ACTA ARITHMETICA
125.1 (2006)

New pseudorandom sequences constructed using multiplicative inverses

by

Huaning Liu (Xi'an)

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

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

In [5] Mauduit and Sárközy first introduced the following measures of pseudorandomness: the *well-distribution measure* of E_N is defined by

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

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

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

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

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

is defined for all a, b, t, $D = (d_1, \dots, d_k)$ with $1 \le a + jb + d_i \le N$ ($i = 1, \dots, k$). In [6] the connection between the measures W and C_2 was studied.

A pseudorandom sequence E_N is considered to be "good" if both $W(E_N)$ and $C_k(E_N)$ (at least for small k) are "small" in terms of N. Later Cas-

---

2000 *Mathematics Subject Classification*: Primary 11K45.

Key words and phrases: pseudorandom, binary sequence, exponential sums.

Supported by the National Natural Science Foundation of China under Grant No. 60472068; and the Natural Science Foundation of the Education Department of Shaanxi Province of China under Grant No. 06JK168.

saigne, Mauduit and Sárközy [3] proved that this terminology is justified since for almost all $E_N \in \{-1,+1\}^N$, both $W(E_N)$ and $C_k(E_N)$ are less than $N^{1/2}(\log N)^c$. Moreover, it was shown in [5] that the Legendre symbol forms a "good" pseudorandom sequence. In [1] and [2], Cassaigne and coauthors studied the pseudorandomness of the Liouville function, defined as $\lambda(n) = (-1)^{\Omega(n)}$ ($\Omega(n)$ being the number of prime factors of n counted with multiplicity) and also of $\gamma(n) = (-1)^{\omega(n)}$ ($\omega(n)$ being the 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 sums, where $\mathrm{e}(y) = e^{2\pi iy}$, p is a prime, and $\overline{a}$ is the multiplicative inverse of a modulo p such that $1 \le \overline{a} \le p-1$. Fouvry (with coauthors) [4] showed that the signs of $K(1,n;p)$ form a "good" pseudorandom binary sequence.

Assume that p is a prime number, $f(x) \in \mathbb{F}_p[x]$ has degree k ($0 < k < p$) and no multiple zero in $\overline{\mathbb{F}}_p$, and $r_p(n)$ is defined to be the least non-negative residue of n modulo p. Define the binary sequence $E_p = (e_1, \ldots, e_p)$ by

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

Mauduit and Sárközy [7] proved that this large family of finite binary sequences has strong pseudorandom properties.

As was said in [5], 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. Define

$$e_n = \begin{cases} (-1)^{\overline{n}+\overline{n+x}} & \text{if } p \nmid n \text{ and } p \nmid n+x, \\ 1 & \text{otherwise}, \end{cases} \tag{1.1}$$

where x is an integer with $1 \le x \le p-1$. We shall prove that $\{e_n\}$ is a "good" pseudorandom sequence:

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

$$W(E_{p-1}) \ll p^{1/2}\log^3 p, \quad C_2(E_{p-1}) \ll p^{1/2}\log^5 p, \quad Q_2(E_{p-1}) \ll p^{1/2}\log^5 p.$$

2. Some lemmas. We need the following lemmas.

LEMMA 2.1 ([9]). *Let p be a prime, and m and n be integers. Then*

$$K(m,n;p) \ll (m,n,p)^{1/2}p^{1/2},$$

where (m,n,p) denotes the greatest common divisor of m, n and p.

LEMMA 2.2 ([8]). *For any polynomials $g(x), h(x) \in \mathbb{F}_p[x]$ such that the rational function $f(x) = g(x)/h(x)$ is not constant on $\mathbb{F}_p$, let s be the number of distinct roots of $h(x)$. Then*

$$\Bigg| \sum_{\substack{n\in\mathbb{F}_p\\ h(n)\neq 0}} \mathrm{e}\left(\frac{g(n)}{h(n)p}\right)\Bigg| \leq (\max(\deg(g),\deg(h)) + s - 1)\sqrt{p}.$$

LEMMA 2.3. *For $1 \leq a, b, x, r, s \leq p-1$ and $1 \leq u \leq p$, we have*

$$\Psi = \sum_{\substack{j=0\\ p\nmid a+jb\\ p\nmid a+jb+x}}^{p-1} \mathrm{e}\left(\frac{r\overline{a+jb} + s\overline{a+jb+x} + uj}{p}\right) \ll \sqrt{p}.$$

