Research Article

Xiaolin Chen*

Constructions of pseudorandom binary lattices using cyclotomic classes in finite fields

https://doi.org/10.1515/math-2020-0086
received November 22, 2019; accepted September 10, 2020

Abstract: In 2006, Hubert, Mauduit and Sárközy extended the notion of binary sequences to \( n \)-dimensional binary lattices and introduced the measures of pseudorandomness of binary lattices. In 2011, Gyarmati, Mauduit and Sárközy extended the notions of family complexity, collision and avalanche effect from binary sequences to binary lattices. In this paper, we construct pseudorandom binary lattices by using cyclotomic classes in finite fields and study the pseudorandom measure of order \( k \), family complexity, collision and avalanche effect. Results indicate that such binary lattices are “good,” and their families possess a nice structure in terms of family complexity, collision and avalanche effect.

Keywords: pseudorandom, binary lattice, cyclotomic class, finite field, character sum

MSC 2020: 11K45, 11B50, 94A55, 94A60

1 Introduction

The need for pseudorandom binary lattices arises in many applications, so numerous papers have been written on this subject. In these papers, some measures are introduced and studied. For example, Hubert, Mauduit and Sárközy [1] extended the notion of binary sequences to \( n \)-dimensional binary lattices and introduced the measures of pseudorandomness of binary lattices. For details, let \( \mathbb{I}_n \) denote the set of \( n \)-dimensional vectors all whose coordinates are in \( \{0, 1, \ldots, N - 1\} \). That is,

\[
\mathbb{I}_n = \{x = (x_1, \ldots, x_n) : x_1, \ldots, x_n \in \{0, 1, \ldots, N - 1\}\}.
\]

A function of the type \( \eta(x) = \eta(x_1, \ldots, x_n) : \mathbb{I}_n \rightarrow \{-1, +1\} \) is called an \( n \)-dimensional binary \( N \)-lattice or briefly a binary lattice.

Let \( k \in \mathbb{N} \), and \( \mathbf{u}_i \ (i = 1, \ldots, n) \) denote the \( n \)-dimensional unit vector whose \( i \)-th coordinate is 1 and the others are 0. Write

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

where the maximum is taken over all \( n \)-dimensional vectors \( \mathbf{B} = (b_1, \ldots, b_n), \mathbf{d}_1, \ldots, \mathbf{d}_k, \mathbf{T} = (t_1, \ldots, t_n) \) such that their coordinates are non-negative integers, \( b_1, \ldots, b_n \) are non-zero, \( \mathbf{d}_1, \ldots, \mathbf{d}_k \) are distinct and all 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 \( \mathbb{I}_n^k \). Then \( Q_k(\eta) \) is called the pseudorandom measure of order \( k \) of \( \eta \).

* Corresponding author: Xiaolin Chen, School of Applied Mathematics, Shanxi University of Finance and Economics, Taiyuan 030006, Shanxi, People’s Republic of China, e-mail: chenxl@sxufe.edu.cn

Open Access. © 2020 Xiaolin Chen, published by De Gruyter. This work is licensed under the Creative Commons Attribution 4.0 International License.
An \( n \)-dimensional binary \( N \)-lattice \( \eta \) is considered as a “good” pseudorandom binary lattice if \( Q_k(\eta) \) is “small” in terms of \( N \) for small \( k \). This terminology is justified since Hubert, Mauduit and Sárközy [1] proved that for a fixed \( k \in \mathbb{N} \) and for a truly random \( n \)-dimensional binary \( N \)-lattice \( \eta \) we have

\[
N^2 \ll Q_k(\eta) \ll N^{2\log N}.
\]

with probability greater than \( 1 - \varepsilon \), while the trivial upper bound for \( Q_k(\eta) \) is \( N^n \).

In 2011, Gyarmati, Mauduit and Sárközy [2] extended the notions of family complexity, collision and avalanche effect from binary sequences to binary lattices.

