ACTA ARITHMETICA
130.2 (2007)

A family of pseudorandom binary sequences constructed by the multiplicative inverse

by

Huaning Liu (Xi'an)

1. Introduction. Let p be an odd prime. For each integer a with $t < a \le t+u$ and $(a,p)=1$, there exists one and only one $\overline{a}$ such that $0 < \overline{a} < p$ and $a\overline{a} \equiv 1 \pmod{p}$. Let $r(p,u,t)$ be the number of cases in which a and $\overline{a}$ are of opposite parity, that is

$$r(p,u,t) = \sum_{\substack{t<a\le t+u\\ (a,p)=1\\ 2\nmid a+\overline{a}}} 1.$$

Define

$$E(p,u,t) = r(p,u,t) - \frac{1}{2}\sum_{\substack{t<a\le t+u\\ (a,p)=1}} 1 \quad\text{and}\quad S(p,u) = \sum_{t=1}^{p} |E(p,u,t)|^2.$$

W. Zhang [14] showed that

$$S(p,u) = \frac{1}{4}\,up + O(u^2\sqrt{p}\log^2 p)$$

by proving the estimate

$$\sum_{\substack{n=1\\ p\nmid n+x}}^{p-1} (-1)^{\overline{n}+\overline{n+x}} \ll \sqrt{p}\log^2 p.$$

Therefore it is natural to expect that the sequence $\{(-1)^{\overline{n}+\overline{n+x}}\}$ behaves like a random sequence of $\pm$ signs.

2000 *Mathematics Subject Classification*: Primary 11K45.

Key words and phrases: pseudorandom binary sequence, multiplicative inverse, exponential sum.

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.

 © Instytut Matematyczny PAN, 2007

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

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

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

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

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,

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

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 [10] the connection between the measures W and C_2 was studied.

The sequence E_N is considered to be 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. Later J. Cassaigne, C. Mauduit and A. 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 $N^{1/2} \log^c N$.

It was shown in [9] that the Legendre symbol forms a good pseudorandom sequence. In [1] and [2], J. Cassaigne and coauthors studied the pseudorandomness of the Liouville function, defined as $\lambda(n) = (-1)^{\Omega(n)}$ ($\Omega(n) =$ the number of prime factors of n counted with multiplicity) and also of $\gamma(n) = (-1)^{\omega(n)}$ ($\omega(n) =$ the number of distinct prime factors of n). Moreover, let

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

denote the Kloosterman sums, where $e(y) = e^{2\pi i y}$, p is a prime, and $\overline{a}$ is the multiplicative inverse of a modulo p such that $1 \le \overline{a} \le p-1$. E. Fouvry (with coauthors) [4] showed that the signs of $K(1, n; p)$ form a good pseudorandom binary sequence.

Furthermore, let p be an odd prime, and g a primitive root modulo p. Define $\operatorname{ind} n$ by $1 \le \operatorname{ind} n \le p-1$ and $n \equiv g^{\operatorname{ind} n} \pmod p$. Write $N = p-1$ and define the sequence $E_N = \{e_1, \dots, e_N\}$ by

$$e_n = \begin{cases} +1 & \text{if } 1 \le \operatorname{ind} n \le (p-1)/2, \\ -1 & \text{if } (p+1)/2 \le \operatorname{ind} n \le p-1. \end{cases}$$

A. Sárközy [13] showed that E_N is also a good pseudorandom binary sequence.

However, the above constructions produce only a few good sequences while in certain applications (e.g., in cryptography) one needs large families of good pseudorandom binary sequence. Therefore some large families of pseudorandom binary sequences were introduced in [5], [6], [8] and [11].

As was said in [9], the analysis of the known constructions leads to the conclusion that, although the new constructions are superior to the previous ones from many points of view, there is a price paid for this so that there is no perfect construction. Thus the selection of the construction method to be applied must depend on the application in mind; the construction which is superior in a certain situation may fail in another one. This also means that the search for new approaches and new constructions should be continued.

