BULLETIN OF THE BRAZILIAN MATHEMATICAL SOCIETY

Bull Braz Math Soc, New Series 39(3), 387-399

On a problem of D.H. Lehmer and pseudorandom binary sequences*

Huaning Liu and Cundian Yang

Abstract. Let p be an odd prime, and $f(x), g(x) \in \mathbb{F}_p[x]$. Define

$$e'_n = \begin{cases} +1, & \text{if } \overline{f(n)} \equiv R_p(g(n)) (\mathrm{mod}\ 2), \\ -1, & \text{if } \overline{f(n)} \not\equiv R_p(g(n)) (\mathrm{mod}\ 2), \end{cases}$$

where $\overline{x}$ is the inverse of x modulo p with $\overline{x} \in \{1, \ldots, p-1\}$, and $R_p(x)$ denotes the unique $r \in \{0, 1, \ldots, p-1\}$ with $x \equiv r (\mathrm{mod}\ p)$. This paper shows that the sequences $\{e'_n\}$ is a "good" pseudorandom binary sequences, and give a generalization on a problem of D.H. Lehmer.

Keywords: pseudorandom binary sequence, multiplicative inverse, exponential sum.

Mathematical subject classification: 11K45, 11A07, 68Q99.

1 Introduction

Let p be an odd prime number, and let $\overline{n}$ be the multiplicative inverse of n modulo p such that $1 \le \overline{n} \le p-1$ and $n\overline{n} \equiv 1 (\mathrm{mod}\ p)$. D.H. Lehmer [10] asked us to study the case that n and $\overline{n}$ are of opposite parity. W. Zhang [22] showed that

$$\sum_{\substack{n=1 \\ 2 \nmid n+\overline{n}}}^{p-1} 1 = \frac{1}{2}p + O\left(p^{1/2} \log^2 p\right)$$

Received 31 January 2007.

*Supported by the National Natural Science Foundation of China under Grant No. 60472068 and No. 10671155; Natural Science Foundation of Shaanxi province of China under Grant No. 2006A04; and the Natural Science Foundation of the Education Department of Shaanxi Province of China under Grant No. 06JK168.

by proving the estimate

$$\left|\sum_{n=1}^{p-1}(-1)^{n+\overline{n}}\right| \ll p^{1/2}\log^2 p. \tag{1.1}$$

This means that almost half of the $p-1$ integers $n \in \{1,\dots,p-1\}$ satisfy $\overline{n} \equiv n \pmod 2$ while the other half satisfy $\overline{n} \not\equiv n \pmod 2$. S.R. Louboutin et al. [15] generalized (1.1) to short sums. For details, they proved that

$$\left|\sum_{M\le n\le N}(-1)^{n+\overline{n}}\right| \le \frac{8}{\pi^2}p^{1/2}\log^2(5p)+2, \qquad \text{for} \qquad 1\le M<N<p.$$

This shows that the sequence $\{(-1)^{n+\overline{n}}\}$ forms a "good" pseudorandom binary sequence.

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

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

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 denoted 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 $D=(d_1,\dots,d_k)$ 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, $D=(d_1,\dots,d_k)$ with $1 \le a+jb+d_i \le N (i=1,2,\dots,k)$. In [18] the connection between the measures W and C_2 was studied.

The sequence is considered as a "good" pseudorandom sequence if both $W(E_N)$ and $C_k(E_N)$ (at least for small k) are "small" in terms of N. J. Cassaigne, C. Mauduit and A. Sárközy [6] 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 $N^{\frac{1}{2}}(\log N)^c$. Later a few pseudorandom binary sequences were given and studied (see [4], [5], [8], [9], [11], [12], [13], [14], [16], [17], [19], [21]), and the properties of the pseudorandom measures were also researched in [2] and [3].

