PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 137, Number 3, March 2009, Pages 793–803
S 0002-9939(08)09706-2
Article electronically published on October 29, 2008

A LARGE FAMILY OF PSEUDORANDOM BINARY LATTICES

HUANING LIU

(Communicated by Wen-Ching Winnie Li)

Abstract. Recently P. Hubert, C. Mauduit and A. Sárközy introduced and studied the notion of pseudorandomness of binary lattices and gave a pseudorandom binary lattice. Later in other papers C. Mauduit and A. Sárközy constructed some large families of "good" binary lattices. In this paper a large family of pseudorandom binary lattices is presented by using the multiplicative inverse and the quadratic character of finite fields.

1. Introduction and results

Pseudorandom binary sequences play an important role in cryptography, so in a series of papers a new constructive approach has been developed to study the pseudorandomness of the binary sequences

$$E_N = (e_1, e_2, \cdots, e_N) \in \{-1, +1\}^N .$$

Measures of pseudorandomness were introduced by C. Mauduit and A. Sárközy [17], and properties of the measures have been studied in [1], [2] and [18]. Later many pseudorandom binary sequences were given and studied (see [3], [4], [6], [7], [8], [9], [11], [12], [13], [15], [16], [19], and [23]). For example, let p be an odd prime, $e_n^{(1)} = \left(\frac{n}{p}\right)$, and $E_{p-1}^{(1)} = \left(e_1^{(1)}, e_2^{(1)}, \cdots, e_{p-1}^{(1)}\right)$. C. Mauduit and A. Sárközy [17] proved that $E_{p-1}^{(1)}$ forms a good pseudorandom binary sequence. Let $\overline{n}$ be the multiplicative inverse of n modulo p such that $1 \le \overline{n} \le p-1$ and $n\overline{n} \equiv 1 (\mathrm{mod} p)$. Denote $e_n^{(2)} = (-1)^{n+\overline{n}} \left(\frac{n}{p}\right)$ and $E_{p-1}^{(2)} = \left(e_1^{(2)}, e_2^{(2)}, \cdots, e_{p-1}^{(2)}\right)$. The author [12] studied the pseudorandomness of $E_{p-1}^{(2)}$. Moreover, let $f(x), g(x) \in \mathbb{F}_p[x]$, and

$$e_n^{(3)} = \begin{cases} \left(\frac{f(n)}{p}\right), & \text{if } (f(n), p) = 1, \\ +1, & \text{if } p \mid f(n), \end{cases}$$

$$e_n^{(4)} = \begin{cases} (-1)^{R_p(f(n)) + \overline{f(n)}}, & \text{if } (f(n), p) = 1, \\ +1, & \text{if } p \mid f(n), \end{cases}$$

Received by the editors November 28, 2007.
2000 *Mathematics Subject Classification.* Primary 11K45.
Key words and phrases. Pseudorandom binary lattice, quadratic character, multiplicative inverse.
This research was supported by the National Grand Fundamental Research 973 Programs of China under Grants 2007CB807902 and 2007CB807903.

$$e_n^{(5)} = \begin{cases} (-1)^{R_p(g(n))+\overline{f(n)}}, & \text{if } (f(n),p)=1, \\ +1, & \text{if } p \mid f(n), \end{cases}$$

where $R_p(x)$ denotes the unique $r \in \{0,1,\cdots,p-1\}$ with $x \equiv r(\mathrm{mod} p)$. Define

$$E_p^{(3)} = \left(e_1^{(3)}, e_2^{(3)}, \cdots, e_p^{(3)}\right),$$
$$E_p^{(4)} = \left(e_1^{(4)}, e_2^{(4)}, \cdots, e_p^{(4)}\right),$$
$$E_p^{(5)} = \left(e_1^{(5)}, e_2^{(5)}, \cdots, e_p^{(5)}\right).$$

The pseudorandomness of $E_p^{(3)}$, $E_p^{(4)}$ and $E_p^{(5)}$ was studied in [7], [15] and [14], respectively.

P. Hubert, C. Mauduit and A. Sárközy [10] extended this constructive theory of pseudorandomness to several dimensions. Let I_N^n denote the set of the n-dimensional vectors all of whose coordinates are selected from the set $\{0,1,\cdots,N-1\}$:

$$I_N^n = \{\mathbf{x} = (x_1,\cdots,x_n) : x_1,\cdots,x_n \in \{0,1,\cdots,N-1\}\}.$$

A function of the type $\eta(\mathbf{x}) : I_N^n \to \{-1,+1\}$ is called an n-dimensional binary N-lattice or briefly a binary lattice. If $k \in \mathbb{N}$, and $\mathbf{u}_i$ $(i = 1,\cdots,n)$ denotes the n-dimensional unit vector whose i-th coordinate is 1 and the other coordinates are 0, then write

$$\mathbb{Q}_k(\eta) = \max_{\mathbf{B},\mathbf{d}_1,\cdots,\mathbf{d}_k,\mathbf{T}} \left| \sum_{j_1=0}^{t_1} \cdots \sum_{j_n=0}^{t_n} \eta\left(j_1 b_1 \mathbf{u}_1 + \cdots + j_n b_n \mathbf{u}_n + \mathbf{d}_1\right) \right.$$
$$\left. \times \cdots \times \eta\left(j_1 b_1 \mathbf{u}_1 + \cdots + j_n b_n \mathbf{u}_n + \mathbf{d}_k\right) \right|,$$