Let p be an odd prime. 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 $1 \le x \le p-1$. Let $E'_{p-1} = \{e'_1, \dots, e'_{p-1}\}$ be defined by (1.1). In [7] we proved that

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

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

However, it is usually not enough to control correlations of order 2 to ensure the pseudorandom behavior of a sequence, in particular in the case of applications to cryptography. Therefore in the report for our paper [7] the referee suggested completing that study by showing analogous results for correlations of larger order, C_k and Q_k for $k > 2$. Moreover, he/she suggested completing that work by studying the measure of pseudorandomness for the more general construction obtained by

$$e''_n = \begin{cases} (-1)^{\overline{f(n)}+\overline{f(n+x)}} & \text{if } p \nmid f(n) \text{ and } p \nmid f(n+x), \\ 1 & \text{otherwise}, \end{cases} \tag{1.2}$$

where f is a suitable polynomial over $\mathbb{F}_p$.

In this paper, we realize the referee's suggestions. The main results are the following.

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*

$$C_k(E'_{p-1}) \ll kp^{1/2} \log^{2k+1} p, \qquad Q_k(E'_{p-1}) \ll kp^{1/2} \log^{2k+1} p.$$

THEOREM 1.2. *Let p be an odd prime, and let $f(x) \in \mathbb{F}_p[x]$ have degree d with $0 < d < p$ and no multiple zero in $\overline{\mathbb{F}}_p$. Let $E''_{p-1} = \{e''_1, \ldots, e''_{p-1}\}$ be defined by* (1.2). *Assume that $k \in \mathbb{N}$ with $2 \le k \le p$, and one of the following conditions holds*:

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

Then

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

REMARK. Since there is a very good (polynomial time) algorithm for computing the multiplicative inverse modulo p, these two sequences can be generated fast.

2. Some lemmas. To prove the theorems, we need the following lemmas.

LEMMA 2.1 ([12]). *Let $g(x), h(x) \in \mathbb{F}_p[x]$ be such that the rational function $f(x) = g(x)/h(x)$ is not constant on $\mathbb{F}_p$, and let s be the number of distinct roots of $h(x)$. Then*

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

LEMMA 2.2. *For any integers $s_1, \ldots, s_l$, $d_1, \ldots, d_l$ with $(s_1 \cdots s_l, p) = 1$ and $d_1 < \cdots < d_l$, the polynomial*

$$\Omega_1(n) := \sum_{i=1}^{l} s_i \prod_{\substack{j=1 \\ j \neq i}}^{l} (n + d_j)$$

is not the zero polynomial on $\mathbb{F}_p$.

Proof. Suppose that $\Omega_1(n) \equiv 0 \pmod p$. Then the coefficients of $n^{l-1}, \dots, n, n^0$ must be congruent to 0 modulo p. So we have

$$\sum_{j=1}^{l} s_j \Big(\sum_{\substack{1 \le i_1 < \cdots < i_k \le l \\ i_1, \dots, i_k \ne j}} d_{i_1} \cdots d_{i_k} \Big) \equiv 0 \pmod p, \qquad k = 0, 1, \dots, l-1. \tag{2.1}$$

This gives

$$\sum_{j=1}^{l} s_j \Big(\sum_{m=1}^{k+1} (-1)^{m-1} d_j^{m-1} \sum_{\substack{1 \le i_m < \cdots < i_k \le l \\ m \le k}} d_{i_m} \cdots d_{i_k} \Big) \equiv 0 \pmod p, \quad k = 0, 1, \dots, l-1. \tag{2.2}$$

Substitute the kth equation into the $(k+1)$st equation for $k = 0, 1, \dots, l-2$. Then we have

$$\begin{cases} s_1 + s_2 + \cdots + s_l \equiv 0 \pmod p, \\ s_1 d_1 + s_2 d_2 + \cdots + s_l d_l \equiv 0 \pmod p, \\ s_1 d_1^2 + s_2 d_2^2 + \cdots + s_l d_l^2 \equiv 0 \pmod p, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ s_1 d_1^{l-2} + s_2 d_2^{l-2} + \cdots + s_l d_l^{l-2} \equiv 0 \pmod p, \\ s_1 d_1^{l-1} + s_2 d_2^{l-1} + \cdots + s_l d_l^{l-1} \equiv 0 \pmod p. \end{cases} \tag{2.3}$$