Proof. If $u = p$, from the properties of a residue system we get

$$\Psi = \sum_{\substack{j=0\\ p\nmid a+jb\\ p\nmid a+jb+x}}^{p-1} \mathrm{e}\left(\frac{r\overline{a+jb} + s\overline{a+jb+x}}{p}\right) = \sum_{\substack{j=0\\ p\nmid a+j\\ p\nmid a+j+x}}^{p-1} \mathrm{e}\left(\frac{r\overline{a+j} + s\overline{a+j+x}}{p}\right)$$
$$= \sum_{\substack{j=1\\ p\nmid j+x}}^{p-1} \mathrm{e}\left(\frac{r\overline{j} + s\overline{j+x}}{p}\right).$$

Since

$$\overline{j+x} \equiv \overline{jx\overline{x} + xj\overline{j}} \equiv \overline{x}\overline{j}\,\overline{\overline{x}+\overline{j}} \equiv \overline{x}(\overline{j}+\overline{x}-\overline{x})\overline{\overline{j}+\overline{x}} \equiv \overline{x} - \overline{x}^2\,\overline{\overline{j}+\overline{x}} \bmod p,$$

by Lemma 2.1 we have

$$\Psi = \sum_{\substack{j=1\\ p\nmid \overline{j}+\overline{x}}}^{p-1} \mathrm{e}\left(\frac{r\overline{j} + s(\overline{x} - \overline{x}^2\,\overline{\overline{j}+\overline{x}})}{p}\right)$$
$$= \mathrm{e}\left(\frac{\overline{x}(s-r)}{p}\right) \sum_{\substack{j=1\\ p\nmid \overline{j}+\overline{x}}}^{p-1} \mathrm{e}\left(\frac{r(\overline{j}+\overline{x}) - s\overline{x}^2\,\overline{\overline{j}+\overline{x}}}{p}\right)$$
$$= \mathrm{e}\left(\frac{\overline{x}(s-r)}{p}\right) \sum_{\substack{j=1\\ j\neq \overline{x}}}^{p-1} \mathrm{e}\left(\frac{rj - s\overline{x}^2\overline{j}}{p}\right) \ll \sqrt{p}.$$

Now we suppose $1 \leq u \leq p-1$. Then

$$\Psi = \sum_{\substack{j=0\\ p\nmid a+jb\\ p\nmid a+jb+x}}^{p-1} \mathrm{e}\left(\frac{r(a+jb+x) + s(a+jb) + uj(a+jb)(a+jb+x)}{(a+jb)(a+jb+x)p}\right).$$

Let $g(j) = r(a + jb + x) + s(a + jb) + uj(a + jb)(a + jb + x)$, and $h(j) = (a+jb)(a+jb+x)$. Since $1 \le u, b \le p-1$, we have $0 < \deg(h) < \deg(g)$. That is to say, the rational function g/h over $\mathbb{F}_p$ is not constant. Then Lemma 2.2 yields the assertion.

LEMMA 2.4. *For* $1 \le r_1, s_1, r_2, s_2, x \le p-1$, $1 \le d_1 < d_2 \le p-1$ *and* $1 \le u \le p$, *we have*

$$\Omega = \sum_{\substack{n=1\\ p\nmid n+d_1, n+d_1+x\\ p\nmid n+d_2, n+d_2+x}}^{p} \mathrm{e}\left(\frac{r_1\overline{n+d_1}+s_1\overline{n+d_1+x}+r_2\overline{n+d_2}+s_2\overline{n+d_2+x}+un}{p}\right) \ll \sqrt{p}.$$

Proof. Let

$$\begin{aligned} g(n) = {} & r_1(n + d_1 + x)(n + d_2)(n + d_2 + x) + s_1(n + d_1)(n + d_2)(n + d_2 + x)\\ & + r_2(n + d_1)(n + d_1 + x)(n + d_2 + x)\\ & + s_2(n + d_1)(n + d_1 + x)(n + d_2)\\ & + un(n + d_1)(n + d_1 + x)(n + d_2)(n + d_2 + x),\\ h(n) = {} & (n + d_1)(n + d_1 + x)(n + d_2)(n + d_2 + x). \end{aligned}$$

We have

$$\Omega = \sum_{\substack{n=1\\ p\nmid n+d_1, n+d_1+x\\ p\nmid n+d_2, n+d_2+x}}^{p} \mathrm{e}\left(\frac{g(n)}{h(n)p}\right).$$

If $1 \le u \le p-1$, then $0 < \deg(h) < \deg(g)$ and it remains to apply Lemma 2.2.