where the maximum is taken over all n-dimensional vectors $\mathbf{B} = (b_1,\cdots,b_n)$, $\mathbf{d}_1,\cdots,\mathbf{d}_k$, $\mathbf{T} = (t_1,\cdots,t_n)$ whose coordinates are nonnegative integers, $b_1,\cdots,b_n$ are nonzero, $\mathbf{d}_1,\cdots,\mathbf{d}_k$ are distinct, and all the points $j_1 b_1 \mathbf{u}_1 + \cdots + j_n b_n \mathbf{u}_n + \mathbf{d}_i$ occurring in the multiple sum belong to the n-dimensional N-lattice I_N^n. Then $\mathbb{Q}_k(\eta)$ is called the pseudorandom measure of order k of η. An n-dimensional binary N-lattice η is considered as a "good" pseudorandom binary lattice if $\mathbb{Q}_k(\eta)$ is "small" in terms of N for small k. P. Hubert, C. Mauduit and A. Sárközy [10] proved that this terminology is justified since for a fixed $k \in \mathbb{N}$ and for a truly random n-dimensional binary N-lattice $\eta(\mathbf{x})$, we have $N^{n/2} \ll \mathbb{Q}_k(\eta) \ll N^{n/2}(\log N^n)^{1/2}$ with probability $> 1-\epsilon$.

Let p be an odd prime, $n \in \mathbb{N}$, $q = p^n$, and denote the quadratic character of $\mathbb{F}_q$ by γ. Let $v_1,\cdots,v_n$ be linearly independent elements of $\mathbb{F}_q$ over $\mathbb{F}_p$. Assume that $f(x) \in \mathbb{F}_q[x]$ with $0 < \deg(f) < p$, $f(x)$ has no multiple zero in $\overline{\mathbb{F}}_q$, and define

$$\eta_1(\mathbf{x}) = \eta_1\left((x_1,\cdots,x_n)\right)$$
$$= \begin{cases} \gamma(f(x_1v_1+\cdots+x_nv_n)), & \text{for } f(x_1v_1+\cdots+x_nv_n) \neq 0, \\ 1, & \text{for } f(x_1v_1+\cdots+x_nv_n) = 0. \end{cases}$$

For $k = 2$ or $4^{n(\deg(f)+k)} < p$, C. Mauduit and A. Sárközy [20] proved that

$$\mathbb{Q}_k(\eta_1) < k\deg(f)\left(q^{1/2}(\log p+1)^n + 2\right).$$

Moreover, define the boxes $B_1^*, B_2^*, \cdots, B_n^*$ by

$$\begin{aligned} B_1^* &= \left\{ \sum_{i=1}^{n} u_i v_i : 0 \le u_1 \le \frac{p-3}{2}, u_2, \cdots, u_n \in \mathbb{F}_p \right\}, \\ B_j^* &= \left\{ \sum_{i=1}^{n} u_i v_i : u_1 = \cdots = u_{j-1} = \frac{p-1}{2}, 0 \le u_j \le \frac{p-3}{2}, u_{j+1}, \cdots, u_n \in \mathbb{F}_p \right\} \end{aligned}$$

for $j = 2, \cdots, n$, and write $B^* = \bigcup_{j=1}^{n} B_j^*$. Define

$$\begin{aligned} \eta_2(\mathbf{x}) &= \eta_2\left((x_1, \cdots, x_n)\right) \\ &= \begin{cases} +1, & \text{if } f(x_1v_1 + \cdots + x_nv_n) \neq 0 \text{ and } f(x_1v_1 + \cdots + x_nv_n)^{-1} \in B, \\ -1, & \text{otherwise.} \end{cases} \end{aligned}$$

For $0 < k, \deg(f) < p$, $k + \deg(f) \le p + 1$ and $k \deg(f) < \frac{q}{2}$, C. Mauduit and A. Sárközy [21] showed that

$$\mathbb{Q}_k(\eta_2) < \left(2^{k+3} + 1\right) k \deg(f) n^k q^{1/2} \left(\log p + 2\right)^{n+k}.$$

Now we give a family of pseudorandom binary lattices. Define the boxes $B_1, B_2, \cdots, B_n$ by

$$B_1 = \left\{ \sum_{i=1}^{n} u_i v_i : 1 \le u_1 \le p-1, 2 \mid u_1, \text{ and } u_2, \cdots, u_n \in \mathbb{F}_p \right\},$$

$$B_j = \left\{ \sum_{i=1}^{n} u_i v_i : u_1 = \cdots = u_{j-1} = 0, 1 \le u_j \le p-1, 2 \mid u_j, \text{ and } u_{j+1}, \cdots, u_n \in \mathbb{F}_p \right\}$$

for $j = 2, \cdots, n$, and write $B = \bigcup_{j=1}^{n} B_j$. For $f, g, h \in \mathbb{F}_q[x]$, denote the mapping $\eta(\mathbf{x}) : I_p^n \to \{-1, +1\}$ by