That is,

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ d_1 & d_2 & \cdots & d_l \\ \vdots & \vdots & & \vdots \\ d_1^{l-1} & d_2^{l-1} & \cdots & d_l^{l-1} \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_l \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \pmod p. \tag{2.4}$$

Since

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ d_1 & d_2 & \cdots & d_l \\ \vdots & \vdots & & \vdots \\ d_1^{l-1} & d_2^{l-1} & \cdots & d_l^{l-1} \end{vmatrix} = \prod_{1 \le j < i \le l} (d_i - d_j) \ne 0,$$

(2.1) has one and only one solution

$$\begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_l \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \pmod p,$$

which is impossible. This shows that $\Omega_1(n)$ is not the zero polynomial on $\mathbb{F}_p$. ∎

LEMMA 2.3. *For any integers* a, b, u, x, $d_1,\dots,d_k$, $r_1,\dots,r_k$, $s_1,\dots,s_k$ *such that* $d_1<\dots<d_k$ *and* $(bxr_1\cdots r_ks_1\cdots s_k,p)=1$,

$$\Psi_1 := \sum_{\substack{j=0\\ p\nmid(a+jb+d_1)\cdots(a+jb+d_k)\\ p\nmid(a+jb+d_1+x)\cdots(a+jb+d_k+x)}}^{p-1} e\left(\frac{r_1\overline{a+jb+d_1}+\dots+r_k\overline{a+jb+d_k}}{p}\right) \times e\left(\frac{s_1\overline{a+jb+d_1+x}+\dots+s_k\overline{a+jb+d_k+x}+uj}{p}\right)$$

$$\ll k\sqrt{p}.$$

Proof. From the properties of residue systems we have

$$\Psi_1 = \sum_{\substack{j=0\\ p\nmid(j+d_1)\cdots(j+d_k)\\ p\nmid(j+d_1+x)\cdots(j+d_k+x)}}^{p-1} e\left(\frac{r_1\overline{j+d_1}+\dots+r_k\overline{j+d_k}}{p}\right) \times e\left(\frac{s_1\overline{j+d_1+x}+\dots+s_k\overline{j+d_k+x}+u\overline{b}(j-a)}{p}\right).$$

If $p\nmid u$, define

$$H_1(j)=(j+d_1)\cdots(j+d_k)(j+d_1+x)\cdots(j+d_k+x)$$

and

$$\begin{aligned}G_1(j) = {}& r_1(j+d_2)\cdots(j+d_k)(j+d_1+x)\cdots(j+d_k+x)+\cdots\\ &+r_k(j+d_1)\cdots(j+d_{k-1})(j+d_1+x)\cdots(j+d_k+x)\\ &+s_1(j+d_1)\cdots(j+d_k)(j+d_2+x)\cdots(j+d_k+x)+\cdots\\ &+s_k(j+d_1)\cdots(j+d_k)(j+d_1+x)\cdots(j+d_{k-1}+x)\\ &+u\overline{b}(j-a)(j+d_1)\cdots(j+d_k)(j+d_1+x)\cdots(j+d_k+x).\end{aligned}$$

The function $G_1(j)$ cannot be constant over $\mathbb{F}_p$ since the coefficient of j^{2k+1} is $u\overline{b}$. Thus by Lemma 2.1 we have $\Psi_1 \ll k\sqrt{p}$.