If $u = p$, we need to prove $g(n) \not\equiv 0 \bmod p$. Suppose that $g(n) \equiv 0 \bmod p$. Then comparing the coefficients of n^3, n^2, n and n^0 we have

$$(2.1)\quad \begin{cases} r_1 + s_1 + r_2 + s_2 \equiv 0 \bmod p,\\ r_1(d_1 + 2d_2 + 2x) + s_1(d_1 + 2d_2 + x) + r_2(2d_1 + d_2 + 2x)\\ \qquad + s_2(2d_1 + d_2 + x) \equiv 0 \bmod p,\\ r_1(2d_1d_2 + d_2^2 + d_1x + 3d_2x + x^2) + s_1(2d_1d_2 + d_2^2 + d_1x + d_2x)\\ \qquad + r_2(2d_1d_2 + d_1^2 + 3d_1x + d_2x + x^2)\\ \qquad + s_2(2d_1d_2 + d_1^2 + d_1x + d_2x) \equiv 0 \bmod p,\\ r_1(d_1d_2^2 + d_1d_2x + d_2^2x + d_2x^2) + s_1(d_1d_2^2 + d_1d_2x)\\ \qquad + r_2(d_1^2d_2 + d_1^2x + d_1d_2x + d_1x^2) + s_2(d_1^2d_2 + d_1d_2x) \equiv 0 \bmod p. \end{cases}$$

This gives

$$\begin{cases} r_1(d_2-d_1+x)+s_1(d_2-d_1)+r_2x \equiv 0 \bmod p, \\ r_1(d_2^2-d_1^2+2d_2x+x^2)+s_1(d_2^2-d_1^2)+r_2x(2d_1+x) \equiv 0 \bmod p, \\ r_1(d_1d_2^2-d_1^2d_2+d_2^2x+d_2x^2)+s_1(d_1d_2^2-d_1^2d_2)+r_2x(d_1^2+d_1x) \equiv 0 \bmod p, \end{cases}$$

hence

$$\begin{cases} r_1(d_1^2+d_2^2-2d_1d_2-d_1x+d_2x)+s_1(d_1^2+d_2^2-2d_1d_2+d_1x-d_2x) \equiv 0 \bmod p, \\ r_1(d_1^3-2d_1^2d_2+d_1d_2^2-d_1d_2x+d_2^2x-d_1x^2+d_2x^2) \\ \qquad +s_1d_1(d_1^2+d_2^2-2d_1d_2+d_1x-d_2x) \equiv 0 \bmod p. \end{cases}$$

Therefore

$$r_1x(d_2-d_1)(d_2-d_1+x) \equiv 0 \bmod p,$$

and consequently $d_2 \equiv d_1 - x \bmod p$. Inserting this in (2.1), we have

$$\begin{cases} r_1+s_1+r_2+s_2 \equiv 0 \bmod p, \\ 3d_1r_1+(3d_1-x)s_1+(3d_1+x)r_2+3d_1s_2 \equiv 0 \bmod p, \\ d_1^2r_1+(d_1-x)^2s_1+(d_1+x)^2r_2+d_1^2s_2 \equiv 0 \bmod p, \\ d_1^2(d_1-x)r_1+d_1(d_1-x)^2s_1+d_1(d_1^2+x^2)r_2+d_1^2(d_1-x)s_2 \equiv 0 \bmod p. \end{cases}$$

This implies $s_1 \equiv r_2 \equiv 0 \bmod p$, which is impossible. So $g(n) \not\equiv 0 \bmod p$, and an appeal to Lemma 2.2 completes the proof.