Assume that \( n, N \in \mathbb{N} \), and \( F \) is a family of \( n \)-dimensional binary \( N \)-lattices \( \eta : I_N^n \rightarrow \{ -1, +1 \} \). Let \( j \leq N^n \), \( x_1, x_2, \ldots, x_j \in I_N^n \) be \( j \) distinct vectors, and \( (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_j) \in \{ -1, +1 \}^j \). The family complexity or \( f \)-complexity of the family \( F \), denoted by \( \Gamma(F) \), is defined as the greatest integer \( j \) such that for any specification of length \( j \), there is at least one \( \eta \in F \) satisfying

\[
\eta(x_1) = \varepsilon_1, \ \eta(x_2) = \varepsilon_2, \ldots, \ \eta(x_j) = \varepsilon_j.
\]

Obviously, we have the trivial bound

\[
\Gamma(F) \leq \frac{\log |F|}{\log 2}.
\]

Assume that \( n, N \in \mathbb{N} \), \( S \) is a given finite set (e.g., a set of certain polynomials), to each \( s \in S \) we assign a unique \( n \)-dimensional binary \( N \)-lattice \( \eta_s : I_N^n \rightarrow \{ -1, +1 \} \), and let \( F = F(S) \) denote the family of the binary lattices obtained in this way:

\[
F = F(S) = \{ \eta_s : s \in S \}.
\]

**Definition 1.1.** If \( s \in S \), \( s' \in S \), \( s \neq s' \), \( \eta_s = \eta_{s'} \), then this is said to be a collision in \( F = F(S) \). If there is no collision in \( F = F(S) \), then \( F \) is said to be collision free.

**Definition 1.2.** If \( F = F(S) \) is of form (1.1), changing any element \( s \in S \) for any \( s' \in S \) with \( s \neq s' \) changes “many” elements of \( \eta_s : I_N^n \rightarrow \{ -1, +1 \} \), then we speak about the avalanche effect, and we say that \( F = F(S) \) possesses the avalanche property. If for any \( s \in S \), \( s' \in S \), \( s \neq s' \), there are at least \( \left( \frac{j}{2} - o(1) \right) N^n \) points \( x \in I_N^n \) such that \( \eta_s(x) \neq \eta_{s'}(x) \), then \( F \) is said to possess the strict avalanche property.

**Definition 1.3.** If \( n, N \in \mathbb{N} \), \( \eta : I_N^n \rightarrow \{ -1, +1 \} \), \( \eta' : I_N^n \rightarrow \{ -1, +1 \} \), then the distance \( d(\eta, \eta') \) between \( \eta \) and \( \eta' \) is defined by

\[
d(\eta, \eta') = |\{ x \in I_N^n : \eta(x) \neq \eta'(x) \}|.
\]

If \( F = F(S) \) is of form (1.1), then the distance minimum \( m(F) \) in \( F \) is defined by

\[
m(F) = \min_{s, s' \in S} d(\eta_s, \eta_{s'}).
\]

Clearly, \( F \) is collision free if \( m(F) > 0 \), and \( F \) possesses the strict avalanche property if

\[
m(F) \geq \left( \frac{1}{2} - o(1) \right) N^n.
\]

Many pseudorandom binary lattices have been obtained and studied by using the subsets in finite fields (see [1–11]). Suppose that \( q = p^n \) is an odd prime power and \( \mathbb{F}_q \) is a finite field with \( q \) elements. Let \( v_1, \ldots, v_n \) be linearly independent elements of \( \mathbb{F}_q \) over \( \mathbb{F}_p \) and let \( \alpha \) be a primitive element of the finite field \( \mathbb{F}_q \), and \( d > 1 \) be a divisor of \( q - 1 \). The \( d \) th cyclotomic classes \( C^d_{\mathbb{F}_q} \) of \( \mathbb{F}_q \) are defined by
\[ C_i^{(d,q)} = \left\{ \alpha^{d+i} : 0 \leq j \leq \frac{q-1}{d} - 1 \right\}, \]