For $p\mid u$, we have

$$\Psi_1 = \sum_{\substack{j=0\\ p\nmid(j+d_1)\cdots(j+d_k)\\ p\nmid(j+d_1+x)\cdots(j+d_k+x)}}^{p-1} e\left(\frac{r_1\overline{j+d_1}+\dots+r_k\overline{j+d_k}}{p}\right) \times e\left(\frac{s_1\overline{j+d_1+x}+\dots+s_k\overline{j+d_k+x}}{p}\right).$$

Defining

$$F_1(j)=r_1\overline{j+d_1}+\dots+r_k\overline{j+d_k}+s_1\overline{j+d_1+x}+\dots+s_k\overline{j+d_k+x},$$

and $d_{k+1} = d_1 + x, \ldots, d_{2k} = d_k + x$, $r_{k+1} = s_1, \ldots, r_{2k} = s_k$, we get

$$F_1(j) = r_1\overline{j + d_1} + \cdots + r_{2k}\overline{j + d_{2k}}.$$

If there are some n, m with $n < m$ and $d_n = d_m$, then

$$\begin{aligned} F_1(j) = r_1\overline{j + d_1} + \cdots + r_{n-1}\overline{j + d_{n-1}} + (r_n + r_m)\overline{j + d_n} + r_{n+1}\overline{j + d_{n+1}} \\ + \cdots + r_{m-1}\overline{j + d_{m-1}} + r_{m+1}\overline{j + d_{m+1}} + \cdots + r_{2k}\overline{j + d_{2k}}. \end{aligned}$$

If $p \mid r_n + r_m$, we define

$$\begin{aligned} F_1'(j) = r_1\overline{j + d_1} + \cdots + r_{n-1}\overline{j + d_{n-1}} + r_{n+1}\overline{j + d_{n+1}} + \cdots \\ + r_{m-1}\overline{j + d_{m-1}} + r_{m+1}\overline{j + d_{m+1}} + \cdots + r_{2k}\overline{j + d_{2k}}, \end{aligned}$$

hence $F_1(j) \equiv F_1'(j) \pmod{p}$. If $p \nmid r_n + r_m$, then set $F_1'(j) = F_1(j)$.

For $F_1'(j)$, if there still exist some n', m' such that $n' < m'$ and $d_{n'} = d_{m'}$, then we continue the above process. Since $d_1 < \cdots < d_k$, $d_{k+1} < \cdots < d_{2k}$ and $d_1 < d_{k+1}$, we finally get some

$$F_1^*(j) = t_1\overline{j + c_1} + t_2\overline{j + c_2} + \cdots + t_l\overline{j + c_l}$$

with $(t_1 \cdots t_l, p) = 1$, $c_1 < \cdots < c_l$ and $F_1(j) \equiv F_1^*(j) \pmod{p}$. Therefore

$$\Psi_1 = \sum_{\substack{j=0 \\ p\nmid(j+c_1)\cdots(j+c_l)}}^{p-1} e\biggl(\frac{F_1^*(j)}{p}\biggr).$$

Now defining

$$H_1^*(n) = (n + c_1) \cdots (n + c_l) \quad \text{and} \quad G_1^*(n) = \sum_{i=1}^{l} t_i \prod_{\substack{j=1 \\ j\neq i}}^{l} (n + c_j),$$

we have

$$\Psi_1 = \sum_{\substack{n\in\mathbb{F}_p \\ H_1^*(n)\neq 0}} e\biggl(\frac{G_1^*(n)}{H_1^*(n)p}\biggr).$$

By Lemma 2.2 we know that $G_1^*(n)$ is not the zero polynomial on $\mathbb{F}_p$. Note that $\deg(G_1^*) < \deg(H_1^*)$, so $G_1^*(n)/H_1^*(n)$ is not constant on $\mathbb{F}_p$. Then from Lemma 2.1 we also have $\Psi_1 \ll l\sqrt{p} \ll k\sqrt{p}$. ∎

LEMMA 2.4. *Define* p, $f(x)$, d *and* k *as in Theorem* 1.2. *Then for any integers* $l, d_1, \ldots, d_l, s_1, \ldots, s_l$ *with* $1 \le l \le k$, $d_1 < \cdots < d_l$ *and* $(s_1 \cdots s_l, p) = 1$, *the polynomial*

$$\Omega_2(n) := \sum_{i=1}^{l} s_i \prod_{\substack{j=1 \\ j\neq i}}^{l} f(n + d_j)$$

is not the zero polynomial on $\mathbb{F}_p$.

