AIMS Mathematics, 7(3): 4655–4671.
DOI: 10.3934/math.2022259
Received: 04 September 2021
Revised: 11 December 2021
Accepted: 19 December 2021
Published: 24 December 2021

http://www.aimspress.com/journal/Math

Research article

Binary sequences and lattices constructed by discrete logarithms

Yuchan Qi and Huaning Liu*

Research Center for Number Theory and Its Applications, School of Mathematics, Northwest University, Xi'an 710127, China

* **Correspondence:** Email: hnliu@nwu.edu.cn.

Abstract: In 1997, Mauduit and Sárközy first introduced the measures of pseudorandomness for binary sequences. Since then, many pseudorandom binary sequences have been constructed and studied. In particular, Gyarmati presented a large family of pseudorandom binary sequences using the discrete logarithms. Ten years later, to satisfy the requirement from many applications in cryptography (e.g., in encrypting "bit-maps" and watermarking), the definition of binary sequences is extended from one dimension to several dimensions by Hubert, Mauduit and Sárközy. They introduced the measure of pseudorandomness for this kind of several-dimension binary sequence which is called binary lattices. In this paper, large families of pseudorandom binary sequences and binary lattices are constructed by both discrete logarithms and multiplicative inverse modulo p. The upper estimates of their pseudorandom measures are based on estimates of either character sums or mixed exponential sums.

Keywords: discrete logarithm; pseudorandom binary lattice; pseudorandom measure; character sums; exponential sums
Mathematics Subject Classification: 11K45, 11L07, 11L40, 11Z05

1. Introduction and main results

Over 20 years ago, Mauduit and Sárközy (partly with coauthors) started to study pseudorandomness of binary sequences

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

and developed a quantitative and constructive theory of this subject. In particular, in [1] Mauduit and Sárközy introduced the 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

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

where the maximum is taken over all $D = (d_1, \cdots, d_k)$ and M with $0 \le d_1 < \cdots < d_k \le N - M$.

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. Later many pseudorandom binary sequences were given and studied by using number theoretic methods (see [2–6]).

Let p be a prime number and g be a primitive root modulo p. For an integer n with $\gcd(n, p) = 1$, let ind n be the smallest non-negative integer t with $g^t \equiv n \pmod{p}$. That is,

$$n \equiv g^{\text{ind } n} \pmod{p} \qquad \text{and} \qquad 0 \le \text{ind } n \le p-2.$$

We name ind (n) the *discrete logarithm* of n to the base g. Gyarmati [7] presented a large family of pseudorandom binary sequences using the discrete logarithms.

Proposition 1.1. *Let $f(x) \in \mathbb{F}_p[x]$ be a polynomial of degree l, and define $E_{p-1} = (e_1, \cdots, e_{p-1})$ by*

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

Then

$$W\left(E_{p-1}\right) < 38lp^{1/2} (\log p)^2.$$

Moreover, suppose that at least one of the following assumptions holds:

(i) *f is irreducible;*

(ii) *If f has a factorization $f = \varphi_1^{\alpha_1} \varphi_2^{\alpha_2} \cdots \varphi_u^{\alpha_u}$ where $\alpha_i \in \mathbb{N}$ and φ_i is irreducible over $\mathbb{F}_p$, then there exists a number β such that exactly one or two φ_i's have degree β;*

(iii) *$k = 2$;*

(iv) *$(4k)^l < p$ or $(4l)^k < p$.*

Then we have

$$C_k\left(E_{p-1}\right) < 10lk4^k p^{\frac{1}{2}} (\log p)^{k+1}.$$

The first purpose of this paper is to give large families of pseudorandom binary sequences using the discrete logarithms.

Theorem 1.1. *Let $f(x) \in \mathbb{F}_p[x]$ be a polynomial of degree l, and define $E_{p-1} = (e_1, \cdots, e_{p-1})$ by*

$$e_n = \begin{cases} +1, & \text{if } 1 \le \text{ind}\,(f(n) + \overline{n}) \le \frac{p-1}{2}, \\ -1, & \text{if } \frac{p+1}{2} \le \text{ind}\,(f(n) + \overline{n}) \le p-1 \text{ or } p \mid f(n) + \overline{n}, \end{cases}$$

where $\overline{n}$ is the inverse of n modulo p such that $n\overline{n} \equiv 1 \pmod{p}$ and $1 \le \overline{n} \le p-1$. Then

$$W\left(E_{p-1}\right) \ll \deg(f) p^{\frac{1}{2}} (\log p)^2.$$

Moreover, if the congruence $xf(x)+1 \equiv 0 \pmod{p}$ *has no solution, then for any* $k \in \mathbb{N}$ *we have*

$$C_k\left(E_{p-1}\right) \ll 2^k k \deg(f) p^{\frac{1}{2}} (\log p)^{k+1}.$$

Corollary 1.1. *Suppose that* p *is a prime with* $p \equiv 3 \pmod 4$*, and* $f(x) = xg^2(x)$ *with* $g(x) \in \mathbb{F}_p[x]$*. Define* $E_{p-1} = (e_1, \cdots, e_{p-1})$ *by*

$$e_n = \begin{cases} +1, & \text{if } 1 \le \operatorname{ind}(f(n)+\overline{n}) \le \frac{p-1}{2}, \\ -1, & \text{if } \frac{p+1}{2} \le \operatorname{ind}(f(n)+\overline{n}) \le p-1 \text{ or } p \mid f(n)+\overline{n}, \end{cases}$$

Then

$$W\left(E_{p-1}\right) \ll \deg(f) p^{\frac{1}{2}} (\log p)^2.$$

For any $k \in \mathbb{N}$*, we have*

$$C_k\left(E_{p-1}\right) \ll 2^k k \deg(f) p^{\frac{1}{2}} (\log p)^{k+1}.$$

Let f, g be polynomials over $\mathbb{F}_p$. Define $\frac{f(n)}{g(n)} = f(n)g^{-1}(n)$ for $g(n) \neq 0$. Mérai [8] studied the distribution of $\frac{f(n)}{g(n)}$ in the residue classes modulo p and gave nontrivial upper bounds for the well-distribution measure and correlation measure. We also generalize the sequence in Theorem 1.1 by adding a simple rational function.