where \( 0 \leq i \leq d - 1 \). Then \( C_0^{(d,q)} \) is a subgroup of \( \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\} \), and \( C_i^{(d,q)} = \alpha^i C_0^{(d,q)}, 0 \leq i \leq d - 1 \). The \( d \)th cyclotomic classes give a partition of \( \mathbb{F}_q^* \):

\[
\mathbb{F}_q^* = \bigcup_{i=0}^{d-1} C_i^{(d,q)}. 
\]

In this paper, we shall give large families of binary lattices by using the cyclotomic classes in finite fields and study their properties. Our results are the following.

**Theorem 1.1.** Suppose that \( f(x) \in \mathbb{F}_q[x] \) with \( \deg(f) < p \) has no multiple zero in \( \bar{\mathbb{F}}_q \), where \( \bar{\mathbb{F}}_q \) is an algebraic closure of \( \mathbb{F}_q \). Let \( d > 1 \) be a divisor of \( q - 1 \) and \( d \) be even. Define

\[
\eta(x_1, \ldots, x_n) = \begin{cases} 
+1, & \text{if } f(x_1v_1 + \cdots + x_nv_n) \in \{0\} \cup \left( \bigcup_{i=0}^{d-1} C_i^{(d,q)} \right), \\
-1, & \text{if } f(x_1v_1 + \cdots + x_nv_n) \in \bigcup_{i=\frac{d}{2}}^{d-1} C_i^{(d,q)},
\end{cases}
\]

where \( x_i \in \{0, 1, \ldots, N-1\} \) for any \( i \in \{1, \ldots, n\} \). Assume that one of the following conditions holds

(a) \( f \) is irreducible;  (b) \( k = 2; \)  (c) \( 4q^{\deg(f)+k} < p. \)

Then we have

\[
Q_k(\eta) < k2^{k\deg(f)} \cdot q^{\frac{1}{2}(1 + \log p)}n \log^k(1 + d).
\]

**Theorem 1.2.** Suppose that \( K \in \mathbb{N}, K < q, S \) denotes the set of all polynomials \( f(x) \in \mathbb{F}_q[x] \) with \( 0 < \deg(f) \leq K \) of which the multiplicity of each zero in \( \bar{\mathbb{F}}_q \) is less than \( d \). Let \( d > 1 \) be a divisor of \( q - 1 \) and \( d \) be even. Define

\[
\eta_f(x_1, \ldots, x_n) = \begin{cases} 
+1, & \text{if } f(x_1v_1 + \cdots + x_nv_n) \in \{0\} \cup \left( \bigcup_{i=0}^{d-1} C_i^{(d,q)} \right), \\
-1, & \text{if } f(x_1v_1 + \cdots + x_nv_n) \in \bigcup_{i=\frac{d}{2}}^{d-1} C_i^{(d,q)},
\end{cases}
\]

and \( \mathcal{F} = \mathcal{F}(S) = \{\eta_f : f \in S\} \). Then

\[
\Gamma(\mathcal{F}) \geq K.
\]

**Theorem 1.3.** Suppose that \( S \) denotes the set of all monic polynomials \( f(x) \in \mathbb{F}_q[x] \) with \( 0 < \deg(f) \leq L \) which have no multiple zero in \( \bar{\mathbb{F}}_q \), and let \( d > 1 \) be a divisor of \( q - 1 \) and \( d \) be even. Define

\[
\eta_f(x_1, \ldots, x_n) = \begin{cases} 
+1, & \text{if } f(x_1v_1 + \cdots + x_nv_n) \in \{0\} \cup \left( \bigcup_{i=0}^{d-1} C_i^{(d,q)} \right), \\
-1, & \text{if } f(x_1v_1 + \cdots + x_nv_n) \in \bigcup_{i=\frac{d}{2}}^{d-1} C_i^{(d,q)},
\end{cases}
\]