$$\eta(\mathbf{x}) = \eta\left((x_1, \cdots, x_n)\right) =$$

$$\begin{cases} +1, & \text{if } g(x_1v_1 + \cdots + x_nv_n)h(x_1v_1 + \cdots + x_nv_n) = 0, \\ \gamma(h(x_1v_1 + \cdots + x_nv_n)), & \text{if } g(x_1v_1 + \cdots + x_nv_n)h(x_1v_1 + \cdots + x_nv_n) \neq 0, \\ & f(x_1v_1 + \cdots + x_nv_n) \in B,\ g(x_1v_1 + \cdots + x_nv_n)^{-1} \in B, \\ & \text{or } f(x_1v_1 + \cdots + x_nv_n) \notin B,\ g(x_1v_1 + \cdots + x_nv_n)^{-1} \notin B, \\ -\gamma(h(x_1v_1 + \cdots + x_nv_n)), & \text{if } g(x_1v_1 + \cdots + x_nv_n)h(x_1v_1 + \cdots + x_nv_n) \neq 0, \\ & f(x_1v_1 + \cdots + x_nv_n) \in B,\ g(x_1v_1 + \cdots + x_nv_n)^{-1} \notin B, \\ & \text{or } f(x_1v_1 + \cdots + x_nv_n) \notin B,\ g(x_1v_1 + \cdots + x_nv_n)^{-1} \in B. \end{cases}$$

We shall prove the following:

Theorem 1.1. *If p, q, n, B and η are defined as above, $k \in \mathbb{N}$, and one of the following conditions holds:*

(i) $g(x)$ has no multiple zero in $\overline{\mathbb{F}}_q$, and $0 < k, \deg(g) < p$, $k + \deg(g) \le p + 1$, $k \deg(g) < \frac{q}{2}$;

(ii) $h(x)$ has no multiple zero in $\overline{\mathbb{F}}_q$, $0 < \deg(h) < p$, and $k = 2$ or $4^{n(\deg(h)+k)} < p$,

then we have

$$\mathbb{Q}_k(\eta) < 2^{2k+1} n^{2k} \left(\deg(f) + k \deg(g) + k \deg(h)\right) q^{\frac{1}{2}} \left(\log p + 2\right)^{n+2k}.$$

Taking $f = 1$ and $g = 1$ in our construction, we have $\eta = \eta_1$. Furthermore, $E_{p-1}^{(1)}$, $E_{p-1}^{(2)}$, $E_p^{(3)}$, $E_p^{(4)}$, $E_p^{(5)}$ can be considered as special cases of our construction for $n = 1$.

2. Some lemmas

To prove Theorem 1.1, we need the following lemmas.

Lemma 2.1. *Let $\mathbb{F}_q$ be a finite field of characteristic p, and let ψ be a nontrivial additive character and χ a multiplicative character on $\mathbb{F}_q$ of order d. For two rational functions $f, g \in \mathbb{F}_q[x]$, define $K(\psi, f; \chi, g) = \sum_{x \in \mathbb{F}_q \setminus \mathcal{S}} \psi(f(x))\chi(g(x))$, where $\mathcal{S}$ is the set of poles of f and g. If one of the following conditions holds:*

(i) $f(x)$ is not of the form $(A(x))^p - A(x)$ with a rational function $A(x)$ over $\mathbb{F}_q$,

(ii) $g(x)$ has no multiple zero in $\overline{\mathbb{F}}_q$ and is not of a d-th power,

then we have

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

where l is the number of distinct and (noninfinite) poles of g in $\mathbb{F}_q$.

Proof. See [22] or [5]. □

Lemma 2.2. *Suppose that $q = p^n$, ψ is a nontrivial additive character of $\mathbb{F}_q$, χ is a multiplicative character on $\mathbb{F}_q$ of order d, $v_1, \cdots, v_n$ are linearly independent over the prime field of $\mathbb{F}_q$, and $\overline{B} = \{\sum_{i=1}^n j_i v_i : 0 \leq j_i \leq t_i \text{ for } i = 1, 2, \cdots, n\}$. For rational functions $Q/R, g \in \mathbb{F}_q[x]$, if one of the following conditions holds:*

(i) $R(x) \nmid Q(x)$ and there is no polynomial $L(x) \in \mathbb{F}_q[x]$ such that $(L(x))^p \mid R(x)$ and $\deg(L(x)) > 0$,

(ii) $g(x)$ has no multiple zero in $\overline{\mathbb{F}}_q$ and is not of a d-th power,

then we have

$$\sum_{\substack{z \in \overline{B} \\ R(z) \neq 0}} \psi\left(\frac{Q(z)}{R(z)}\right) \chi(g(z)) < (\max(\deg(Q), \deg(R)) + l)\, q^{1/2} (\log p + 2)^n,$$

where l is the number of distinct and (noninfinite) poles of g in $\mathbb{F}_q$.