Theorem 1.2. *Suppose that* p *is a prime number and* $s < \log p$ *is a positive integer. Let* $f(x), g(x) \in \mathbb{F}_p[x]$ *and let* $0 \le a_1 < a_2 < \cdots < a_s \le p-1$ *be integers with* $\gcd(g(x), (x-a_1)\cdots(x-a_s)) = 1$*. Define* $E_p = (e_1, \cdots, e_p)$ *by*

$$e_n = \begin{cases} +1 & \text{if } p \nmid (n-a_1)\cdots(n-a_s), p \nmid f(n) + \dfrac{g(n)}{(n-a_1)\cdots(n-a_s)} \\ & \quad \text{and } 1 \le \operatorname{ind}\left(f(n) + \dfrac{g(n)}{(n-a_1)\cdots(n-a_s)}\right) \le \dfrac{p-1}{2}, \\ -1 & \text{otherwise.} \end{cases}$$

Then

$$W\left(E_p\right) \ll (\deg(f) + \deg(g) + s)\, p^{\frac{1}{2}} (\log p)^2.$$

Moreover, if the congruence $(x-a_1)\cdots(x-a_s)f(x) + g(x) \equiv 0 \pmod{p}$ *has no solution and one of the following two conditions holds:*

(i) $\min\{s, k\} \le 2$ *and* $\max\{s, k\} \le p-1$*,*

(ii) $(4k)^s \le p$ *or* $(4s)^k \le p$*,*

then for any $k \in \mathbb{N}$ *we have*

$$C_k\left(E_p\right) \ll 2^k k (\deg(f) + \deg(g) + s) p^{\frac{1}{2}} (\log p)^{k+1}.$$

Hubert, Dartyge and Sárközy [9] wrote the first paper on pseudorandom binary lattices in 2006, since then, about 25 papers have been published in this field. One can refer to [9–16] for further related

results and constructions. In [9], the definition of binary sequences is extended from one dimension to several dimensions by considering functions of type

$$\eta:\ I_N^n \to \{+1,-1\},$$

where I_N^n denotes the set of the n-dimensional vectors whose all coordinates are selected from the set $\{0,1,\cdots,N-1\}$:

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

We say that η is an n-dimensional binary N-lattice or briefly binary lattice. Let $k \in \mathbb{N}$ and let $\mathbf{u}_i$ $(i = 1,\cdots,n)$ be the n-dimensional unit vector whose i-coordinate is 1 and other coordinates are 0. The measure of pseudorandomness of a binary lattice is defined as follows:

$$Q_k(\eta) = \max_{\mathbf{B},\mathbf{d}_1,\cdots,\mathbf{d}_k,\mathbf{T}} \left| \sum_{j_1=0}^{t_1} \cdots \sum_{j_n=0}^{t_n} \eta(j_1b_1\mathbf{u}_1 + \cdots + j_nb_n\mathbf{u}_n + \mathbf{d}_1) \right.$$
$$\left. \times \cdots \times \eta(j_1b_1\mathbf{u}_1 + \cdots + j_nb_n\mathbf{u}_n + \mathbf{d}_k) \right|,$$

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 non-negative integers, $b_1,\cdots,b_n$ are non-zero, $\mathbf{d}_1,\cdots,\mathbf{d}_k$ are distinct, and the points $j_1b_1\mathbf{u}_1 + \cdots + j_nb_n\mathbf{u}_n + \mathbf{d}_i$ occurring in the multiple sum belong to I_N^n.

A binary lattice η is said to have strong pseudorandom properties, or briefly, it is considered as a "good" pseudorandom lattice if for fixed n, k and "large"N, the measure $Q_k(\eta)$ is "small" (much smaller, than the trivial upper bound N^n). Gyarmati, Mauduit and Sárközy gave the following constructions in [11].

Proposition 1.2. *Let p be an odd prime, $f(x,y) \in \mathbb{F}_p[x,y]$ be a polynomial of degree l. Suppose that $f(x,y)$ is square-free and it is not of the form $\prod_{j=1}^{r} f_j\left(\alpha_j x + \beta_j y\right)$, where $\alpha_j,\beta_j \in \mathbb{F}_p$ and $f_j(x) \in \mathbb{F}_p[x]$ for $j = 1,\cdots,r$. Assume that $k \in \mathbb{N}$ and one of the following conditions holds:*

a) $f(x,y)$ is irreducible,

b) $k = 2$,

c) $(4l)^k \le p$.

Define $\eta : I_p^2 \to \{-1,+1\}$ by

$$\eta(x,y) = \begin{cases} +1, & \text{if } (f(x,y),p) = 1 \text{ and } 1 \le \operatorname{ind} f(x,y) \le \frac{p-1}{2}, \\ -1, & \text{otherwise.} \end{cases}$$

Then we have

$$Q_k(\eta) \ll lk4^k p^{\frac{3}{2}} (\log p)^{k+1}.$$

The second purpose of this paper is to construct a large family of pseudorandom binary lattices using the discrete logarithms.

Theorem 1.3. *Let p be an odd prime, and let $f(x_1,\cdots,x_n) \in \mathbb{F}_p[x_1,\cdots,x_n]$ be a polynomial in n variables. Define $\eta : I_{p-1}^n \to \{-1,+1\}$ by*

$$\eta(x_1,\cdots,x_n) = \begin{cases} +1 & \text{if } (f(x_1)\cdots f(x_n),p) = 1 \\ & \quad \text{and } 0 \le R_p(\operatorname{ind}(f(x_1)\cdots f(x_n)) + \overline{x_1\cdots x_n}) \le \frac{p-1}{2}, \\ -1 & \text{otherwise,} \end{cases}$$

where $R_p(z)$ denotes the unique $r \in \{0, 1, \cdots, p-1\}$ such that $z \equiv r (\mathrm{mod}\ p)$. Then we have

$$\mathbb{Q}_k(\eta) \ll 2^k k \deg(f) p^{n-\frac{1}{2}} (\log p)^{2k+1}.$$

2. Proof of Theorem 1.1, Corollary 1.1 and Theorem 1.2.

We need the following lemmas.

Lemma 2.1. *Let p be a prime number, and let χ be a non-principal character modulo p of order d. Suppose that $f(x) \in \mathbb{F}_p[x]$ has s distinct roots in $\overline{\mathbb{F}}_p$, and $f(x)$ is not the constant multiple of the d-th power of a polynomial over $\mathbb{F}_p$. Let y be real number with $0 < y \leq p$. Then for any $x \in \mathbb{R}$ we have*

$$\left| \sum_{x<n\leq x+y} \chi(f(n)) \right| \leq 9sp^{\frac{1}{2}} \log p.$$

Proof. This is Lemma 2 in [7]. □

Lemma 2.2. *Let p be a prime number, and let $1 \leq d \leq p-1$ with $d \mid p-1$. Then*

$$\sum_{\substack{\chi \bmod p \\ \chi \neq \chi_0 \\ \chi^d = \chi_0}} \left| \sum_{l=1}^{\frac{p-1}{2}} \chi\left(g^l\right) \right| \leq 2d \log(d+1).$$

Proof. This is Lemma 3 in [7]. □

Lemma 2.3. *Suppose that p is a prime number and $1 \leq \delta_1, \cdots, \delta_k \leq p-2$, $0 \leq d_1 < d_2 < \cdots < d_k < p$ are integers. Let $a_1, \cdots, a_s \in \mathbb{F}_p$ be distinct numbers and let*

$$h(x) = (x - a_1) \cdots (x - a_s).$$

If one of the following two conditions holds:

(i) $\min\{s, k\} \leq 2$ *and* $\max\{s, k\} \leq p-1$,

(ii) $(4k)^s \leq p$ *or* $(4s)^k \leq p$,

then the polynomial

$$H(x) = h(x + d_1)^{p-1-\delta_1} \cdots h(x + d_k)^{p-1-\delta_k}$$

has a $(p-1-\delta_u)$-th root in $\mathbb{F}_p$.