Define

$$e_n^{(1)} = \begin{cases} (-1)^{\overline{n}+\overline{n+x}}, & \text{if } p \nmid n(n+x), \\ 1, & \text{otherwise,} \end{cases} \qquad e_n^{(2)} = (-1)^{n+\overline{n}}\left(\frac{n}{p}\right),$$

and

$$E_{p-1}^{(1)} = \left(e_1^{(1)}, \ldots, e_{p-1}^{(1)}\right),\ E_{p-1}^{(2)} = \left(e_1^{(2)}, \ldots, e_{p-1}^{(2)}\right).$$

The first author proved that

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

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

in [12] and [13] respectively. Moreover, suppose that $f(x) \in \mathbb{F}_p[x]$ has degree $(0 <)d(< p)$ and no multiple zero in $\overline{\mathbb{F}}_p$. Let $E_{p-1}^{(3)} = \left(e_1^{(3)}, \ldots, e_{p-1}^{(3)}\right)$ be defined by

$$e_n^{(3)} = \begin{cases} (-1)^{\overline{f(n)}+\overline{f(n+x)}}, & \text{if } p \nmid f(n)f(n+x), \\ 1, & \text{otherwise.} \end{cases}$$

Assume that $k \in \mathbb{N}$ such that $k = 2$ or $(4d)^k < p$. The first author [14] showed that

$$W(E_{p-1}^{(3)}) \ll dp^{1/2}(\log p)^3, \quad C_k(E_{p-1}^{(3)}) \ll kdp^{1/2}(\log p)^{2k+1},$$
$$Q_k(E_{p-1}^{(3)}) \ll kdp^{1/2}(\log p)^{2k+1}.$$

Furthermore, let $f(x) \in \mathbb{F}_p[x]$ of degree d with $1 \le d < p$, and let s be its number of distinct roots in $\overline{\mathbb{F}}_p[x]$. Define

$$e_n = \begin{cases} +1, & \text{if } \overline{f(n)} \equiv R_p(f(n)) (\text{mod } 2), \\ -1, & \text{if } \overline{f(n)} \not\equiv R_p(f(n)) (\text{mod } 2), \end{cases} \tag{1.2}$$

and $E_p = (e_1, \ldots, e_p)$, where $R_p(x)$ denotes the unique $r \in \{0, 1, \ldots, p-1\}$ with $x \equiv r \pmod p$. S.R. Louboutin et al. [15] proved that

$$W(E_p) \ll (d+s)p^{1/2}(\log p)^3, \quad C_2(E_p) \ll (d+s)p^{1/2}(\log p)^5.$$

This shows that $\{e_n\}$ is a "good" pseudorandom binary sequence.

In this paper we shall give a generalization on (1.2) by using Lemma 5 of [19]. Following is the main theorem.

Theorem 1.1. *Let p be an odd prime, $f(x) \in \mathbb{F}_p[x]$ has degree $(0 <)d(< p)$ and no multiple zero in $\overline{\mathbb{F}}_p$. For any $g(x) \in \mathbb{F}_p[x]$, define*

$$e'_n = \begin{cases} +1, & \text{if } \overline{f(n)} \equiv R_p(g(n)) (\mathrm{mod}\ 2), \\ -1, & \text{if } \overline{f(n)} \not\equiv R_p(g(n)) (\mathrm{mod}\ 2), \end{cases} \tag{1.3}$$

and $E'_p = \{e'_1, \ldots, e'_p\}$. Assume that $k \in \mathbb{N}$ with $2 \le k \le p$, and one of the following conditions holds:

$$(i) \quad k = 2; \qquad (ii) \quad (4d)^k < p.$$

Then we have

$$\begin{aligned} W\left(E'_p\right) &\ll (d + \deg g)p^{1/2}(\log p)^3, \\ C_k\left(E'_p\right) &\ll (kd + \deg g)p^{1/2}(\log p)^{2k+1}, \\ Q_k\left(E'_p\right) &\ll (kd + \deg g)p^{1/2}(\log p)^{2k+1}. \end{aligned}$$

There are some generalizations on the problem of D.H. Lehmer. Let $q > 2$ be an odd number, and

$$N(q) = \sum_{\substack{n=1 \\ (n,q)=1 \\ 2 \nmid n+\overline{n}}}^{q} 1.$$

W. Zhang [23] proved that

$$N(q) = \frac{1}{2}\phi(q) + O\left(q^{\frac{1}{2}} d^2(q) \log^2 q\right),$$

where $\phi(q)$ is the Euler function, and $d(q)$ is the divisor function. For any nonnegative integer k, let

$$N(q,k) = \sum_{\substack{n=1 \\ (n,q)=1 \\ 2 \nmid n+\overline{n}}}^{q} (n - \overline{n})^{2k}.$$