Proof. This lemma can be easily deduced from Lemma 5 of [11]. ∎

LEMMA 2.5. *Define p, $f(x)$, d and k as in Theorem 1.2. For any integers a, b, u, x, $d_1,\ldots,d_k$, $r_1,\ldots,r_k$, $s_1,\ldots,s_k$ such that $d_1<\cdots<d_k$ and $(bxr_1\cdots r_k s_1\cdots s_k,p)=1$, we have*

$$\Psi_2 := \sum_{\substack{j=0\\ p\nmid f(a+jb+d_1)\cdots f(a+jb+d_k)\\ p\nmid f(a+jb+d_1+x)\cdots f(a+jb+d_k+x)}}^{p-1} e\biggl(\frac{r_1\overline{f(a+jb+d_1)}+\cdots+r_k\overline{f(a+jb+d_k)}}{p}\biggr) \times e\biggl(\frac{s_1\overline{f(a+jb+d_1+x)}+\cdots+s_k\overline{f(a+jb+d_k+x)}+uj}{p}\biggr) \ll kd\sqrt{p}.$$

Proof. From the properties of residue systems we have

$$\Psi_2 = \sum_{\substack{j=0\\ p\nmid f(j+d_1)\cdots f(j+d_k)\\ p\nmid f(j+d_1+x)\cdots f(j+d_k+x)}}^{p-1} e\biggl(\frac{r_1\overline{f(j+d_1)}+\cdots+r_k\overline{f(j+d_k)}}{p}\biggr) \times e\biggl(\frac{s_1\overline{f(j+d_1+x)}+\cdots+s_k\overline{f(j+d_k+x)}+u\overline{b}(j-a)}{p}\biggr).$$

If $p\nmid u$, define

$$H_2(j)=f(j+d_1)\cdots f(j+d_k)f(j+d_1+x)\cdots f(j+d_k+x)$$

and

$$\begin{aligned} G_2(j) = {} & r_1f(j+d_2)\cdots f(j+d_k)f(j+d_1+x)\cdots f(j+d_k+x)+\cdots\\ &+r_kf(j+d_1)\cdots f(j+d_{k-1})f(j+d_1+x)\cdots f(j+d_k+x)\\ &+s_1f(j+d_1)\cdots f(j+d_k)f(j+d_2+x)\cdots f(j+d_k+x)+\cdots\\ &+s_kf(j+d_1)\cdots f(j+d_k)f(j+d_1+x)\cdots f(j+d_{k-1}+x)\\ &+u\overline{b}(j-a)f(j+d_1)\cdots f(j+d_k)f(j+d_1+x)\cdots f(j+d_k+x). \end{aligned}$$

The function $G_2(j)$ cannot be constant over $\mathbb{F}_p$ since $p\nmid u\overline{b}$. Thus by Lemma 2.1 we have $\Psi_2\ll kd\sqrt{p}$.

For $p\mid u$, we have

$$\Psi_2 = \sum_{\substack{j=0\\ p\nmid f(j+d_1)\cdots f(j+d_k)\\ p\nmid f(j+d_1+x)\cdots f(j+d_k+x)}}^{p-1} e\biggl(\frac{r_1\overline{f(j+d_1)}+\cdots+r_k\overline{f(j+d_k)}}{p}\biggr) \times e\biggl(\frac{s_1\overline{f(j+d_1+x)}+\cdots+s_k\overline{f(j+d_k+x)}}{p}\biggr).$$

Defining

$$F_2(j)=r_1\overline{f(j+d_1)}+\cdots+r_k\overline{f(j+d_k)}+s_1\overline{f(j+d_1+x)}+\cdots+s_k\overline{f(j+d_k+x)},$$

and $d_{k+1} = d_1 + x, \ldots, d_{2k} = d_k + x$, $r_{k+1} = s_1, \ldots, r_{2k} = s_k$, we get

$$F_2(j) = r_1\overline{f(j+d_1)} + \cdots + r_{2k}\overline{f(j+d_{2k})}.$$

If there are some n, m with $n < m$ and $d_n = d_m$, then

$$\begin{aligned} F_2(j) = r_1\overline{f(j+d_1)} + \cdots + r_{n-1}\overline{f(j+d_{n-1})} + (r_n + r_m)\overline{f(j+d_n)} \\ + r_{n+1}\overline{f(j+d_{n+1})} + \cdots + r_{m-1}\overline{f(j+d_{m-1})} \\ + r_{m+1}\overline{f(j+d_{m+1})} + \cdots + r_{2k}\overline{f(j+d_{2k})}. \end{aligned}$$