Proof. This lemma can be deduced from Lemma 2.1 in the same way as Lemma 4 is derived from Lemma 3 in [21] with slight modifications. For completeness we give a detailed proof. It is not hard to show that

$$\left| \sum_{\substack{z \in \overline{B} \\ R(z) \neq 0}} \psi\left(\frac{Q(z)}{R(z)}\right) \chi(g(z)) \right| = \left| \sum_{\substack{m \in \mathbb{F}_q \\ R(m) \neq 0}} \psi\left(\frac{Q(m)}{R(m)}\right) \chi(g(m)) \sum_{b \in \overline{B}} \frac{1}{q} \sum_{h \in \mathbb{F}_q} \psi\left(h(m-b)\right) \right|$$

$$\leq \frac{1}{q} \sum_{h \in \mathbb{F}_q} \left| \sum_{\substack{m \in \mathbb{F}_q \\ R(m) \neq 0}} \psi\left(\frac{Q(m) + hmR(m)}{R(m)}\right) \chi(g(m)) \right| \left| \sum_{b \in \overline{B}} \psi(hb) \right|. \tag{2.1}$$

Assume that there are polynomials $K, L \in \mathbb{F}_q[x]$ with $(K, L) = 1$ and

$$\frac{Q(m) + hmR(m)}{R(m)} = \left(\frac{k(m)}{L(m)}\right)^p - \frac{k(m)}{L(m)}.$$

Then

$$(Q(m) + hmR(m))\,(L(m))^p = K(m)R(m)\left((K(m))^{p-1} - (L(m))^{p-1}\right).$$

Since $R(m) \mid (Q(m) + hmR(m))\,(L(m))^p$ and $R(m) \nmid Q(m)$, we get $\deg(L(m)) > 0$. On the other hand, from $(L(m))^p \mid K(m)R(m)\left((K(m))^{p-1} - (L(m))^{p-1}\right)$ and $(K(m), L(m)) = 1$ we have $(L(m))^p \mid R(m)$, which contradicts Condition (i). That is to say, if $R(x) \nmid Q(x)$ and there is no polynomial $L(x) \in \mathbb{F}_q[x]$ such that $(L(x))^p \mid R(x)$ and $\deg(L(x)) > 0$, then $Q(x)/R(x)$ is not of the form $(A(x))^p - A(x)$ with a rational function $A(x)$ over $\mathbb{F}_q$. So from Lemma 2.1 we have

$$\left| \sum_{\substack{m \in \mathbb{F}_q \\ R(m) \neq 0}} \psi\left(\frac{Q(m) + hmR(m)}{R(m)}\right) \chi(g(m)) \right| \leq (\max(\deg(Q), \deg(R)) + l)\, q^{1/2}. \tag{2.2}$$

On the other hand, from (3.21) of [21] we have

$$\sum_{h \in \mathbb{F}_q} \left| \sum_{b \in \overline{B}} \psi(hb) \right| < q\,(\log p + 2)^n\,. \tag{2.3}$$

Now combining (2.1)-(2.3) we immediately get the following lemma. □

Lemma 2.3. *Let $q = p^n$ and $\mathbb{F}_q$ be a finite field, $s_1, \cdots, s_m$ be nonzero elements of $\mathbb{F}_q$, $y_1, \cdots, y_m$ be distinct elements of $\mathbb{F}_q$, $g(x) \in \mathbb{F}_q[x]$. Define*

$$Q(x) = \sum_{i=1}^{m} s_i \prod_{\substack{1 \leq j \leq m \\ j \neq i}} g(x + y_j) \quad \textit{with} \quad g(x + y_1) \cdots g(x + y_m) \neq 0.$$

If $g(x)$ has no multiple zero in $\overline{\mathbb{F}}_q$ and $0 < m, \deg(g) < p$, $m + \deg(g) \leq p + 1$, $m \deg(g) < \frac{q}{2}$, then $Q(x)$ is not the 0 polynomial.

Proof. This is Lemma 1 of [21]. □

Lemma 2.4. *Let $q = p^n$ and $\mathbb{F}_q$ be a finite field, $z_1, \cdots, z_k$ be distinct elements of $\mathbb{F}_q$, $h(x) \in \mathbb{F}_q[x]$ with $h(x) = ah_1(x)$, where $a \in \mathbb{F}_q$ and $h_1(x)$ is a monic polynomial. Define $H(x) = h_1(x + z_1) \cdots h_1(x + z_k)$. If $h(x)$ has no multiple zero in $\overline{\mathbb{F}}_q$, $0 < \deg(h) < p$, and $k = 2$ or $4^{n(\deg(h)+k)} < p$, then $H(x)$ has at least one zero in $\overline{\mathbb{F}}_q$ whose multiplicity is odd.*

Proof. See Lemma 2 and Theorem 2 of [20]. □

Lemma 2.5. *Let $\mathbb{F}_q$ be a finite field with $q = p^n$, and let ψ be a nontrivial additive character and γ the quadratic character of $\mathbb{F}_q$. Let $f, g, h \in \mathbb{F}_q[x]$ with $h(x) = ah_1(x)$, where $a \in \mathbb{F}_q$ and $h_1(x)$ is a monic polynomial. For integers l, m, k with $l \geq 0$, $m, k > 0$ and $l, m \leq k$, let $x_1, \cdots, x_l$ be distinct elements of $\mathbb{F}_q$, $y_1, \cdots, y_m$ be distinct elements of $\mathbb{F}_q$, and $z_1, \cdots, z_k$ be distinct elements of $\mathbb{F}_q$. Suppose that $v_1, \cdots, v_n$ are linearly independent over the prime field of $\mathbb{F}_q$ and $b_1, \cdots, b_n$ are positive integers. Define*

$$B' = \left\{ \sum_{i=1}^{n} j_i(b_i v_i) : 0 \leq j_i \leq t_i, \ \textit{for} \ \ i = 1, \cdots, n \right\}.$$