W. Zhang [24] gave a sharp asymptotic formula for $N(q,k)$ as following:

$$N(q,k) = \frac{1}{(2k+1)(2k+2)}\phi(q)q^{2k} + O\left(4^k q^{2k+\frac{1}{2}} d^2(q)\log^2 q\right).$$

Moreover, for $0 \le x, y \le 1$, he [24] proved that

$$F_q(x,y) = \sum_{\substack{n\le xq, \overline{n}\le yq \\ (n,q)=1 \\ 2\nmid n+\overline{n}}} 1 = \frac{1}{2}xy\phi(q) + O\left(q^{\frac{1}{2}} d^2(q)\log^2 q\right).$$

C. Cobeli and A. Zaharescu [7] gave a generalization on this problem. For details, let p be a prime, C be an irreducible curve of degree $\le d$ in $\mathbb{A}^r\left(\overline{\mathbb{F}}_p\right)$, defined over $\mathbb{F}_p$ and not contained in any hyperplane. Let $\mathbf{a} = (a_1, \ldots, a_r)$, $\mathbf{b} = (b_1, \ldots, b_r) \in \mathbb{Z}^r$ with $a_1, \ldots, a_r \ge 1$. We say that an $\mathbf{x} = (x_1, \ldots, x_r) \in \mathbb{Z}^r$, with $0 \le x_1, \ldots, x_r < p$, is a Lehmer point with respect to p, r, C, $\mathbf{a}$ and $\mathbf{b}$ if $\mathbf{x} (\mathrm{mod}\ p) \in C$ and $x_j \equiv b_j (\mathrm{mod}\ a_j)$, for $1 \le j \le r$. We denote by $\mathcal{L}(p, r, C, \mathbf{a}, \mathbf{b})$ the set of Lehmer points. For $\mathbf{t} = (t_1, \ldots, t_r)$, $0 \le t_1, \ldots, t_r \le 1$, let

$$F(p, r, C, \mathbf{a}, \mathbf{b}; \mathbf{t}) = \#\left\{\mathbf{x} = (x_1, \ldots, x_r) \in \mathcal{L}(p, r, C, \mathbf{a}, \mathbf{b}) : x_j \le t_j p, 1 \le j \le r\right\}.$$

C. Cobeli and A. Zaharescu showed that

$$F(p, r, C, \mathbf{a}, \mathbf{b}; \mathbf{t}) = \frac{t_1 \cdots t_r}{a_1 \cdots a_r} p + O_{r,d}\left(p^{\frac{1}{2}} \log^r p\right).$$

Furthermore, let $k \ge 1$, $q \ge 2$ be integers and let $a_1, \ldots, a_{k+1} \ge 2$ and $b_1, \ldots, b_{k+1} \ge 0$ with $0 \le b_i < a_i$, for all $i \in \{1, 2, \ldots, k+1\}$, be integers such that $(q, a_1 a_2 \cdots a_{k+1}) = 1$. Denote

$$N(\mathbf{a}, \mathbf{b}; q) = \sum_{\substack{n_1=1 \\ (n_1,q)=1 \\ n_1 \equiv b_1 (\mathrm{mod}\ a_1) \\ \overline{n_1 \cdots n_k} \equiv b_{k+1} (\mathrm{mod}\ a_{k+1})}}^{q-1} \cdots \sum_{\substack{n_k=1 \\ (n_k,q)=1 \\ n_k \equiv b_k (\mathrm{mod}\ a_k)}}^{q-1} 1.$$

E. Alkan, F. Stan and A. Zaharescu [1] showed that

$$N(\mathbf{a}, \mathbf{b}; q) = \frac{\phi^k(q)}{a_1 a_2 \cdots a_{k+1}} + O_{k,\epsilon}\left(q^{k-\frac{1}{2}+\epsilon}\right).$$

Now we give a generalization on the problem of D.H. Lehmer, by using Theorem 1.1. We shall prove the following:

Theorem 1.2. *Define p, $f(x)$, $g(x)$, d and k in the same way as in Theorem* 1.1. *For any integers a, b, $d_1, d_2, \ldots, d_k$ with $0 \le a < b$, $(b, p) = 1$ and $0 \le d_1 < d_2 < \cdots < d_k$, define $D = (d_1, d_2, \ldots, d_k)$, and*

$$N(a, b, D, k, f, g, p) = \sum_{\substack{n=1 \\ n\equiv a(\bmod\ b) \\ p\nmid f(n+d_1)\cdots f(n+d_k) \\ 2\nmid R_p(g(n+d_1))+\overline{f(n+d_1)} \\ \cdots\cdots \\ 2\nmid R_p(g(n+d_k))+\overline{f(n+d_k)}}}^{p} 1. \tag{1.4}$$

Then we have

$$N(a, b, D, k, f, g, p) = \frac{p}{2^k b} + O\left((kd + \deg g)p^{1/2}(\log p)^{2k+1}\right).$$

2 Some Lemmas

To prove the theorems, we need the following lemmas.

Lemma 2.1 ([20]). *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 the polynomial $h(x)$, then we have*

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

Lemma 2.2. *Define p, $f(x)$, d and k in the same way as in Theorem* 1.1. *Then for any integers l, $d_1, \ldots, d_l$, $s_1, \ldots, s_l$ with $1 \le l \le k$, $d_1 < d_2 < \cdots < d_l$ and $(s_1 \cdots s_l, p) = 1$, the polynomial*

$$\Omega(n) := \sum_{i=1}^{l} s_i \prod_{\substack{j=1 \\ j\neq i}}^{l} f(n + d_j)$$

is not constant on $\mathbb{F}_p$.

Proof. This lemma can be easily deduced from Lemma 5 of [19]. □

Lemma 2.3. *Define p, $f(x)$, $g(x)$, d and k in the same way as in Theorem* 1.1. *For any integers a, b, u, $d_1, d_2, \ldots, d_k$, $r_1, \ldots, r_k$, $s_1, \ldots, s_k$ such that $d_1 < d_2 < \cdots < d_k$ and $(br_1 \cdots r_k, p) = 1$, we have*

$$\begin{aligned}\Psi &:= \sum_{\substack{j=0\\ p\nmid f(a+jb+d_1)\cdots f(a+jb+d_k)}}^{p-1} \mathrm{e}\left(\frac{r_1\overline{f(a+jb+d_1)}+\cdots+r_k\overline{f(a+jb+d_k)}}{p}\right)\\ &\quad\times \mathrm{e}\left(\frac{s_1g(a+jb+d_1)+\cdots+s_kg(a+jb+d_k)+uj}{p}\right)\\ &\ll (kd+\deg g)\sqrt{p}.\end{aligned}$$

Proof. From the properties of residue systems we have

$$\begin{aligned}\Psi &= \sum_{\substack{j=0\\ p\nmid f(j+d_1)\cdots f(j+d_k)}}^{p-1} \mathrm{e}\left(\frac{r_1\overline{f(j+d_1)}+\cdots+r_k\overline{f(j+d_k)}}{p}\right)\\ &\quad\times \mathrm{e}\left(\frac{s_1g(j+d_1)+\cdots+s_kg(j+d_k)+u\overline{b}(j-a)}{p}\right).\end{aligned}$$

Define $R(j) = \prod_{t=1}^{k} f(j+d_t)$, and

$$\begin{aligned}Q(j) &= \sum_{i=1}^{k} r_i \prod_{\substack{t=1\\ t\neq i}}^{k} f(j+d_t)\\ &\quad+\big(s_1g(j+d_1)+\cdots+s_kg(j+d_k)+u\overline{b}(j-a)\big)\prod_{t=1}^{k} f(j+d_t).\end{aligned}$$

Therefore

$$\Psi = \sum_{\substack{j\in\mathbb{F}_p\\ R(j)\neq 0}} \mathrm{e}\left(\frac{Q(j)}{R(j)p}\right).$$

If $p \nmid s_1g(j+d_1)+\cdots+s_kg(j+d_k)+u\overline{b}(j-a)$, then $0 < \deg R < \deg Q$ and the rational function Q/R over $\mathbb{F}_p$ is not constant. Then from Lemma 2.1 we have $\Psi \ll (kd+\deg g)\sqrt{p}$.