Proof. From

$$H(x) = \Big((x + d_1 - a_1) \cdots (x + d_1 - a_s)\Big)^{p-1-\delta_1} \times \cdots \times \Big((x + d_k - a_1) \cdots (x + d_k - a_s)\Big)^{p-1-\delta_k},$$

we have if there exists a c such that

$$d_i - a_j = c, \qquad i \in \{1, \cdots, k\}, j \in \{1, \cdots, s\},$$

has exactly one solution which is (d_u, a_v) for some $1 \le u \le k, 1 \le v \le s$, then $a_v - d_u$ is a $(p-1-\delta_u)$-th root of the function $H(x)$.

Consider the sets $\mathcal{A} = \{a_1, a_2, \ldots, a_s\}, \mathcal{D} = \{d_1, d_2, \ldots, d_k\}$. It was proved in [17, Theorem 2] that under any of the following conditions:

(i) $\min\{s, k\} \le 2$ and $\max\{s, k\} \le p-1$,

(ii) $(4k)^s \le p$ or $(4s)^k \le p$,

there is a $c \in \mathbb{Z}_p$ such that

$$a + d = c \quad a \in \mathcal{A}, d \in \mathcal{D}$$

has exactly one solution. Thus the statement of the lemma follows easily from this. □

Now we prove Theorem 1.1. For $1 \le n \le p-1$ with $(f(n)+\overline{n}, p) = 1$ we have

$$\frac{1}{p-1}\sum_{\chi \bmod p}\sum_{l=1}^{\frac{p-1}{2}}\overline{\chi}\left(g^l\right)\chi\left(f(n)+\overline{n}\right) = \begin{cases} 1, & \text{if } 1 \le \operatorname{ind}\left(f(n)+\overline{n}\right) \le \frac{p-1}{2}, \\ 0, & \text{otherwise.} \end{cases}$$

Therefore

$$\begin{aligned} e_n &= \frac{2}{p-1}\sum_{\chi \bmod p}\sum_{l=1}^{\frac{p-1}{2}}\overline{\chi}\left(g^l\right)\chi\left(f(n)+\overline{n}\right) - 1 \\ &= \frac{2}{p-1}\sum_{\substack{\chi \bmod p \\ \chi \neq \chi_0}}\sum_{l=1}^{\frac{p-1}{2}}\overline{\chi}\left(g^l\right)\chi\left(f(n)+\overline{n}\right). \end{aligned} \tag{2.1}$$

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

$$\sum_{j=0}^{t-1} e_{a+jb} = \frac{2}{p-1}\sum_{\substack{\chi \bmod p \\ \chi \neq \chi_0}}\sum_{l=1}^{\frac{p-1}{2}}\overline{\chi}\left(g^l\right)\sum_{j=0}^{t-1}\chi\left(f(a+jb)+\overline{a+jb}\right) + O\left(\deg(f)\right),$$

where the error term equals to the number of n such that $(f(n)+\overline{n}, p) > 1$. Write $\delta = \operatorname{ord}\chi$. From Lemma 2.1 we have

$$\sum_{j=0}^{t-1}\chi\left(f(a+jb)+\overline{a+jb}\right) = \sum_{j=0}^{t-1}\chi\left((a+jb)^\delta f(a+jb)+(a+jb)^{\delta-1}\right) \ll \deg(f)p^{\frac{1}{2}}\log p, \tag{2.2}$$

since the polynomial $(a+jb)^\delta f(a+jb)+(a+jb)^{\delta-1}$ has a zero $j = -a\overline{b}$ of order $\delta - 1$. Hence from Lemma 2.2 we get

$$\sum_{j=0}^{t-1} e_{a+jb} \ll \frac{1}{p-1}\sum_{\substack{\chi \bmod p \\ \chi \neq \chi_0}}\left|\sum_{l=1}^{\frac{p-1}{2}}\overline{\chi}\left(g^l\right)\right| \deg(f)p^{\frac{1}{2}}\log p \ll \deg(f)p^{\frac{1}{2}}(\log p)^2.$$

Therefore

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

Now we consider the correlation measure of E_{p-1}. We suppose that the congruence $xf(x)+1\equiv 0\pmod p$ has no solution. For $0\le d_1<\cdots<d_k\le p-1-M$, from (2.1) we have

$$\begin{aligned}&\sum_{n=1}^{M}e_{n+d_1}\cdots e_{n+d_k}\\&=\frac{2^k}{(p-1)^k}\sum_{\substack{\chi_1 \bmod p\\ \chi_1\neq\chi_0}}\sum_{l_1=1}^{\frac{p-1}{2}}\overline{\chi}_1\left(g^{l_1}\right)\cdots\sum_{\substack{\chi_k \bmod p\\ \chi_k\neq\chi_0}}\sum_{l_k=1}^{\frac{p-1}{2}}\overline{\chi}_k\left(g^{l_k}\right)\\&\times\sum_{n=1}^{M}\chi_1\left(f(n+d_1)+\overline{n+d_1}\right)\cdots\chi_k\left(f(n+d_k)+\overline{n+d_k}\right)+O\left(k\deg(f)\right).\end{aligned}\tag{2.3}$$

Let χ^* be a generator of the group modulo p characters, and let

$$\chi_u=(\chi^*)^{\delta_u},\qquad 1\le\delta_u\le p-2\qquad\text{for}\qquad u\in\{1,2,\cdots,k\}.\tag{2.4}$$

Then

$$\begin{aligned}&\sum_{n=1}^{M}\chi_1\left(f(n+d_1)+\overline{n+d_1}\right)\cdots\chi_k\left(f(n+d_k)+\overline{n+d_k}\right)\\&=\sum_{n=1}^{M}\chi^*\left(\left(f(n+d_1)+\overline{n+d_1}\right)^{\delta_1}\cdots\left(f(n+d_k)+\overline{n+d_k}\right)^{\delta_k}\right)\\&=\sum_{n=1}^{M}\chi^*\left(((n+d_1)f(n+d_1)+1)^{\delta_1}(n+d_1)^{p-1-\delta_1}\cdots((n+d_k)f(n+d_k)+1)^{\delta_k}(n+d_k)^{p-1-\delta_k}\right).\end{aligned}$$

Since $xf(x)+1\equiv 0\pmod p$ has no solution, $-d_u$ is the $(p-1-\delta_u)$-th zero of the polynomial

$$((n+d_1)f(n+d_1)+1)^{\delta_1}(n+d_1)^{p-1-\delta_1}\cdots((n+d_k)f(n+d_k)+1)^{\delta_k}(n+d_k)^{p-1-\delta_k}$$

for $u=1,2,\cdots,k$. Thus this function is not the constant multiple of the $(p-1)$-th power of a polynomial over $\mathbb{F}_p$, from Lemma 2.1 we get

$$\sum_{n=1}^{M}\chi_1\left(f(n+d_1)+\overline{n+d_1}\right)\cdots\chi_k\left(f(n+d_k)+\overline{n+d_k}\right)\ll k\deg(f)p^{\frac{1}{2}}\log p.\tag{2.5}$$