For $r_1, \cdots, r_l, s_1, \cdots, s_m \in \mathbb{F}_q^*$, *denote*

$$T := \sum_{\substack{z \in B' \\ g(z+y_1)\cdots g(z+y_m) \neq 0}} \gamma\left(h_1(z+z_1)\cdots h_1(z+z_k)\right)$$
$$\times \psi\left(r_1 f(z+x_1) + \cdots + r_l f(z+x_l) + s_1 g(z+y_1)^{-1} + \cdots + s_m g(z+y_m)^{-1}\right).$$

If one of the following conditions holds:

(i) $g(x)$ *has no multiple zero in* $\overline{\mathbb{F}}_q$, *and* $0 < m, \deg(g) < p$, $m + \deg(g) \leq p+1$, $m\deg(g) < \frac{q}{2}$;

(ii) $h(x)$ *has no multiple zero in* $\overline{\mathbb{F}}_q$, $0 < \deg(h) < p$, *and* $k = 2$ *or* $4^{n(\deg(h)+k)} < p$,

then we have $T < (\deg(f) + m\deg(g) + k\deg(h))\, q^{1/2} (\log p + 2)^n$.

Proof. Define $R(z) = g(z+y_1)\cdots g(z+y_m)$, $H(z) = h_1(z+z_1)\cdots h_1(z+z_k)$, and

$$Q(z) = (r_1 f(z+x_1) + \cdots + r_l f(z+x_l))\, g(z+y_1)\cdots g(z+y_m) + \sum_{i=1}^{m} s_i \prod_{\substack{1 \leq j \leq m \\ j \neq i}} g(z+y_j).$$

Then we get $T = \sum_{\substack{z \in B' \\ R(z) \neq 0}} \psi\left(\frac{Q(z)}{R(z)}\right) \gamma\left(H(z)\right)$.

First we suppose that $g(x)$ has no multiple zero in $\overline{\mathbb{F}}_q$ and $0 < m, \deg(g) < p$, $m + \deg(g) \leq p+1$, $m\deg(g) < \frac{q}{2}$. It is not hard to show that there is no polynomial $L(x) \in \mathbb{F}_q[x]$ such that $(L(x))^p \mid R(x)$ and $\deg(L(x)) > 0$. Moreover, by Lemma 2.3 we know that $\sum_{i=1}^{m} s_i \prod_{\substack{1 \leq j \leq m \\ j \neq i}} g(z+y_j)$ is not the 0 polynomial. Then we have $R(x) \nmid Q(x)$.

Next assume that $h(x)$ has no multiple zero in $\overline{\mathbb{F}}_q$, $0 < \deg(h) < p$, and $k = 2$ or $4^{n(\deg(h)+k)} < p$. By Lemma 2.4 we know that $H(x)$ has at least one zero in $\overline{\mathbb{F}}_q$ whose multiplicity is odd. Then $H(x)$ cannot be a 2-nd power.

Now from Lemma 2.2 we immediately get

$$T < (\deg(f) + m\deg(g) + k\deg(h))\, q^{1/2} (\log p + 2)^n. \qquad \square$$

3. Proof of Theorem 1.1

Let $q = p^n$ and $\mathbb{F}_q$ be a finite field, and let ψ_1 be the canonical additive character of $\mathbb{F}_q$. Let $b_1, \cdots, b_n$ be positive integers, and write $\mathbf{d}_i = \left(d_1^{(i)}, \cdots, d_n^{(i)}\right)$ for $i = 1, 2, \cdots, k$. Define $B' = \{\sum_{i=1}^n j_i(b_i v_i) : 0 \leq j_i \leq t_i, \text{ for } i = 1, \cdots, n\}$, $z = j_1(b_1 v_1) + \cdots + j_n(b_n v_n)$, $z_l = d_1^{(l)} v_1 + \cdots + d_n^{(l)} v_n$, for $l = 1, \cdots, k$. Noting that

$$2\left(\frac{1}{q}\sum_{b \in B}\sum_{r \in \mathbb{F}_q} \psi_1\left(r(x-b)\right) - \frac{1}{2}\right) = \begin{cases} +1, & \text{if } x \in B, \\ -1, & \text{if } x \notin B, \end{cases}$$

we have

(3.1)

$$\begin{aligned}
&\sum_{j_1=0}^{t_1}\cdots\sum_{j_n=0}^{t_n}\eta\left(j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_1\right)\cdots\eta\left(j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_k\right)\\
&=\sum_{\substack{z\in B'\\ g(z+z_1)\cdots g(z+z_k)h(z+z_1)\cdots h(z+z_k)\neq 0}} 2^{2k}\prod_{i=1}^{k}\left[\left(\frac{1}{q}\sum_{b\in B}\sum_{r\in\mathbb{F}_q}\psi_1(r\left(f(z+z_i)-b\right))-\frac{1}{2}\right)\right.\\
&\qquad\left.\times\left(\frac{1}{q}\sum_{c\in B}\sum_{s\in\mathbb{F}_q}\psi_1\left(s\left(g(z+z_i)^{-1}-c\right)\right)-\frac{1}{2}\right)\gamma\left(h(z+z_i)\right)\right]\\
&\quad+\sum_{\substack{z\in B'\\ g(z+z_1)\cdots g(z+z_k)h(z+z_1)\cdots h(z+z_k)=0}}1\\
&:=\Sigma_1+\Sigma_2.
\end{aligned}$$