If $p \mid s_1 g(j+d_1) + \cdots + s_k g(j+d_k) + u\overline{b}(j-a)$, by Lemma 2.2 we know that $Q(j)$ can not be constant on $\mathbb{F}_p$. Then from Lemma 2.1 we get $\Psi \ll kd\sqrt{p}$.

Therefore $\Psi \ll (kd + \deg g)\sqrt{p}$. □

3 Proof of the theorems

First we prove Theorem 1.1. For $1 \le a + tb + d_i \le p$, $i = 1, 2, \ldots, k$, $0 \le d_1 < d_2 < \cdots < d_k$, by (1.3) and the trigonometric identity

$$\sum_{u=1}^{p} \mathrm{e}\left(\frac{un}{p}\right) = \begin{cases} p, & \text{if } p \mid n, \\ 0, & \text{if } p \nmid n. \end{cases} \tag{3.1}$$

we have

$$\begin{aligned}
&\sum_{j=0}^{t} e'_{a+jb+d_1} \cdots e'_{a+jb+d_k} \\
&= \sum_{\substack{j=0 \\ p\nmid f(a+jb+d_1) \\ \cdots \\ f(a+jb+d_k)}}^{t} (-1)^{\overline{f(a+jb+d_1)}+R_p(g(a+jb+d_1))+\cdots+\overline{f(a+jb+d_k)}+R_p(g(a+jb+d_k))} + O(kd) \\
&= \frac{1}{p^{2k+1}} \sum_{\substack{j=0 \\ p\nmid f(a+jb+d_1) \\ \cdots \\ f(a+jb+d_k)}}^{p-1} \sum_{l=0}^{t} \sum_{u=1}^{p} \mathrm{e}\left(\frac{u(j-l)}{p}\right) \sum_{m_1=1}^{p-1} \sum_{r_1=1}^{p} \mathrm{e}\left(\frac{r_1\left(\overline{f(a+jb+d_1)} - m_1\right)}{p}\right) \\
&\quad \times \sum_{n_1=1}^{p} \sum_{s_1=1}^{p} \mathrm{e}\left(\frac{s_1\left(g(a+jb+d_1) - n_1\right)}{p}\right) \cdots \sum_{m_k=1}^{p-1} \sum_{r_k=1}^{p} \mathrm{e}\left(\frac{r_k\left(\overline{f(a+jb+d_k)} - m_k\right)}{p}\right) \\
&\quad \times \sum_{n_k=1}^{p} \sum_{s_k=1}^{p} \mathrm{e}\left(\frac{s_k\left(g(a+jb+d_k) - n_k\right)}{p}\right) (-1)^{m_1+n_1+\cdots+m_k+n_k} + O(kd) \\
&= \frac{1}{p^{2k+1}} \sum_{r_1=1}^{p-1} \left(\sum_{m_1=1}^{p-1} (-1)^{m_1} \mathrm{e}\left(-\frac{m_1 r_1}{p}\right)\right) \sum_{s_1=1}^{p} \left(\sum_{n_1=1}^{p} (-1)^{n_1} \mathrm{e}\left(-\frac{n_1 s_1}{p}\right)\right) \cdots \\
&\quad \times \sum_{r_k=1}^{p-1} \left(\sum_{m_k=1}^{p-1} (-1)^{m_k} \mathrm{e}\left(-\frac{m_k r_k}{p}\right)\right) \sum_{s_k=1}^{p} \left(\sum_{n_k=1}^{p} (-1)^{n_k} \mathrm{e}\left(-\frac{n_k s_k}{p}\right)\right) \sum_{u=1}^{p} \left(\sum_{l=0}^{t} \mathrm{e}\left(-\frac{ul}{p}\right)\right)
\end{aligned}$$

$$\times \sum_{\substack{j=0 \\ p\nmid f(a+jb+d_1) \\ \cdots \\ f(a+jb+d_k)}}^{p-1} \mathrm{e}\left(\frac{r_1\overline{f(a+jb+d_1)}+\cdots+r_k\overline{f(a+jb+d_k)}}{p}\right)$$

$$\times \mathrm{e}\left(\frac{s_1 g(a+jb+d_1)+\cdots+s_k g(a+jb+d_k)+uj}{p}\right)+O(kd).$$

