d_2)\chi_2(a+jb+d_2)) \\
&\qquad \times \sum_{r=1}^{p-1} (-1)^r \chi'(r) \sum_{s=1}^{p-1} (-1)^s \chi''(s).
\end{aligned}$$

Noting that

$$\sum_{r=1}^{p-1} (-1)^r \chi(r) = 0, \qquad \text{if } \ \chi(-1) = 1,$$

while if $\chi(-1) = -1$, from [6] and Theorem 12.11, 12.20 of [1] we have

$$\begin{aligned}
\sum_{r=1}^{p-1} (-1)^r \chi(r) &= 2\chi(2) \sum_{r=1}^{(p-1)/2} \chi(r) = \frac{2(1-2\chi(2))}{p} \sum_{r=1}^{p-1} r\chi(r) \\
&= \frac{2(1-2\chi(2))i}{\pi} \tau(\chi) L(1, \overline{\chi}).
\end{aligned}$$

So from Lemma 2.5 we get

$$\begin{aligned}
\sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} &= \frac{4(-1)^{d_1+d_2+1}}{\pi^2 (p-1)^2} \sum_{j=0}^{t} \chi_2(a+jb+d_1)\chi_2(a+jb+d_2) \\
&\quad \times \sum_{\substack{\chi'(-1)=-1 \\ \chi' \bmod p}} \sum_{\substack{\chi''(-1)=-1 \\ \chi'' \bmod p}} (1-2\chi'(2))(1-2\chi''(2))\chi'(a+jb+d_1)\chi''(a+jb+d_2) \\
&\quad \times \ \tau(\chi')\tau(\chi'') L(1, \overline{\chi}') L(1, \overline{\chi}'') \\
&\ll p^{\frac{1}{2}} \log^3 p.
\end{aligned}$$

Therefore

$$Q_2\left(E_{p-1}\right) = \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \right| \ll p^{\frac{1}{2}} \log^3 p. \tag{3.1}$$

Now taking $a = 0$, $b = 1$, $j = n - 1$ and $t = M - 1$ in (3.1), we immediately get

$$C_2\left(E_{p-1}\right) = \max_{M,D}\left|\sum_{n=1}^{M} e_{n+d_1} e_{n+d_2}\right| \ll p^{\frac{1}{2}} \log^3 p.$$

This completes the proof of Theorem 1.1.

Acknowledgments

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

References

[1] T. M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, New York, 1976. MR0434929 (55:7892)

[2] 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), pp. 367–390. MR1671629 (2000c:11126)

[3] J. Cassaigne, S. Ferenczi, C. Mauduit, J. Rivat and A. Sárközy, On finite pseudorandom binary sequencs IV: the Liouville function, II, *Acta Arithmetica,* 95 (2000), pp. 343–359. MR1785199 (2002c:11087)

[4] J. Cassaigne, C. Mauduit and A. Sárközy, On finite pseudorandom binary sequencs VII: the measures of pseudorandomness, *Acta Arithmetica,* 103 (2002), pp. 97–108. MR1904866 (2004c:11139)

[5] E. Fouvry, P. Michel, J. Rivat and A. Sárközy, On the pseudorandomness of the signs of Kloosterman sums, *Journal of the Australian Mathematical Society,* 77 (2004), pp. 425–436. MR2099811 (2005h:11165)

[6] T. Funakura, On Kronecker's limit formula for Dirichlet series with periodic coefficients, *Acta Arithmetica,* 55 (1990), pp. 59–73. MR1056115 (91j:11064)

[7] R. K. Guy, *Unsolved problems in number theory*, Springer-Verlag, New York, 1994. MR1299330 (96e:11002)

[8] S. R. Louboutin, J. Rivat and A. Sárközy, On a problem of D. H. Lehmer, *Proceedings of the American Mathematical Society,* to appear.

[9] C. Mauduit and A. Sárközy, On finite pseudorandom binary sequences I: measure of pseudorandomness, the Legendre symbol, *Acta Arithmetica,* 82 (1997), pp. 365–377. MR1483689 (99g:11095)

[10] C. Mauduit and A. Sárközy, On the measures of pseudorandomness of binary sequences, *Discrete Mathematics,* 271 (2003), pp. 195–207. MR1999543 (2004e:11081)

[11] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Act. Sci. Ind., Vol. 1041, Hermann, Paris, 1948. MR0027151 (10:262c)

[12] A. Weil, On some exponential sums, *Proc. Nat. Acad. Sci.,* 34 (1948), pp. 204–207. MR0027006 (10:234e)

[13] W. Zhang, A problem of D. H. Lehmer and its generalization (I), *Compositio Mathematica,* 86 (1993), pp. 307–316. MR1219630 (94f:11104)

[14] W. Zhang, A problem of D. H. Lehmer and its generalization (II), *Compositio Mathematica,* 91 (1994), pp. 47–56. MR1273925 (95f:11079)

[15] W. Zhang, On the difference between a D. H. Lehmer number and its inverse modulo q, *Acta Arithmetica,* 68 (1994), pp. 255–263. MR1308126 (96a:11100)

[16] W. Zhang, On a problem of D. H. Lehmer and Kloosterman sums, *Monatshefte für Mathematik,* 139 (2003), pp. 247–257. MR1994384 (2004e:11088)

[17] W. Zhang, On a problem of D. H. Lehmer and general Kloosterman sums, *Acta Mathematica Sinica English Series,* 20 (2004), pp. 515–524. MR2084715 (2005h:11226)

[18] W. Zhang, Z. Xu and Y. Yi, A problem of D. H. Lehmer and its mean square value formula, *Journal of Number Theory,* 103 (2003), pp. 197–213. MR2020268 (2004m:11128)

Department of Mathematics, Northwest University, Xi'an, Shaanxi, People's Republic of China

E-mail address: hnliu@nwu.edu.cn