Combining (2.3), (2.5) and Lemma 2.2 we have

$$\sum_{n=1}^{M}e_{n+d_1}\cdots e_{n+d_k}\ll\frac{2^k}{(p-1)^k}\left(\sum_{\substack{\chi \bmod p\\ \chi\neq\chi_0}}\left|\sum_{l=1}^{\frac{p-1}{2}}\overline{\chi}\left(g^l\right)\right|\right)^k k\deg(f)p^{\frac{1}{2}}\log p\ll 2^k k\deg(f)p^{\frac{1}{2}}(\log p)^{k+1}.$$

Therefore

$$C_k\left(E_{p-1}\right) = \max_{M,D}\left|\sum_{n=1}^{M} e_{n+d_1}e_{n+d_2}\cdots e_{n+d_k}\right| \ll 2^k k\deg(f)p^{\frac{1}{2}}(\log p)^{k+1}.$$

This proves Theorem 1.1.

Now we prove Corollary 1.1. From $f(x) = xg^2(x)$ we get $xf(x) = (xg(x))^2$. Since -1 is a quadratic non-residue modulo p for $p \equiv 3 \pmod 4$, the congruence $xf(x) + 1 \equiv 0 \pmod p$ has no solution. So, from Theorem 1.1, we conclude that

$$W\left(E_{p-1}\right) \ll \deg(f)p^{\frac{1}{2}}(\log p)^2,$$
$$C_k\left(E_{p-1}\right) \ll 2^k k\deg(f)p^{\frac{1}{2}}(\log p)^{k+1}.$$

This completes the proof of Corollary 1.1.

Now we prove Theorem 1.2. For $1 \le n \le p-1$ with $\left(f(n) + \frac{g(n)}{(n-a_1)\cdots(n-a_s)}, p\right) = 1$, we have

$$\begin{aligned}&\frac{1}{p-1}\sum_{\chi \bmod p}\sum_{l=1}^{\frac{p-1}{2}}\overline{\chi}\left(g^l\right)\chi\left(f(n) + \frac{g(n)}{(n-a_1)\cdots(n-a_s)}\right)\\ &= \begin{cases} 1, & \text{if } 1 \le \operatorname{ind}\left(f(n) + \frac{g(n)}{(n-a_1)\cdots(n-a_s)}\right) \le \frac{p-1}{2},\\ 0, & \text{otherwise.}\end{cases}\end{aligned}$$

Therefore

$$\begin{aligned} e_n &= \frac{2}{p-1}\sum_{\chi \bmod p}\sum_{l=1}^{\frac{p-1}{2}}\overline{\chi}\left(g^l\right)\chi\left(f(n) + \frac{g(n)}{(n-a_1)\cdots(n-a_s)}\right) - 1\\ &= \frac{2}{p-1}\sum_{\substack{\chi \bmod p\\ \chi \ne \chi_0}}\sum_{l=1}^{\frac{p-1}{2}}\overline{\chi}\left(g^l\right)\chi\left(f(n) + \frac{g(n)}{(n-a_1)\cdots(n-a_s)}\right)\end{aligned}$$

and then

$$\begin{aligned}\sum_{j=0}^{t-1} e_{a+jb} &= \frac{2}{p-1}\sum_{\substack{\chi \bmod p\\ \chi \ne \chi_0}}\sum_{l=1}^{\frac{p-1}{2}}\overline{\chi}\left(g^l\right)\sum_{j=0}^{t-1}\chi\left(f(a+jb) + \frac{g(a+jb)}{(a+jb-a_1)\cdots(a+jb-a_s)}\right)\\ &\quad + O\left(\deg(f) + \deg(g) + s\right),\end{aligned}$$

where the error term equals to the number of n such that $\left(f(n) + \frac{g(n)}{(n-a_1)\cdots(n-a_s)}, p\right) > 1$. Since $\gcd(g(n), (n-a_1)\cdots(n-a_s)) = 1$ and $\delta = \operatorname{ord}\chi$, we obtain the following estimate similar to (2.2).

$$\begin{aligned}&\sum_{j=0}^{t-1}\chi\left(f(a+jb) + \frac{g(a+jb)}{(a+jb-a_1)\cdots(a+jb-a_s)}\right)\\ &= \sum_{j=0}^{t-1}\chi\left(((a+jb-a_1)\cdots(a+jb-a_s))^{\delta}f(a+jb)\right)\end{aligned}$$

$$+((a+jb-a_1)\cdots(a+jb-a_s))^{\delta-1}g(a+jb)\Big)$$
$$\ll (\deg(f)+\deg(g)+s)\,p^{\frac{1}{2}}\log p.$$

Hence from Lemma 2.2 we get

$$\begin{aligned}\sum_{j=0}^{t-1}e_{a+jb} &\ll \frac{1}{p-1}\sum_{\substack{\chi \bmod p\\ \chi\neq\chi_0}}\left|\sum_{l=1}^{\frac{p-1}{2}}\overline{\chi}\left(g^l\right)\right|(\deg(f)+\deg(g)+s)\,p^{\frac{1}{2}}\log p\\ &\ll (\deg(f)+\deg(g)+s)\,p^{\frac{1}{2}}(\log p)^2.\end{aligned}$$

Therefore

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

According to (2.3) and (2.4) we get a similar equality for the correlation measure of E_p that

$$\begin{aligned}&\sum_{n=1}^{M}e_{n+d_1}\cdots e_{n+d_k}\\ =\;&\frac{2^k}{(p-1)^k}\sum_{\substack{\chi_1 \bmod p\\ \chi_1\neq\chi_0}}\sum_{l_1=1}^{\frac{p-1}{2}}\overline{\chi}_1\left(g^{l_1}\right)\cdots\sum_{\substack{\chi_k \bmod p\\ \chi_k\neq\chi_0}}\sum_{l_k=1}^{\frac{p-1}{2}}\overline{\chi}_k\left(g^{l_k}\right)\\ &\times\sum_{n=1}^{M}\chi_1\left(f(n+d_1)+\frac{g(n+d_1)}{(n+d_1+a_1)\cdots(n+d_1-a_s)}\right)\\ &\quad\times\cdots\times\chi_k\left(f(n+d_k)+\frac{g(n+d_k)}{(n+d_k+a_1)\cdots(n+d_k-a_s)}\right)\\ &+O\left(k(\deg(f)+\deg(g)+s)\right)\\ =\;&\frac{2^k}{(p-1)^k}\sum_{\substack{\chi_1 \bmod p\\ \chi_1\neq\chi_0}}\sum_{l_1=1}^{\frac{p-1}{2}}\overline{\chi}_1\left(g^{l_1}\right)\cdots\sum_{\substack{\chi_k \bmod p\\ \chi_k\neq\chi_0}}\sum_{l_k=1}^{\frac{p-1}{2}}\overline{\chi}_k\left(g^{l_k}\right)\\ &\times\sum_{n=1}^{M}\chi^*\Big(((n+d_1-a_1)\cdots(n+d_1-a_s)f(n+d_1)+g(n+d_1))^{\delta_1}\\ &\qquad\times((n+d_1-a_1)\cdots(n+d_1-a_s))^{p-1-\delta_1}\Big)\\ &\quad\times\cdots\times\chi^*\Big(((n+d_k-a_1)\cdots(n+d_k-a_s)f(n+d_k)+g(n+d_k))^{\delta_k}\\ &\qquad\times((n+d_k-a_1)\cdots(n+d_k-a_s))^{p-1-\delta_k}\Big)\\ &+O\left(k(\deg(f)+\deg(g)+s)\right).\end{aligned}$$