3. Proof of Theorem 1.1. For a, b, t with $1 \le a \le a+(t-1)b \le p-1$, by (1.1) we have

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

Since

$$\begin{aligned}\sum_{l=0}^{t-1} \mathrm{e}\left(-\frac{ul}{p}\right) &\ll \frac{1}{|\sin(\pi u/p)|} \quad \text{for} \ \ p\nmid u,\\ \sum_{c=1}^{p-1}(-1)^c \mathrm{e}\left(-\frac{rc}{p}\right) &\ll \frac{1}{|\sin(\pi/2-\pi r/p)|},\end{aligned} \tag{3.1}$$

from Lemma 2.3 we have

$$\begin{aligned}\sum_{j=0}^{t-1} e_{a+jb} &\ll \frac{tp^{1/2}}{p^3}\sum_{r=1}^{p-1}\frac{1}{|\sin(\pi/2-\pi r/p)|}\sum_{s=1}^{p-1}\frac{1}{|\sin(\pi/2-\pi s/p)|}\\ &\quad+\frac{p^{1/2}}{p^3}\sum_{r=1}^{p-1}\frac{1}{|\sin(\pi/2-\pi r/p)|}\sum_{s=1}^{p-1}\frac{1}{|\sin(\pi/2-\pi s/p)|}\sum_{u=1}^{p-1}\frac{1}{|\sin(\pi u/p)|}\\ &\ll p^{1/2}\log^3 p.\end{aligned}$$

Therefore

$$W(E_{p-1}) = \max_{a,b,t}\left|\sum_{j=0}^{t-1} e_{a+jb}\right| \ll p^{1/2}\log^3 p.$$

For $0\le d_1<d_2\le p-1-M$, from (1.1), (3.1) and Lemma 2.4 we have

$$\begin{aligned}\sum_{n=1}^{M} e_{n+d_1}e_{n+d_2} &= \sum_{\substack{n=1\\ p\nmid n+d_1,n+d_1+x\\ p\nmid n+d_2,n+d_2+x}}^{M} (-1)^{\overline{n+d_1}+\overline{n+d_1+x}+\overline{n+d_2}+\overline{n+d_2+x}} + O(1)\\ &= \frac{1}{p^5}\sum_{\substack{n=1\\ p\nmid n+d_1,n+d_1+x\\ p\nmid n+d_2,n+d_2+x}}^{p}\sum_{l=1}^{M}\sum_{u=1}^{p}\mathrm{e}\left(\frac{u(n-l)}{p}\right)\sum_{c_1=1}^{p-1}\sum_{r_1=1}^{p}\mathrm{e}\left(\frac{r_1(\overline{n+d_1}-c_1)}{p}\right)\\ &\quad\times\sum_{d_1=1}^{p-1}\sum_{s_1=1}^{p}\mathrm{e}\left(\frac{s_1(\overline{n+d_1+x}-d_1)}{p}\right)\sum_{c_2=1}^{p-1}\sum_{r_2=1}^{p}\mathrm{e}\left(\frac{r_2(\overline{n+d_2}-c_2)}{p}\right)\\ &\quad\times\sum_{d_2=1}^{p-1}\sum_{s_2=1}^{p}\mathrm{e}\left(\frac{s_2(\overline{n+d_2+x}-d_2)}{p}\right)(-1)^{c_1+d_1+c_2+d_2}+O(1)\\ &= \frac{1}{p^5}\sum_{r_1=1}^{p-1}\sum_{s_1=1}^{p-1}\sum_{r_2=1}^{p-1}\sum_{s_2=1}^{p-1}\sum_{u=1}^{p}\sum_{l=1}^{M}\mathrm{e}\left(-\frac{ul}{p}\right)\\ &\quad\times\sum_{c_1=1}^{p-1}(-1)^{c_1}\mathrm{e}\left(-\frac{r_1c_1}{p}\right)\sum_{d_1=1}^{p-1}(-1)^{d_1}\mathrm{e}\left(-\frac{s_1d_1}{p}\right)\end{aligned}$$

$$\times \sum_{c_2=1}^{p-1}(-1)^{c_2}\mathrm{e}\left(-\frac{r_2c_2}{p}\right)\sum_{d_2=1}^{p-1}(-1)^{d_2}\mathrm{e}\left(-\frac{s_2d_2}{p}\right)$$

$$\times \sum_{\substack{n=1\\ p\nmid n+d_1,n+d_1+x\\ p\nmid n+d_2,n+d_2+x}}^{p} \mathrm{e}\left(\frac{r_1\overline{n+d_1}+s_1\overline{n+d_1+x}+r_2\overline{n+d_2}+s_2\overline{n+d_2+x}+un}{p}\right)$$