If $p \mid r_n + r_m$, we define

$$\begin{aligned} F_2'(j) = r_1\overline{f(j+d_1)} + \cdots + r_{n-1}\overline{f(j+d_{n-1})} + r_{n+1}\overline{f(j+d_{n+1})} + \cdots \\ + r_{m-1}\overline{f(j+d_{m-1})} + r_{m+1}\overline{f(j+d_{m+1})} + \cdots + r_{2k}\overline{f(j+d_{2k})}, \end{aligned}$$

hence $F_2(j) \equiv F_2'(j) \pmod p$. If $p \nmid r_n + r_m$, then set $F_2'(j) = F_2(j)$.

For $F_2'(j)$, if there still exist some n', m' such that $n' < m'$ and $d_{n'} = d_{m'}$, then we continue the above process. Since $d_1 < \cdots < d_k$, $d_{k+1} < \cdots < d_{2k}$ and $d_1 < d_{k+1}$, we finally get some

$$F_2^*(j) = t_1\overline{f(j+c_1)} + t_2\overline{f(j+c_2)} + \cdots + t_l\overline{f(j+c_l)}$$

with $(t_1 \cdots t_l, p) = 1$, $c_1 < \cdots < c_l$ and $F_2(j) \equiv F_2^*(j) \pmod p$. Therefore

$$\Psi_2 = \sum_{\substack{j=0 \\ p\nmid (j+c_1)\cdots(j+c_l)}}^{p-1} e\left(\frac{F_2^*(j)}{p}\right).$$

Now defining

$$H_2^*(n) = f(n+c_1)\cdots f(n+c_l) \quad \text{and} \quad G_2^*(n) = \sum_{i=1}^{l} t_i \prod_{\substack{j=1 \\ j\neq i}}^{l} f(n+c_j),$$

we have

$$\Psi_2 = \sum_{\substack{n\in\mathbb{F}_p \\ H_2^*(n)\neq 0}} e\left(\frac{G_2^*(n)}{H_2^*(n)p}\right).$$

By Lemma 2.4 we know that $G_2^*(n)$ is not the zero polynomial on $\mathbb{F}_p$. Note that $\deg(G_2^*) < \deg(H_2^*)$, so $G_2^*(n)/H_2^*(n)$ is not constant on $\mathbb{F}_p$. Then from Lemma 2.1 we also have $\Psi_2 \ll ld\sqrt{p} \ll kd\sqrt{p}$. ∎

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

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

we have

$$\sum_{j=0}^{t} e'_{a+jb+d_1}\cdots e'_{a+jb+d_k}$$

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

$$+ O(k)$$

$$= \frac{1}{p^{2k+1}} \sum_{\substack{j=0\\ p\nmid(a+jb+d_1)\cdots(a+jb+d_k)\\ p\nmid(a+jb+d_1+x)\cdots(a+jb+d_k+x)}}^{p-1} \sum_{l=0}^{t}\sum_{u=1}^{p} e\left(\frac{u(j-l)}{p}\right)$$

$$\times \sum_{m_1=1}^{p-1}\sum_{r_1=1}^{p} e\left(\frac{r_1(\overline{a+jb+d_1}-m_1)}{p}\right)\sum_{n_1=1}^{p-1}\sum_{s_1=1}^{p} e\left(\frac{s_1(\overline{a+jb+d_1+x}-n_1)}{p}\right)$$

$$\times\cdots\times \sum_{m_k=1}^{p-1}\sum_{r_k=1}^{p} e\left(\frac{r_k(\overline{a+jb+d_k}-m_k)}{p}\right)$$