We assume that $(x-a_1)\cdots(x-a_s)f(x)+g(x)\equiv 0 \pmod p$ has no solution, thus from this and Lemma 2.3 we obtain that the function

$$
\begin{aligned}
&((n+d_1-a_1)\cdots(n+d_1-a_s)f(n+d_1)+g(n+d_1))^{\delta_1}\,((n+d_1-a_1)\cdots(n+d_1-a_s))^{p-1-\delta_1}\\
&\times\cdots\times((n+d_k-a_1)\cdots(n+d_k-a_s)f(n+d_k)+g(n+d_k))^{\delta_k}\\
&\times((n+d_k-a_1)\cdots(n+d_k-a_s))^{p-1-\delta_k}\\
=\;&((n+d_1-a_1)\cdots(n+d_1-a_s)f(n+d_1)+g(n+d_1))^{\delta_1}\\
&\times\cdots\times((n+d_k-a_1)\cdots(n+d_k-a_s)f(n+d_k)+g(n+d_k))^{\delta_k}\times H(n)
\end{aligned}
$$

has a $(p-1-\delta_u)$-th root in $\mathbb{F}_p$. Then this function is not the constant multiple of the $(p-1)$-th power of a polynomial over $\mathbb{F}_p$, so from Lemmas 2.1 and 2.2 we have

$$
\begin{aligned}
&\sum_{n=1}^{M} e_{n+d_1}\cdots e_{n+d_k}\\
\ll\;&\frac{2^k}{(p-1)^k}\left(\sum_{\substack{\chi \bmod p\\ \chi\neq\chi_0}}\left|\sum_{l=1}^{\frac{p-1}{2}}\overline{\chi}\left(g^l\right)\right|\right)^k k(\deg(f)+\deg(g)+s)p^{\frac{1}{2}}\log p\\
\ll\;&2^k k(\deg(f)+\deg(g)+s)p^{\frac{1}{2}}(\log p)^{k+1}.
\end{aligned}
$$

Therefore,

$$
\begin{aligned}
C_k\left(E_p\right) =\;& \max_{M,D}\left|\sum_{n=1}^{M} e_{n+d_1}e_{n+d_2}\cdots e_{n+d_k}\right|\\
\ll\;&2^k k(\deg(f)+\deg(g)+s)p^{\frac{1}{2}}(\log p)^{k+1}.
\end{aligned}
$$

This proves Theorem 1.2.

3. Estimate of mixed exponential sums and proof of Theorem 1.3

We need the following estimates for mixed exponential sums to prove Theorem 1.2.

Lemma 3.1. *Let p be a prime number. Let ψ be a nontrivial additive character and χ a multiplicative character of $\mathbb{F}_p$ of order d. Furthermore, let $F=\frac{f}{g}$, $Q=\frac{q}{r}$ be non-zero rational functions over $\mathbb{F}_p$ and let s be the number of distinct zeros of g in $\overline{\mathbb{F}}_p$. Assume that $\mathcal{S}$ is the set of poles of F and Q. If one of the following conditions holds:*

(i) $g(x)\nmid f(x)$,

(ii) *$Q(x)$ is not of the form $bB(x)^d$ for any $b\in\mathbb{F}_p$ and $B(x)\in\mathbb{F}_p(x)$.*

If $1\le N<p$, then we have

$$
\left|\sum_{\substack{0\le n<N\\ n\notin\mathcal{S}}}\psi(F(n))\chi(Q(n))\right|\le 3(\max\{\deg(f),\deg(g)\}+s+\deg(q)+\deg(r))p^{1/2}\log p. \tag{3.1}
$$

Proof. See Theorem 5 in [18]. □

Lemma 3.2. *Assume that $p > 2$ is a prime, $\delta_1, \cdots, \delta_k$ are integers, and χ^* is a generator of the group of characters modulo p. Let $u_1, \cdots, u_k$ be integers with $(u_1 \cdots u_k, p) = 1$, and let*

$$\mathbf{d}_1 = (d_{11}, \cdots, d_{1n}), \cdots, \mathbf{d}_k = (d_{k1}, \cdots, d_{kn})$$

be distinct vectors whose coordinates are integers. Suppose that $f(x) \in \mathbb{F}_p[x]$. Let $1 \le N < p$. For any integers $1 \le t_1, \cdots, t_n < N$ and $1 \le b_1, \cdots, b_n < p$, define

$$\begin{aligned}\Psi \;=\; & \sum_{\substack{j_1=0 \\ ((j_1b_1+d_{11})\cdots(j_1b_1+d_{k1}),\ p)=1}}^{t_1} \cdots \sum_{\substack{j_n=0 \\ ((j_nb_n+d_{1n})\cdots(j_nb_n+d_{kn}),\ p)=1}}^{t_n} \\ & \times\chi^*\left(f(j_1b_1+d_{11})^{\delta_1}\cdots f(j_nb_n+d_{1n})^{\delta_1}\cdots f(j_1b_1+d_{k1})^{\delta_k}\cdots f(j_nb_n+d_{kn})^{\delta_k}\right) \\ & \times e\left(\frac{u_1\overline{j_1b_1+d_{11}}\cdots\overline{j_nb_n+d_{1n}}+\cdots+u_k\overline{j_1b_1+d_{k1}}\cdots\overline{j_nb_n+d_{kn}}}{p}\right).\end{aligned}$$

Then we have

$$\Psi \ll k\deg(f)p^{n-\frac{1}{2}}\log p.$$

Proof. This lemma can be proved by using the methods in [15] with slight modifications. For a completeness we give detailed proof. Without loss of generality, we may assume that $d_{11}, \cdots, d_{k1}$ are not the same, since $\mathbf{d}_1, \cdots, \mathbf{d}_k$ are distinct. If there are l distinct elements in $\{d_{11}, \cdots, d_{k1}\}$, we find that

$$\{d_{11}, \cdots, d_{k1}\} = \{d_{i_11}, \cdots, d_{i_l1}\},$$

where $d_{i_11}, \cdots, d_{i_l1}$ are distinct. Then

$$\begin{aligned}& u_1\overline{x_1+d_{11}}\cdots\overline{x_n+d_{1n}}+\cdots+u_k\overline{x_1+d_{k1}}\cdots\overline{x_n+d_{kn}} \\ &= \left(\sum_{\substack{j=1 \\ d_{j1}=d_{i_1}1}}^{k} u_j\overline{x_2+d_{j2}}\cdots\overline{x_n+d_{jn}}\right)\overline{x_1+d_{i_11}}+\cdots+\left(\sum_{\substack{j=1 \\ d_{j1}=d_{i_l}1}}^{k} u_j\overline{x_2+d_{j2}}\cdots\overline{x_n+d_{jn}}\right)\overline{x_1+d_{i_l1}}.\end{aligned}$$