It is easy to show that

$$\Sigma_2\le k\deg(gh). \tag{3.2}$$

Let $h(x)=ah_1(x)$, where $a\in\mathbb{F}_q$ and $h_1(x)$ is a monic polynomial. Noting that $\frac{1}{q}\sum_{b\in B}1-\frac{1}{2}=-\frac{1}{2q}$, we get

(3.3)

$$\begin{aligned}
\Sigma_1&=\frac{2^{2k}\gamma(a^k)}{q^{2k}}\sum_{\substack{z\in B'\\ g(z+z_1)\cdots g(z+z_k)\neq 0}}\prod_{i=1}^{k}\left(\sum_{b\in B}\sum_{r\in\mathbb{F}_q^*}\psi_1\left(r\left(f(z+z_i)-b\right)\right)-\frac{1}{2}\right)\\
&\qquad\times\prod_{j=1}^{k}\left(\sum_{c\in B}\sum_{s\in\mathbb{F}_q^*}\psi_1\left(s\left(g(z+z_j)^{-1}-c\right)\right)-\frac{1}{2}\right)\gamma\left(h_1(z+z_1)\cdots h_1(z+z_k)\right)\\
&=\frac{\gamma(a^k)}{q^{2k}}\sum_{\substack{z\in B'\\ g(z+z_1)\cdots g(z+z_k)\neq 0}}\sum_{l=0}^{k}(-1)^l2^l\sum_{(b_1,\cdots,b_l)\in B^l}\sum_{(r_1,\cdots,r_l)\in(\mathbb{F}_q^*)^l}\sum_{1\le i_1<\cdots<i_l\le k}\\
&\qquad\times\psi_1(r_1(f(z+z_{i_1})-b_1)+\cdots+r_l(f(z+z_{i_l})-b_l))\,\gamma\left(h_1(z+z_1)\cdots h_1(z+z_k)\right)\\
&\qquad+\frac{\gamma(a^k)}{q^{2k}}\sum_{\substack{z\in B'\\ g(z+z_1)\cdots g(z+z_k)\neq 0}}\sum_{l=0}^{k}\sum_{m=1}^{k}(-1)^{m+l}2^{m+l}\sum_{(b_1,\cdots,b_l)\in B^l}\sum_{(r_1,\cdots,r_l)\in(\mathbb{F}_q^*)^l}\\
&\qquad\times\sum_{1\le i_1<\cdots<i_l\le k}\times\psi_1\left(r_1\left(f(z+z_{i_1})-b_1\right)+\cdots+r_l\left(f(z+z_{i_l})-b_l\right)\right)\\
&\qquad\times\sum_{(c_1,\cdots,c_m)\in B^m}\sum_{(s_1,\cdots,s_m)\in(\mathbb{F}_q^*)^m}\sum_{1\le j_1<\cdots<j_m\le k}\psi_1\left(s_1\left(g(z+z_{j_1})^{-1}-c_1\right)\right.\\
&\qquad\left.+\cdots+s_m\left(g(z+z_{j_m})^{-1}-c_m\right)\right)\gamma\left(h_1(z+z_1)\cdots h_1(z+z_k)\right)\\
&:=S_1+S_2.
\end{aligned}$$

Using the methods of (3.26)-(3.29) in [21] we can have

$$\sum_{r\in\mathbb{F}_q^*}\left|\sum_{b\in B}\psi_1(rb)\right| < nq\left(\log p+\frac{3}{2}\right). \tag{3.4}$$

Therefore

$$\begin{aligned}
S_1 &\le \frac{1}{q^{2k}}\sum_{l=0}^{k}2^l\sum_{(r_1,\cdots,r_l)\in(\mathbb{F}_q^*)^l}\ \sum_{1\le i_1<\cdots<i_l\le k}\\
&\times\Bigg|\sum_{\substack{z\in B'\\ g(z+z_1)\cdots g(z+z_k)\neq 0}}\psi_1(r_1f(z+z_{i_1})+\cdots\\
&\qquad\qquad +r_lf(z+z_{i_l}))\,\gamma\left(h_1(z+z_1)\cdots h_1(z+z_k)\right)\Bigg|\\
&\times\left|\sum_{(b_1,\cdots,b_l)\in B^l}\psi_1\left(-r_1b_1-\cdots-r_lb_l\right)\right|\\
&\le \frac{1}{q^{2k-1}}\sum_{l=0}^{k}2^l\binom{k}{l}\left(\sum_{r\in\mathbb{F}_q^*}\left|\sum_{b\in B}\psi_1(rb)\right|\right)^l < \frac{1}{q^{2k-1}}\sum_{l=0}^{k}2^l\binom{k}{l}\left(nq\left(\log p+\frac{3}{2}\right)\right)^l\\
&= \frac{1}{q^{2k-1}}\left(2nq\left(\log p+\frac{3}{2}\right)+1\right)^k.
\end{aligned} \tag{3.5}$$