$$+\ O(1)$$

$$\ll \frac{Mp^{1/2}}{p^5}\sum_{r_1=1}^{p-1}\frac{1}{|\sin(\pi/2-\pi r_1/p)|}\sum_{s_1=1}^{p-1}\frac{1}{|\sin(\pi/2-\pi s_1/p)|}$$

$$\times\sum_{r_2=1}^{p-1}\frac{1}{|\sin(\pi/2-\pi r_2/p)|}\sum_{s_2=1}^{p-1}\frac{1}{|\sin(\pi/2-\pi s_2/p)|}$$

$$+\frac{p^{1/2}}{p^5}\sum_{r_1=1}^{p-1}\frac{1}{|\sin(\pi/2-\pi r_1/p)|}\sum_{s_1=1}^{p-1}\frac{1}{|\sin(\pi/2-\pi s_1/p)|}$$

$$\times\sum_{r_2=1}^{p-1}\frac{1}{|\sin(\pi/2-\pi r_2/p)|}\sum_{s_2=1}^{p-1}\frac{1}{|\sin(\pi/2-\pi s_2/p)|}\sum_{u=1}^{p-1}\frac{1}{|\sin(\pi u/p)|}$$

$$\ll p^{1/2}\log^5 p.$$

Therefore

$$C_2(E_{p-1}) = \max_{M,D}\left|\sum_{n=1}^{M} e_{n+d_1}e_{n+d_2}\right| \ll p^{1/2}\log^5 p.$$

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

$$\sum_{j=0}^{t} e_{a+jb+d_1}e_{a+jb+d_2}$$

$$= \sum_{\substack{j=0\\ p\nmid a+jb+d_1,a+jb+d_1+x\\ p\nmid a+jb+d_2,a+jb+d_2+x}}^{t} (-1)^{\overline{a+jb+d_1}+\overline{a+jb+d_1+x}+\overline{a+jb+d_2}+\overline{a+jb+d_2+x}}+O(1)$$

$$= \frac{1}{p^5}\sum_{\substack{j=0\\ p\nmid a+jb+d_1,a+jb+d_1+x\\ p\nmid a+jb+d_2,a+jb+d_2+x}}^{p}\sum_{l=0}^{t}\sum_{u=1}^{p}\mathrm{e}\left(\frac{u(j-l)}{p}\right)\sum_{c_1=1}^{p-1}\sum_{r_1=1}^{p}\mathrm{e}\left(\frac{r_1(\overline{a+jb+d_1}-c_1)}{p}\right)$$

$$\times\sum_{d_1=1}^{p-1}\sum_{s_1=1}^{p}\mathrm{e}\left(\frac{s_1(\overline{a+jb+d_1+x}-d_1)}{p}\right)\sum_{c_2=1}^{p-1}\sum_{r_2=1}^{p}\mathrm{e}\left(\frac{r_2(\overline{a+jb+d_2}-c_2)}{p}\right)$$

$$\times\sum_{d_2=1}^{p-1}\sum_{s_2=1}^{p}\mathrm{e}\left(\frac{s_2(\overline{a+jb+d_2+x}-d_2)}{p}\right)(-1)^{c_1+d_1+c_2+d_2}+O(1)$$
$$=\frac{1}{p^5}\sum_{r_1=1}^{p-1}\sum_{s_1=1}^{p-1}\sum_{r_2=1}^{p-1}\sum_{s_2=1}^{p-1}\sum_{u=1}^{p}\sum_{l=0}^{t}\mathrm{e}\left(-\frac{ul}{p}\right)\sum_{c_1=1}^{p-1}(-1)^{c_1}\mathrm{e}\left(-\frac{r_1c_1}{p}\right)$$
$$\times\sum_{d_1=1}^{p-1}(-1)^{d_1}\mathrm{e}\left(-\frac{s_1d_1}{p}\right)\sum_{c_2=1}^{p-1}(-1)^{c_2}\mathrm{e}\left(-\frac{r_2c_2}{p}\right)\sum_{d_2=1}^{p-1}(-1)^{d_2}\mathrm{e}\left(-\frac{s_2d_2}{p}\right)$$
$$\times\sum_{\substack{j=0\\ p\nmid a+jb+d_1,a+jb+d_1+x\\ p\nmid a+jb+d_2,a+jb+d_2+x}}^{p}\mathrm{e}\left(\frac{r_1\overline{a+jb+d_1}+s_1\overline{a+jb+d_1+x}}{p}\right)$$
$$\times\mathrm{e}\left(\frac{r_2\overline{a+jb+d_2}+s_2\overline{a+jb+d_2+x}+uj}{p}\right)+O(1).$$