Let

$$a_{i_1} = \sum_{\substack{j=1 \\ d_{j1}=d_{i_1}1}}^{k} u_j\overline{x_2+d_{j2}}\cdots\overline{x_n+d_{jn}}, \ldots, a_{i_l} = \sum_{\substack{j=1 \\ d_{j1}=d_{i_l}1}}^{k} u_j\overline{x_2+d_{j2}}\cdots\overline{x_n+d_{jn}},$$

and define

$$\begin{aligned}\Delta \;=\; & \Big\{(x_2,\ldots,x_n)\in\mathbb{B} : ((x_2+d_{12})\cdots(x_2+d_{k2}),p)=1,\ldots,((x_n+d_{1n}) \\ & \cdots(x_n+d_{kn}),p)=1, p\nmid \sum_{\substack{j=1 \\ d_{j1}=d_{i_1}1}}^{k} u_j\overline{x_2+d_{j2}}\cdots\overline{x_n+d_{jn}}\end{aligned}$$

$$,\ldots,p\nmid \sum_{\substack{j=1\\ d_{j1}=d_{i_j1}}}^{k} u_j\overline{x_2+d_{j2}}\cdots\overline{x_n+d_{jn}}\Big\},$$

where

$$\mathbb{B}=\{(x_2,\cdots,x_n)\mid x_i=j_ib_i,\ 0\le j_i\le t_i,\ i=2,\cdots,n.\}.$$

It is not hard to see that

$$|\Delta|\le p^{n-1}+O\left(kp^{n-2}\right),$$

where the error term equals to the number of vectors $(x_2,\cdots,x_n)$ such that

$$\left((x_2+d_{12})\cdots(x_2+d_{k2}),p\right)>1.$$

Then we have

$$\begin{aligned}\Psi &= \sum_{\substack{x_2=0\\ (x_2,\ldots,x_n)\in\Delta}}^{p-1}\cdots\sum_{x_n=0}^{p-1}\chi^*\left(f(x_2+d_{12})^{\delta_1}\cdots f(x_2+d_{k2})^{\delta_k}\right)\cdots\chi^*\left(f(x_n+d_{1n})^{\delta_1}\cdots f(x_n+d_{kn})^{\delta_k}\right)\\ &\quad\times\sum_{\substack{j_1=0\\ ((j_1b_1+d_{11})\cdots(j_1b_1+d_{k1}),p)=1}}^{t_1}\chi^*\left(f(j_1b_1+d_{11})^{\delta_1}\cdots f(j_1b_1+d_{k1})^{\delta_k}\right)\\ &\quad\times e\left(\frac{a_{i_1}\overline{j_1b_1+d_{i_11}}+\cdots+a_{i_l}\overline{j_1b_1+d_{i_l1}}}{p}\right)\\ &\quad+O\left(kp^{n-1}\right).\end{aligned}$$

Define

$$z(x_1)=(x_1+d_{i_11})\cdots(x_1+d_{i_l1}),$$

and

$$g(x_1)=\sum_{j=1}^{l}a_{i_j}\prod_{\substack{m=1\\ m\ne j}}^{l}(x_1+d_{i_m1}).$$

We get

$$\begin{aligned}&\sum_{\substack{j_1=0\\ ((j_1b_1+d_{11})\cdots(j_1b_1+d_{k1}),p)=1}}^{t_1}\chi^*\left(f(j_1b_1+d_{11})^{\delta_1}\cdots f(j_1b_1+d_{k1})^{\delta_k}\right)\\ &\quad\times e\left(\frac{a_{i_1}\overline{j_1b_1+d_{i_11}}+\cdots+a_{i_l}\overline{j_1b_1+d_{i_l1}}}{p}\right)\\ &=\sum_{\substack{j_1=0\\ ((j_1b_1+d_{11})\cdots(j_1b_1+d_{k1}),p)=1}}^{t_1}\chi^*\left(f(j_1b_1+d_{11})^{\delta_1}\cdots f(j_1b_1+d_{k1})^{\delta_k}\right)e\left(\frac{g(j_1b_1)}{z(j_1b_1)p}\right).\end{aligned}$$

Since $-d_{i_1 1}, \ldots, -d_{i_l 1}$ are not zeros of $g(x)$, we have $z(x) \nmid g(x)$. There exist at most $k\deg(f)$ different roots for the function $f(j_1b_1+d_{11})^{\delta_1}\cdots f(j_1b_1+d_{k1})^{\delta_k}$. Thus we can use Lemma 3.1 to get

$$\begin{aligned}
&\sum_{\substack{j_1=0\\((j_1b_1+d_{11})\cdots(j_1b_1+d_{k1}),p)=1}}^{t_1} \chi^*\left(f(j_1b_1+d_{11})^{\delta_1}\cdots f(j_1b_1+d_{k1})^{\delta_k}\right)\\
&\times e\left(\frac{a_{i_1}\overline{j_1b_1+d_{i_1 1}}+\cdots+a_{i_l}\overline{j_1b_1+d_{i_l 1}}}{p}\right)\\
&\ll k\deg(f)p^{\frac{1}{2}}\log p,
\end{aligned}$$

Therefore,

$$\Psi \ll k\deg(f)p^{n-\frac{1}{2}}\log p.$$

This completes the proof of Lemma 3.2. □

Now we prove Theorem 1.3. For $x_1, \cdots, x_n$ with $(f(x_1)\cdots f(x_n), p) = 1$ we have

$$\begin{aligned}
&\frac{2}{p}\sum_{v=0}^{\frac{p-1}{2}}\sum_{u=0}^{p-1} e\left(\frac{u(\mathrm{ind}\,(f(x_1)\cdots f(x_n))+\overline{x_1\cdots x_n}-v)}{p}\right)-1\\
&=\begin{cases} 1, & \text{if } 0\le R_p\,(\mathrm{ind}\,(f(x_1)\cdots f(x_n))+\overline{x_1\cdots x_n})\le\frac{p-1}{2},\\ -1, & \text{otherwise.}\end{cases}
\end{aligned}$$