On the other hand, by Lemma 2.5 and (3.4) we also have

$$\begin{aligned}
S_2 &\le \frac{1}{q^{2k}}\sum_{l=0}^{k}\sum_{m=1}^{k}2^{m+l}\sum_{(r_1,\cdots,r_l)\in(\mathbb{F}_q^*)^l}\ \sum_{1\le i_1<\cdots<i_l\le k}\ \sum_{(s_1,\cdots,s_m)\in(\mathbb{F}_q^*)^m}\ \sum_{1\le j_1<\cdots<j_m\le k}\\
&\times\Bigg|\sum_{\substack{z\in B'\\ g(z+z_1)\cdots g(z+z_k)\neq 0}}\gamma\left(h_1(z+z_1)\cdots h_1(z+z_k)\right)\psi_1\left(r_1f(z+z_{i_1})+\cdots\right.\\
&\quad\left.+\,r_lf(z+z_{i_l})+s_1g(z+z_{j_1})^{-1}+\cdots+s_mg(z+z_{j_m})^{-1}\right)\Bigg|\\
&\times\left|\sum_{(b_1,\cdots,b_l)\in B^l}\psi_1(-r_1b_1-\cdots-r_lb_l)\right|\cdot\left|\sum_{(c_1,\cdots,c_m)\in B^m}\psi_1(-s_1c_1-\cdots-s_mc_m)\right|\\
&\le \frac{1}{q^{2k}}\sum_{l=0}^{k}\sum_{m=1}^{k}2^{m+l}\sum_{(r_1,\cdots,r_l)\in(\mathbb{F}_q^*)^l}\ \sum_{1\le i_1<\cdots<i_l\le k}\ \sum_{(s_1,\cdots,s_m)\in(\mathbb{F}_q^*)^m}\ \sum_{1\le j_1<\cdots<j_m\le k}\\
&\times\Bigg|\sum_{\substack{z\in B'\\ g(z+z_{j_1})\cdots g(z+z_{j_m})\neq 0}}\gamma\left(h_1(z+z_1)\cdots h_1(z+z_k)\right)\psi_1\left(r_1f(z+z_{i_1})+\cdots\right.
\end{aligned} \tag{3.6}$$

$$
\begin{aligned}
&+ r_l f(z+z_{i_l}) + s_1 g(z+z_{j_1})^{-1} + \cdots + s_m g(z+z_{j_m})^{-1}) \Bigg| \\
&\times \left| \sum_{(b_1,\cdots,b_l)\in B^l} \psi_1(-r_1b_1-\cdots-r_lb_l) \right| \cdot \left| \sum_{(c_1,\cdots,c_m)\in B^m} \psi_1(-s_1c_1-\cdots-s_mc_m) \right| \\
&+ \frac{1}{q^{2k}} k\deg(g) \sum_{l=0}^{k}\sum_{m=1}^{k} 2^{m+l}\binom{k}{l}\binom{k}{m} \sum_{(r_1,\cdots,r_l)\in(\mathbb{F}_q^*)^l} \sum_{(s_1,\cdots,s_m)\in(\mathbb{F}_q^*)^m} \\
&\times \left| \sum_{(b_1,\cdots,b_l)\in B^l} \psi_1(-r_1b_1-\cdots-r_lb_l) \right| \cdot \left| \sum_{(c_1,\cdots,c_m)\in B^m} \psi_1\left(-s_1c_1-\cdots-s_mc_m\right) \right| \\
&< \frac{1}{q^{2k}} \sum_{l=0}^{k}\sum_{m=1}^{k} 2^{m+l}\binom{k}{l}\binom{k}{m} \left(\sum_{r\in\mathbb{F}_q^*} \left| \sum_{b\in B} \psi_1(rb) \right| \right)^{l+m} \\
&\quad \times \left(\left(\deg(f)+m\deg(g)+k\deg(h)\right) q^{1/2} \left(\log p+2\right)^n \right) \\
&\quad + \frac{1}{q^{2k}} k\deg(g) \sum_{l=0}^{k}\sum_{m=1}^{k} 2^{m+l}\binom{k}{l}\binom{k}{m} \left(\sum_{r\in\mathbb{F}_q^*} \left| \sum_{b\in B} \psi_1(rb) \right| \right)^{l+m} \\
&< \frac{1}{q^{2k}} \left(\deg(f)+k\deg(g)+k\deg(h)\right) q^{1/2} \left(\log p+2\right)^n \\
&\quad \times \sum_{l=0}^{k}\sum_{m=1}^{k} 2^{m+l}\binom{k}{l}\binom{k}{m} \left(nq\left(\log p+\frac{3}{2}\right)\right)^{l+m} \\
&\quad + \frac{1}{q^{2k}} k\deg(g) \sum_{l=0}^{k}\sum_{m=1}^{k} 2^{m+l}\binom{k}{l}\binom{k}{m} \left(nq\left(\log p+\frac{3}{2}\right)\right)^{l+m} \\
&< \frac{1}{q^{2k}} \left(\deg(f)+k\deg(g)+k\deg(h)\right) q^{1/2} \left(\log p+2\right)^n \left(2nq\left(\log p+\frac{3}{2}\right)+1\right)^{2k} \\
&\quad + \frac{1}{q^{2k}} k\deg(g) \left(2nq\left(\log p+\frac{3}{2}\right)+1\right)^{2k}.
\end{aligned}
$$