By Lemma 2.4 we get

$$\sum_{\substack{j=0\\ p\nmid a+jb+d_1\\ p\nmid a+jb+d_1+x\\ p\nmid a+jb+d_2\\ p\nmid a+jb+d_2+x}}^{p}\mathrm{e}\left(\frac{r_1\overline{a+jb+d_1}+s_1\overline{a+jb+d_1+x}}{p}\right)$$
$$\times\mathrm{e}\left(\frac{r_2\overline{a+jb+d_2}+s_2\overline{a+jb+d_2+x}+uj}{p}\right)$$
$$=\mathrm{e}\left(-\frac{ua\overline{b}}{p}\right)$$
$$\times\sum_{\substack{j=0\\ p\nmid j+d_1,j+d_1+x\\ p\nmid j+d_2,j+d_2+x}}^{p}\mathrm{e}\left(\frac{r_1\overline{j+d_1}+s_1\overline{j+d_1+x}+r_2\overline{j+d_2}+s_2\overline{j+d_2+x}+u\overline{b}j}{p}\right)$$
$$\ll p^{1/2}.$$

Then from (3.1) we have

$$\sum_{j=0}^{t}e_{a+jb+d_1}e_{a+jb+d_2}$$
$$\ll\frac{tp^{1/2}}{p^5}\sum_{r_1=1}^{p-1}\frac{1}{|\sin(\pi/2-\pi r_1/p)|}\sum_{s_1=1}^{p-1}\frac{1}{|\sin(\pi/2-\pi s_1/p)|}$$
$$\times\sum_{r_2=1}^{p-1}\frac{1}{|\sin(\pi/2-\pi r_2/p)|}\sum_{s_2=1}^{p-1}\frac{1}{|\sin(\pi/2-\pi s_2/p)|}$$

$$+\frac{p^{1/2}}{p^5}\sum_{r_1=1}^{p-1}\frac{1}{|\sin(\pi/2-\pi r_1/p)|}\sum_{s_1=1}^{p-1}\frac{1}{|\sin(\pi/2-\pi s_1/p)|}$$
$$\times\sum_{r_2=1}^{p-1}\frac{1}{|\sin(\pi/2-\pi r_2/p)|}\sum_{s_2=1}^{p-1}\frac{1}{|\sin(\pi/2-\pi s_2/p)|}\sum_{u=1}^{p-1}\frac{1}{|\sin(\pi u/p)|}$$
$$\ll p^{1/2}\log^5 p.$$

Therefore

$$Q_2(E_{p-1}) = \max_{a,b,t,D}\left|\sum_{j=0}^{t} e_{a+jb+d_1}e_{a+jb+d_2}\right| \ll p^{1/2}\log^5 p.$$

This completes the proof of Theorem 1.1.

References

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

[2] —, —, —, —, —, *On finite pseudorandom binary sequences IV: The Liouville function, II*, ibid. 95 (2000), pp. 343–359.

[3] J. Cassaigne, C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences VII: The measures of pseudorandomness*, ibid. 103 (2002), 97–118.

[4] E. Fouvry, P. Michel, J. Rivat and A. Sárközy, *On the pseudorandomness of the signs of Kloosterman sums*, J. Austral. Math. Soc. 77 (2004), 425–436.

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

[6] —, —, *On the measures of pseudorandomness of binary sequences*, Discrete Math. 271 (2003), 195–207.

[7] —, —, *Construction of pseudorandom binary sequences by using the multiplicative inverse*, Acta Math. Hungar. 108 (2005), 239–252.

[8] C. J. Moreno and O. Moreno, *Exponential sums and Goppa codes: I*, Proc. Amer. Math. Soc. 111 (1991), 523–531.

[9] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Act. Sci. Ind. 1041, Hermann, Paris, 1948.

Department of Mathematics
Northwest University
Xi'an, Shaanxi, P.R. China
E-mail: hnliu@nwu.edu.cn

Received on 9.11.2005
and in revised form on 1.8.2006 (5093)