Therefore

$$\begin{aligned}
&\eta(x_1,\cdots,x_n)\\
&=\frac{2}{p}\sum_{v=0}^{\frac{p-1}{2}}\sum_{u=0}^{p-1} e\left(\frac{u(\,\mathrm{ind}\,(f(x_1)\cdots f(x_n))+\overline{x_1\cdots x_n}-v)}{p}\right)-1\\
&=\frac{2}{p}\sum_{u=1}^{p-1}\left(\sum_{v=0}^{\frac{p-1}{2}} e\left(-\frac{uv}{p}\right)\right) e\left(\frac{u\,\mathrm{ind}\,(f(x_1)\cdots f(x_n))}{p}\right) e\left(\frac{u\overline{x_1\cdots x_n}}{p}\right)+\frac{1}{p}\\
&=\frac{2}{p(p-1)}\sum_{u=1}^{p-1}\left(\sum_{v=0}^{\frac{p-1}{2}} e\left(-\frac{uv}{p}\right)\right)\sum_{\chi}\sum_{\mathrm{mod}\ p}\sum_{l=0}^{p-2}\overline{\chi}(g^l)e\left(\frac{ul}{p}\right)\chi\left(f(x_1)\cdots f(x_n)\right) e\left(\frac{u\overline{x_1\cdots x_n}}{p}\right)+\frac{1}{p}. \quad (3.2)
\end{aligned}$$

Let $b_1, \cdots, b_n$ be positive integers, and write $\mathbf{d}_i = (d_{i1}, \cdots, d_{in})$ for $i \in \{1, \cdots, k\}$. By (3.2) we get

$$\begin{aligned}
&\sum_{j_1=0}^{t_1}\cdots\sum_{j_n=0}^{t_n}\eta\left(j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_1\right)\cdots\eta\left(j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_k\right)\\
&=\sum_{j_1=0}^{t_1}\cdots\sum_{j_n=0}^{t_n}\eta\left(j_1b_1+d_{11},\cdots,j_nb_n+d_{1n}\right)\cdots\eta\left(j_1b_1+d_{k1},\cdots,j_nb_n+d_{kn}\right)\\
&=\frac{2^k}{p^k(p-1)^k}\sum_{u_1=1}^{p-1}\left(\sum_{v_1=0}^{\frac{p-1}{2}} e\left(\frac{-u_1v_1}{p}\right)\right)\cdots\sum_{u_k=1}^{p-1}\left(\sum_{v_k=0}^{\frac{p-1}{2}} e\left(\frac{-u_kv_k}{p}\right)\right)
\end{aligned}$$

$$\times \sum_{\chi_1 \bmod p} \sum_{l_1=0}^{p-2} \overline{\chi}_1(g^{l_1}) e\left(\frac{u_1 l_1}{p}\right) \cdots \sum_{\chi_k \bmod p} \sum_{l_k=0}^{p-2} \overline{\chi}_k(g^{l_k}) e\left(\frac{u_k l_k}{p}\right)$$

$$\times \sum_{\substack{j_1=0 \\ ((j_1b_1+d_{11})\cdots(j_1b_1+d_{k1}),\ p)=1}}^{t_1} \cdots \sum_{\substack{j_n=0 \\ ((j_nb_n+d_{1n})\cdots(j_nb_n+d_{kn}),\ p)=1}}^{t_n}$$

$$\times \chi_1\left(f(j_1b_1+d_{11})\cdots f(j_nb_n+d_{1n})\right)\cdots\chi_k\left(f(j_1b_1+d_{k1})\cdots f(j_nb_n+d_{kn})\right)$$

$$\times e\left(\frac{u_1\overline{j_1b_1+d_{11}}\cdots\overline{j_nb_n+d_{1n}}+\cdots+u_k\overline{j_1b_1+d_{k1}}\cdots\overline{j_nb_n+d_{kn}}}{p}\right)$$

$$+O\left(k\deg(f)p^{n-1}\right). \tag{3.3}$$

Let χ^* be a generator of the group of characters modulo p, and let $\chi_u = (\chi^*)^{\delta_u}$, where $1 \le \delta_u \le p-1$ for $u \in \{1, 2, \cdots, k\}$. From Lemma 3.2 we have

$$\sum_{\substack{j_1=0 \\ ((j_1b_1+d_{11})\cdots(j_1b_1+d_{k1}),\ p)=1}}^{t_1} \cdots \sum_{\substack{j_n=0 \\ ((j_nb_n+d_{1n})\cdots(j_nb_n+d_{kn}),\ p)=1}}^{t_n}$$

$$\times \chi_1\left(f(j_1b_1+d_{11})\cdots f(j_nb_n+d_{1n})\right)\cdots\chi_k\left(f(j_1b_1+d_{k1})\cdots f(j_nb_n+d_{kn})\right)$$

$$\times e\left(\frac{u_1\overline{j_1b_1+d_{11}}\cdots\overline{j_nb_n+d_{1n}}+\cdots+u_k\overline{j_1b_1+d_{k1}}\cdots\overline{j_nb_n+d_{kn}}}{p}\right)$$

$$= \sum_{\substack{j_1=0 \\ ((j_1b_1+d_{11})\cdots(j_1b_1+d_{k1}),\ p)=1}}^{t_1} \cdots \sum_{\substack{j_n=0 \\ ((j_nb_n+d_{1n})\cdots(j_nb_n+d_{kn}),\ p)=1}}^{t_n}$$

$$\times \chi^*\left(f(j_1b_1+d_{11})^{\delta_1}\cdots f(j_nb_n+d_{1n})^{\delta_1}\cdots f(j_1b_1+d_{k1})^{\delta_k}\cdots f(j_nb_n+d_{kn})^{\delta_k}\right)$$

$$\times e\left(\frac{u_1\overline{j_1b_1+d_{11}}\cdots\overline{j_nb_n+d_{1n}}+\cdots+u_k\overline{j_1b_1+d_{k1}}\cdots\overline{j_nb_n+d_{kn}}}{p}\right)$$

$$\ll k\deg(f)p^{n-\frac{1}{2}}\log p. \tag{3.4}$$

Then combining (3.3) and (3.4) we get

$$\sum_{j_1=0}^{t_1}\cdots\sum_{j_n=0}^{t_n}\eta\left(j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_1\right)\cdots\eta\left(j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_k\right)$$

$$\ll \frac{2^k}{p^k(p-1)^k}\sum_{u_1=1}^{p-1}\left|\sum_{v_1=0}^{\frac{p-1}{2}} e\left(\frac{-u_1v_1}{p}\right)\right|\cdots\sum_{u_k=1}^{p-1}\left|\sum_{v_k=0}^{\frac{p-1}{2}} e\left(\frac{-u_kv_k}{p}\right)\right|$$

$$\times \sum_{\chi_1 \bmod p}\left|\sum_{l_1=0}^{p-2}\overline{\chi}_1(g^{l_1})e\left(\frac{u_1l_1}{p}\right)\right|\cdots\sum_{\chi_k \bmod p}\left|\sum_{l_k=0}^{p-2}\overline{\chi}_k(g^{l_k})e\left(\frac{u_kl_k}{p}\right)\right|$$