$$\times \sum_{n_k=1}^{p-1}\sum_{s_k=1}^{p} e\left(\frac{s_k(\overline{a+jb+d_k+x}-n_k)}{p}\right)(-1)^{m_1+n_1+\cdots+m_k+n_k} + O(k)$$

$$= \frac{1}{p^{2k+1}} \sum_{r_1=1}^{p-1}\left(\sum_{m_1=1}^{p-1}(-1)^{m_1} e\left(-\frac{m_1 r_1}{p}\right)\right)\sum_{s_1=1}^{p-1}\left(\sum_{n_1=1}^{p-1}(-1)^{n_1} e\left(-\frac{n_1 s_1}{p}\right)\right)$$

$$\times\cdots\times \sum_{r_k=1}^{p-1}\left(\sum_{m_k=1}^{p-1}(-1)^{m_k} e\left(-\frac{m_k r_k}{p}\right)\right)\sum_{s_k=1}^{p-1}\left(\sum_{n_k=1}^{p-1}(-1)^{n_k} e\left(-\frac{n_k s_k}{p}\right)\right)$$

$$\times \sum_{u=1}^{p}\left(\sum_{l=0}^{t} e\left(-\frac{ul}{p}\right)\right)$$

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

$$\times e\left(\frac{s_1\overline{a+jb+d_1+x}+\cdots+s_k\overline{a+jb+d_k+x}+uj}{p}\right)$$

$$+ O(k).$$

Since

$$(3.2)\qquad \begin{aligned} &\sum_{l=0}^{t} e\Big(-\frac{ul}{p}\Big) \ll \frac{1}{|\sin(\pi u/p)|} \quad \text{for } p\nmid u,\\ &\sum_{m=1}^{p-1}(-1)^m e\Big(-\frac{rm}{p}\Big) \ll \frac{1}{|\sin(\pi/2-\pi r/p)|},\end{aligned}$$

from Lemma 2.3 we have

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

Therefore

$$(3.3)\quad Q_k(E'_{p-1}) = \max_{a,b,t,D}\bigg|\sum_{j=0}^{t} e'_{a+jb+d_1}\cdots e'_{a+jb+d_k}\bigg| \ll kp^{1/2}\log^{2k+1} p.$$

Taking $a=0$, $b=1$, $j=n-1$ and $t=M-1$ in (3.3), we immediately get

$$C_k(E'_{p-1}) = \max_{M,D}\bigg|\sum_{n=1}^{M} e'_{n+d_1}\cdots e'_{n+d_k}\bigg| \ll kp^{1/2}\log^{2k+1} p.$$

This proves Theorem 1.1.

Now we prove Theorem 1.2. For $1\le a+tb+d_i\le p-1$, $i=1,\dots,k$, $0\le d_1<\dots<d_k$, by (1.2) and (3.1) we have

$$\begin{aligned}&\sum_{j=0}^{t} e''_{a+jb+d_1}\cdots e''_{a+jb+d_k}\\ &= \sum_{\substack{j=0\\ p\nmid f(a+jb+d_1)\cdots f(a+jb+d_k)\\ p\nmid f(a+jb+d_1+x)\cdots f(a+jb+d_k+x)}}^{t} (-1)^{\overline{f(a+jb+d_1)}+\overline{f(a+jb+d_1+x)}+\cdots+\overline{f(a+jb+d_k)}}\\ &\quad\times(-1)^{\overline{f(a+jb+d_k+x)}} + O(kd)\\ &= \frac{1}{p^{2k+1}} \sum_{\substack{j=0\\ p\nmid f(a+jb+d_1)\cdots f(a+jb+d_k)\\ p\nmid f(a+jb+d_1+x)\cdots f(a+jb+d_k+x)}}^{p-1} \sum_{l=0}^{t}\sum_{u=1}^{p} e\Big(\frac{u(j-l)}{p}\Big)\end{aligned}$$

$$\times \sum_{m_1=1}^{p-1} \sum_{r_1=1}^{p} e\left(\frac{r_1(\overline{f(a+jb+d_1)}-m_1)}{p}\right)$$