Since

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

$$\sum_{m=1}^{p-1}(-1)^m\mathrm{e}\left(-\frac{mr}{p}\right) \ll \frac{1}{\left|\sin\left(\frac{\pi}{2}-\frac{\pi r}{p}\right)\right|},$$

from Lemma 2.3 we have

$$\begin{aligned}
&\sum_{j=0}^{t} e'_{a+jb+d_1}\cdots e'_{a+jb+d_k}\\
&\ll \frac{t}{p^{2k+1}}\left(\sum_{r=1}^{p-1}\frac{1}{\left|\sin\left(\frac{\pi}{2}-\frac{\pi r}{p}\right)\right|}\right)^k\left(\sum_{s=1}^{p}\frac{1}{\left|\sin\left(\frac{\pi}{2}-\frac{\pi s}{p}\right)\right|}\right)^k (kd+\deg g)\sqrt{p}\\
&\quad+\frac{1}{p^{2k+1}}\left(\sum_{r=1}^{p-1}\frac{1}{\left|\sin\left(\frac{\pi}{2}-\frac{\pi r}{p}\right)\right|}\right)^k\left(\sum_{s=1}^{p}\frac{1}{\left|\sin\left(\frac{\pi}{2}-\frac{\pi s}{p}\right)\right|}\right)^k\left(\sum_{u=1}^{p-1}\frac{1}{\left|\sin\left(\frac{\pi u}{p}\right)\right|}\right)(kd+\deg g)\sqrt{p}\\
&\ll (kd+\deg g)p^{1/2}(\log p)^{2k+1}.
\end{aligned}$$

Therefore

$$\begin{aligned}
Q_k\left(E'_p\right) &= \max_{a,b,t,D}\left|\sum_{j=0}^{t} e'_{a+jb+d_1}\cdots e'_{a+jb+d_k}\right| \\
&\ll (kd+\deg g)p^{1/2}(\log p)^{2k+1}.
\end{aligned} \tag{3.2}$$

Taking $k=1$ and $d_1=0$ in (3.2), we get

$$W\left(E'_p\right)=\max_{a,b,t}\left|\sum_{j=0}^{t-1} e'_{a+jb}\right| \ll (d+\deg g)p^{1/2}(\log p)^3.$$

And taking $a = 0$, $b = 1$, $j = n - 1$ and $t = M - 1$ in (3.2), we immediately have

$$C_k\left(E'_p\right) = \max_{M,D}\left|\sum_{n=1}^{M} e'_{n+d_1}\cdots e'_{n+d_k}\right| \ll (kd + \deg g)\, p^{1/2}(\log p)^{2k+1}.$$

This proves Theorem 1.1.

Now we prove Theorem 1.2. By (1.4) we get

$$N(a,b,D,k,f,g,p) = \sum_{\substack{n=1\\ n\equiv a(\bmod b)\\ p\nmid f(n+d_1)\cdots f(n+d_k)\\ 2\nmid R_p(g(n+d_1))+\overline{f(n+d_1)}\\ \cdots\cdots\\ 2\nmid R_p(g(n+d_k))+\overline{f(n+d_k)}}}^{p} 1$$

$$= \frac{1}{2^k}\sum_{\substack{n=1\\ n\equiv a(\bmod b)\\ p\nmid f(n+d_1)\cdots f(n+d_k)}}^{p}\left(1-(-1)^{R_p(g(n+d_1))+\overline{f(n+d_1)}}\right)\cdots\left(1-(-1)^{R_p(g(n+d_k))+\overline{f(n+d_k)}}\right)$$

$$= \frac{1}{2^k}\sum_{\substack{n=1\\ n\equiv a(\bmod b)\\ p\nmid f(n+d_1)\cdots f(n+d_k)}}^{p} 1 + \frac{1}{2^k}\sum_{l=1}^{k}(-1)^l \sum_{1\le i_1<\cdots<i_l\le k}$$

$$\times \sum_{\substack{n=1\\ n\equiv a(\bmod b)\\ p\nmid f(n+d_1)\cdots f(n+d_k)}}^{p} (-1)^{R_p(g(n+d_{i_1}))+\overline{f(n+d_{i_1})}+\cdots+R_p(g(n+d_{i_l}))+\overline{f(n+d_{i_l})}}.$$