$$\times k\deg(f)p^{n-\frac{1}{2}}\log p$$

$$\ll \frac{1}{p^k(p-1)^k}\sum_{u_1=1}^{p-1}\frac{1}{\left\langle\frac{u_1}{p}\right\rangle}\sum_{\chi_1 \bmod p}\left|\sum_{l_1=0}^{p-2}\overline{\chi}_1(g^{l_1})e\left(\frac{u_1l_1}{p}\right)\right|$$

$$\times\cdots\times\sum_{u_k=1}^{p-1}\frac{1}{\left\langle\frac{u_k}{p}\right\rangle}\sum_{\chi_k \bmod p}\left|\sum_{l_k=0}^{p-2}\overline{\chi}_k(g^{l_k})e\left(\frac{u_k l_k}{p}\right)\right|$$
$$\times 2^k k\deg(f)p^{n-\frac{1}{2}}\log p, \tag{3.5}$$

where $\langle\theta\rangle = \min(\theta - \lfloor\theta\rfloor,\ 1-(\theta-\lfloor\theta\rfloor))$ denotes the distance from θ to nearest integer. Noting that

$$\begin{aligned}
&\sum_{\chi \bmod p}\left|\sum_{l=0}^{p-2}\overline{\chi}(g^l)e\left(\frac{ul}{p}\right)\right| \\
=\ &\sum_{m=0}^{p-2}\left|\sum_{l=0}^{p-2}e\left(\frac{m\mathrm{ind}\, g^l}{p-1}\right)e\left(\frac{ul}{p}\right)\right| \\
=\ &\sum_{m=0}^{p-2}\left|\sum_{l=0}^{p-2}e\left(\frac{ml}{p-1}+\frac{ul}{p}\right)\right| \\
\ll\ &\sum_{m=0}^{p-2}\frac{1}{\left\langle\frac{m}{p-1}+\frac{u}{p}\right\rangle}\ll (p-1)\log(p-1).
\end{aligned} \tag{3.6}$$

Combining (3.5) and (3.6) we obtain

$$\begin{aligned}
&\sum_{j_1=0}^{t_1}\cdots\sum_{j_n=0}^{t_n}\eta(j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_1)\cdots\eta(j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_k) \\
\ll\ &2^k k\deg(f)p^{n-\frac{1}{2}}(\log p)^{2k+1}.
\end{aligned}$$

Therefore,

$$\mathbb{Q}_k(\eta)\ll 2^k k\deg(f)p^{n-\frac{1}{2}}(\log p)^{2k+1}.$$

This completes the proof of Theorem 1.3.

4. Conclusions

In this paper, a method is given for the application of primitive characters modulo p and the estimates of both character sums and mixed exponential sums to the estimates of pseudorandom measures. The binary sequences in Theorem 1.1, Corollary 1.1 and Theorem 1.2 are demonstrated to be pseudorandom, since the upper bounds of both the well-distribution measure and the correlation measure of those sequences are $o(p)$ as $p\to\infty$. With the growth of the number of dimensions, the error term of the pseudorandom measure in (3.3) is up to $k\deg(f)p^{n-1}$, thus the result in Theorem 1.3 is the best one by now which is based on Lemma 3.2.

Acknowledgments

The authors express their gratitude to the referee for his/her helpful and detailed comments. This work is supported by National Natural Science Foundation of China under Grant No. 12071368, and the Science and Technology Program of Shaanxi Province of China under Grant No. 2019JM-573 and 2020JM-026.

Conflict of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. C. Mauduit, A. Sárközy, On finite pseudorandom binary sequencs I: Measure of pseudorandomness, the Legendre symbol, *Acta Arith.*, **82** (1997), 365–377. https://doi.org/10.4064/aa-82-4-365-377
2. H. Liu, A family of elliptic curve pseudorandom binary sequences, *Des. Codes Cryptogr.*, **73** (2014), 251–265. https://doi.org/10.1007/s10623-013-9822-7
3. C. Mauduit, J. Rivat, A. Sárközy, Construction of pseudorandom binary sequences using additive characters, *Monatsh. Math.*, **141** (2004), 197–208. https://doi.org/10.1007/s00605-003-0112-8
4. C. Mauduit, A. Sárközy, Construction of pseudorandom binary sequences by using the multiplicative inverse, *Acta Math. Hung.*, **108** (2005), 239–252. https://doi.org/10.1007/s10474-005-0222-y
5. L. Mérai, Remarks on pseudorandom binary sequences over elliptic curves, *Fund. Inform.*, **114** (2012), 301–308. https://doi.org/10.3233/FI-2012-630
6. J. Rivat, A. Sárközy, Modular constructions of pseudorandom binary sequences with composite moduli, *Period. Math. Hung.*, **51** (2006), 75–107. https://doi.org/10.1007/s10998-005-0031-7
7. K. Gyarmati, On a family of pseudorandom binary sequences, *Period. Math. Hung.*, **49** (2005), 45–63. https://doi.org/10.1007/s10998-004-0522-y
8. L. Mérai, A construction of pseudorandom binary sequences using rational functions, *Unif. Distrib. Theory*, **4** (2009), 35–49.
9. P. Hubert, C. Mauduit, A. Sárközy, On pseudorandom binary lattices, *Acta Arith.*, **125** (2006), 51–62. https://doi.org/10.4064/aa125-1-5
10. K. Gyarmati, C. Mauduit, A. Sárközy, Pseudorandom binary sequences and lattices, *Acta Arith.*, **135** (2008), 181–197. https://doi.org/10.4064/aa135-2-6
11. K. Gyarmati, C. Mauduit, A. Sárközy, Constructions of pseudorandom binary lattices, *Unif. Distrib. Theory*, **4** (2009), 59–80.
12. K. Gyarmati, On new measures of pseudorandomness of binary lattices, *Acta Math. Hung.*, **131** (2011), 346–359. https://doi.org/10.1007/s10474-010-0041-7
13. K. Gyarmati, C. Mauduit, A. Sárközy, Measures of pseudorandomness of finite binary lattices, II. (The symmetry measures), *Ramanujan J.*, **25** (2011), 155–178. https://doi.org/10.1007/s11139-010-9255-0
14. K. Gyarmati, C. Mauduit, A. Sárközy, On finite pseudorandom binary lattices, *Discrete Appl. Math.*, **216** (2017), 589–597. https://doi.org/10.1016/j.dam.2015.07.012
15. H. Liu, Large families of pseudorandom binary lattices by using the multiplicative inverse modulo p, *Int. J. Number Theory*, **15** (2019), 527–546. https://doi.org/10.1142/S1793042119500271

16. C. Mauduit, A. Sárközy, Construction of pseudorandom binary lattices by using the multiplicative inverse, *Monatsh. Math.*, **153** (2008), 217–231. https://doi.org/10.1007/s00605-007-0479-z

17. L. Goubin, C. Mauduit, A. Sárközy, Construction of large families of pseudorandom binary sequences, *J. Number Theory*, **106** (2004), 56–69. https://doi.org/10.1016/j.jnt.2003.12.002

18. L. Mérai, A construction of pseudorandom binary sequences using both additive and multiplicative characters, *Acta Arith.*, **139** (2009), 241–252.

AIMS Press