Now from (3.1)-(3.3) and (3.5)-(3.6) we get

$$
\begin{aligned}
&\sum_{j_1=0}^{t_1}\cdots\sum_{j_n=0}^{t_n} \eta\left(j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_1\right)\cdots\eta\left(j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_k\right) \\
&< k\deg(gh) + \frac{1}{q^{2k-1}}\left(2nq\left(\log p+\frac{3}{2}\right)+1\right)^k \\
&\quad + \frac{1}{q^{2k}} k\deg(g)\left(2nq\left(\log p+\frac{3}{2}\right)+1\right)^{2k} \\
&\quad + \frac{1}{q^{2k}}\left(\deg(f)+k\deg(g)+k\deg(h)\right) q^{1/2}(\log p+2)^n\left(2nq\left(\log p+\frac{3}{2}\right)+1\right)^{2k} \\
&< 2^{2k+1}n^{2k}\left(\deg(f)+k\deg(g)+k\deg(h)\right) q^{\frac{1}{2}} \left(\log p+2\right)^{n+2k}.
\end{aligned}
$$

Therefore

$$\mathbb{Q}_k(\eta) < 2^{2k+1} n^{2k} \left(\deg(f) + k\deg(g) + k\deg(h)\right) q^{\frac{1}{2}} \left(\log p + 2\right)^{n+2k}.$$

This proves Theorem 1.1.

References

1. 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), pp. 1–29. MR2195573 (2006j:60007)
2. J. Cassaigne, C. Mauduit and A. Sárközy, On finite pseudorandom binary sequences, VII: The measures of pseudorandomness, *Acta Arithmetica,* 103 (2002), pp. 97–118. MR1904866 (2004c:11139)
3. 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), pp. 367–390. MR1671629 (2000c:11126)
4. J. Cassaigne, S. Ferenczi, C. Mauduit, J. Rivat and A. Sárközy, On finite pseudorandom binary sequences, IV: The Liouville function, II, *Acta Arithmetica,* 95 (2000), pp. 343–359. MR1785199 (2002c:11087)
5. F. N. Castro and C. J. Moreno, Mixed exponential sums over finite fields, *Proceedings of the American Mathematical Society,* 128 (2000), pp. 2529–2537. MR1690978 (2000m:11070)
6. 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)
7. L. Goubin, C. Mauduit and A. Sárközy, Construction of large families of pseudorandom binary sequences, *Journal of Number Theory,* 106 (2004), pp. 56–69. MR2049592 (2004m:11121)
8. K. Gyarmati, On a family of pseudorandom binary sequences, *Periodica Mathematica Hungarica,* 49 (2004), pp. 45–63. MR2106465 (2005h:11167)
9. K. Gyarmati, Pseudorandom sequences constructed by the power generator, *Periodica Mathematica Hungarica,* 52 (2006), pp. 9–26. MR2265647 (2007i:11110)
10. P. Hubert, C. Mauduit and A. Sárközy, On pseudorandom binary lattices, *Acta Arithmetica,* 125 (2006), pp. 51–62. MR2275217 (2007k:11124)
11. H. Liu, New pseudorandom sequences constructed using multiplicative inverses, *Acta Arithmetica,* 125 (2006), pp. 11–19. MR2275214 (2007i:11111)
12. H. Liu, New pseudorandom sequences constructed by quadratic residues and Lehmer numbers, *Proceedings of the American Mathematical Society,* 135 (2007), pp. 1309–1318. MR2276639 (2007j:11099)
13. H. Liu, A family of pseudorandom binary sequences constructed by the multiplicative inverse, *Acta Arithmetica*, 130 (2007), pp. 167–180. MR2357654 (2008i:11103)
14. H. Liu and C. Yang, On a problem of D. H. Lehmer and pseudorandom binary sequences, *Bulletin of the Brazilian Mathematical Society,* 39 (2008), pp. 387–399.
15. S. R. Louboutin, J. Rivat and A. Sárközy, On a problem of D. H. Lehmer, *Proceedings of the American Mathematical Society,* 135 (2007), pp. 969–975. MR2262896 (2007g:11089)
16. C. Mauduit, J. Rivat and A. Sárközy, Construction of pseudorandom binary sequences using additive characters, *Monatshefte für Mathematik,* 141 (2004), pp. 197–208. MR2042211 (2005a:11117)
17. 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)
18. C. Mauduit and A. Sárközy, On the measures of pseudorandomness of binary sequences, *Discrete Mathematics,* 271 (2003), pp. 195–207. MR1999543 (2004e:11081)
19. C. Mauduit and A. Sárközy, Construction of pseudorandom binary sequences by using the multiplicative inverse, *Acta Mathematica Hungarica,* 108 (2005), pp. 239–252. MR2162562 (2006c:11092)
20. C. Mauduit and A. Sárközy, On large families of pseudorandom binary lattices, *Uniform Distribution Theory,* 2 (2007), pp. 23–37. MR2318530 (2008h:11079)
21. C. Mauduit and A. Sárközy, Construction of pseudorandom binary lattices by using the multiplicative inverse, *Monatshefte für Mathematik,* 153 (2008), pp. 217–231. MR2379668

22. G. I. Perel′muter, Estimation of a sum along an algebraic curve, *Matematicheskie Zametki,* 5 (1969), pp. 373–380. MR0241424 (39:2764)
23. A. Sárközy, A finite pseudorandom binary sequence, *Studia Scientiarum Mathematicarum Hungarica,* 38 (2001), pp. 377–384. MR1877793 (2003j:11082)

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

E-mail address: hnliumath@hotmail.com