It is easy to show that

$$\frac{1}{2^k}\sum_{\substack{n=1\\ n\equiv a(\bmod b)\\ p\nmid f(n+d_1)\cdots f(n+d_k)}}^{p} 1 = \frac{p}{2^k b} + O(d).$$

On the other hand, by (3.2) we have

$$\sum_{\substack{n=1\\ n\equiv a(\bmod b)\\ p\nmid f(n+d_1)\cdots f(n+d_k)}}^{p} (-1)^{R_p(g(n+d_{i_1}))+\overline{f(n+d_{i_1})}+\cdots+R_p(g(n+d_{i_l}))+\overline{f(n+d_{i_l})}}$$

$$= \sum_{\substack{0\le j\le (p-a)/b \\ p\nmid f(a+jb+d_{i_1})\cdots f(a+jb+d_{i_l})}} (-1)^{R_p(g(n+d_{i_1}))+\overline{f(n+d_{i_1})}+\cdots+R_p(g(n+d_{i_l}))+\overline{f(n+d_{i_l})}} + O(kd)$$

$$= \sum_{0\le j\le (p-a)/b} e'_{a+jb+d_{i_1}}\cdots e'_{a+jb+d_{i_l}} + O(kd)$$

$$\ll (kd+\deg g)p^{1/2}(\log p)^{2k+1}.$$

Therefore

$$N(a,b,D,k,f,g,p) = \frac{p}{2^k b} + O\left((kd+\deg g)p^{1/2}(\log p)^{2k+1}\right).$$

This completes the proof of Theorem 1.2.

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

References

[1] E. Alkan, F. Stan and A. Zaharescu. *Lehmer k-tuples.* Proceedings of the American Mathematical Society, **134** (2006), 2807–2815.

[2] N. Alon, Y. Kohayakawa, C. Mauduit, C.G. Moreira and V. Rödl. *Measures of pseudorandomness for finite sequences: minimal values*. Combinatorics, Probability and Computing, **15** (2006), 1–29.

[3] N. Alon, Y. Kohayakawa, C. Mauduit, C.G. Moreira and V. Rödl. *Measures of pseudorandomness for finite sequences: typical values*. Proceedings of the London Mathematical Society, **95** (2007), 778–812.

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

[5] 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), 343–359.

[6] J. Cassaigne, C. Mauduit and A. Sárközy. *On finite pseudorandom binary sequences VII: the measures of pseudorandomness*. Acta Arithmetica, **103** (2002), 97–108.

[7] C. Cobeli and A. Zaharescu. *Generalization of a problem of Lehmer*. Manuscripta Mathematica, **104** (2001), 301–307.

[8] 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), 425–436.

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

[10] R.K. Guy. *Unsolved problems in number theory*. Springer-Verlag, New York, (1981), 139–140.

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

[12] H. Liu. *New pseudorandom sequences constructed by multiplicative inverse*. Acta Arithmetica, **125** (2006), 11–19.

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

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

[15] S.R. Louboutin, J. Rivat and A. Sárközy. *On a problem of D.H. Lehmer*. Proceedings of the American Mathematical Society, **135** (2007), 969–975.

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

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

[18] C. Mauduit and A. Sárközy. *On the measures of pseudorandomness of binary sequences*. Discrete Mathematics, **271** (2003), 195–207.

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

[20] C.J. Moreno and O. Moreno. *Exponential sums and Goppa codes: I*. Proceedings of the American Mathematical Society, **111** (1991), 523–531.

[21] A. Sárközy. *A finite pseudorandom binary sequence*. Studia Scientiarum Mathematicarum Hungarica, **38** (2001), 377–384.

[22] W. Zhang. *A problem of D.H. Lehmer and its Generalization (I)*. Compositio Mathematica, **86** (1993), 307–316.

[23] W. Zhang. *A problem of D.H. Lehmer and its Generalization (II)*. Compositio Mathematica, **91** (1994), 47–56.

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

Huaning Liu
Department of Mathematics
Northwest University
Xi'an, Shaanxi
P.R. CHINA

E-mail: hnliumath@hotmail.com

Cundian Yang
Department of Mathematics
Shangluo University
Shangluo, Shaanxi
P.R. CHINA

E-mail: slycd@126.com