$$\times \sum_{n_1=1}^{p-1} \sum_{s_1=1}^{p} e\left(\frac{s_1(\overline{f(a+jb+d_1+x)}-n_1)}{p}\right)$$

$$\times \cdots \times \sum_{m_k=1}^{p-1} \sum_{r_k=1}^{p} e\left(\frac{r_k(\overline{f(a+jb+d_k)}-m_k)}{p}\right)$$

$$\times \sum_{n_k=1}^{p-1} \sum_{s_k=1}^{p} e\left(\frac{s_k(\overline{f(a+jb+d_k+x)}-n_k)}{p}\right)(-1)^{m_1+n_1+\cdots+m_k+n_k}$$

$$+ O(kd)$$

$$= \frac{1}{p^{2k+1}} \sum_{r_1=1}^{p-1} \left(\sum_{m_1=1}^{p-1} (-1)^{m_1} e\left(-\frac{m_1 r_1}{p}\right)\right) \sum_{s_1=1}^{p-1} \left(\sum_{n_1=1}^{p-1} (-1)^{n_1} e\left(-\frac{n_1 s_1}{p}\right)\right)$$

$$\times \cdots \times \sum_{r_k=1}^{p-1} \left(\sum_{m_k=1}^{p-1} (-1)^{m_k} e\left(-\frac{m_k r_k}{p}\right)\right) \sum_{s_k=1}^{p-1} \left(\sum_{n_k=1}^{p-1} (-1)^{n_k} e\left(-\frac{n_k s_k}{p}\right)\right)$$

$$\times \sum_{u=1}^{p} \left(\sum_{l=0}^{t} e\left(-\frac{ul}{p}\right)\right)$$

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

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

Then from (3.2) and Lemma 2.5 we get

$$\sum_{j=0}^{t} e''_{a+jb+d_1} \cdots e''_{a+jb+d_k} \ll \frac{t}{p^{2k+1}} \left(\sum_{r=1}^{p-1} \frac{1}{|\sin(\pi/2-\pi r/p)|}\right)^{2k} \cdot kd\sqrt{p}$$

$$+ \frac{1}{p^{2k+1}} \left(\sum_{r=1}^{p-1} \frac{1}{|\sin(\pi/2-\pi r/p)|}\right)^{2k} \left(\sum_{u=1}^{p-1} \frac{1}{|\sin(\pi u/p)|}\right) \cdot kd\sqrt{p}$$

$$\ll kdp^{1/2} \log^{2k+1} p.$$

Therefore

$$(3.4)\qquad Q_k(E''_{p-1}) = \max_{a,b,t,D}\Big|\sum_{j=0}^{t} e''_{a+jb+d_1}\cdots e''_{a+jb+d_k}\Big| \ll kdp^{1/2}\log^{2k+1} p.$$

Taking $k=1$ and $d_1=0$ in (3.4), we have

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

And taking $a=0$, $b=1$, $j=n-1$ and $t=M-1$ in (3.4), we immediately get

$$C_k(E''_{p-1}) = \max_{M,D}\Big|\sum_{n=1}^{M} e''_{n+d_1}\cdots e''_{n+d_k}\Big| \ll kdp^{1/2}\log^{2k+1} p.$$

This completes the proof of Theorem 1.2.

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

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), 343–359.

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

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

[6] K. Gyarmati, *On a family of pseudorandom binary sequences*, Period. Math. Hungar. 49 (2004), 45–63.

[7] H. N. Liu, *New pseudorandom sequences constructed using multiplicative inverses*, Acta Arith. 125 (2006), 11–19.

[8] C. Mauduit, J. Rivat and A. Sárközy, *Construction of pseudorandom binary sequences using additive characters*, Monatsh. Math. 141 (2004), 197–208.

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

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

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

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

[13] A. Sárközy, *A finite pseudorandom binary sequence*, Studia Sci. Math. Hungar. 38 (2001), 377–384.
[14] W. Zhang, *On a problem of P. Gallagher*, Acta Math. Hungar. 78 (1998), 345–357.

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

Received on 24.11.2006
and in revised form on 19.3.2007 (5329)