and \( \mathcal{F} = \mathcal{F}(S) = \{\eta_f : f \in S\} \). Then

\[
m(\mathcal{F}) \geq \frac{q}{2} - 8(2L - 1)q^\frac{1}{2}\log^2(1 + d) - L.
\]
Corollary 1.1. Let $\mathcal{F}, L$ be defined as in Theorem 1.3. If

$$L < \frac{q + q^2 \log^2(1 + d)}{16q^2 \log^2(1 + d) + 1},$$

then $\mathcal{F}$ is collision free. Furthermore, if

$$L = o\left(q^3\right),$$

then $\mathcal{F}$ possesses the strict avalanche property.

2 Estimates for character sums of polynomials

We need the following lemmas to prove the theorems.

Lemma 2.1. Suppose that $\mathbb{F}_q$ is a finite field, $\alpha$ is a generator of the multiplicative group $\mathbb{F}_q^*$, and $\chi$ is a non-trivial multiplicative character such that $\chi^d = \chi_0$. Then

$$\sum_{k=0}^{d-1} \chi(a^k) = 0.$$

Proof. This is Lemma 4A of [12].

Lemma 2.2. Suppose that $\mathbb{F}_q$ is a finite field and $\chi$ is a non-trivial multiplicative character of $\mathbb{F}_q$. Assume that $f(x) \in \mathbb{F}_q[x]$ has $m$ distinct ones among its zeros, and it is not a constant times of a $\chi$th power. Then

$$\left| \sum_{z \in \mathbb{F}_q} \chi(f(z)) \right| \leq (m - 1)q^{\frac{1}{2}}.$$

Proof. This is Theorem 2C’ of [12].

Lemma 2.3. Suppose that $q = p^n$ is an odd prime power and $\mathbb{F}_q$ is a finite field. Let $z_1, \ldots, z_k \in \mathbb{F}_q$ and $0 \leq \delta_1, \ldots, \delta_k < d$ but not every $\delta_i$ be zero. Assume that $f(x) \in \mathbb{F}_q[x]$ with $\deg(f) < p$ has no multiple zero in $\mathbb{F}_q$, and assume that one of the following conditions holds

(a) $f$ is irreducible;  
(b) $k = 2$;  
(c) $4^{p(\deg(f) + k)} < p$.

Then

$$f^{\delta_1}(x + z_1) \cdots f^{\delta_k}(x + z_k) \in \mathbb{F}_q[x]$$

is not a constant times of a $d$th power of a polynomial.

Proof. This is Lemma 5 of [11].

Lemma 2.4. Suppose that $q = p^n$ is a prime power and $\chi$ is a non-trivial multiplicative character of the finite field $\mathbb{F}_q$. Assume that a non-constant polynomial $f(x) \in \mathbb{F}_q[x]$ has $m$ distinct zeros in its splitting field over $\mathbb{F}_q$, and it is not a constant times of a $\chi$th power. Let

$$B = \left\{ \sum_{i=1}^{n} j_i v_i : 0 \leq j_i \leq t_i, 0 \leq t_i \leq p - 1, i = 1, 2, \ldots, n \right\},$$

Constructions of pseudorandom binary lattices
where \( v_1, \ldots, v_n \) are linearly independent over \( \mathbb{F}_p \). Then we get

\[
\left| \sum_{z \in B} \chi(f(z)) \right| < mq^2(1 + \log p)^n.
\]

**Proof.** This is Theorem 2 of [13]. \( \square \)

**Lemma 2.5.** Suppose that \( q = p^n \) is an odd prime power, \( \alpha \) is a primitive element of the finite field \( \mathbb{F}_q \) and \( d > 1 \) be a divisor of \( q - 1 \). Let \( \mathbb{F}_q^* \) denote the set of all multiplicative characters of \( \mathbb{F}_q^* \) and \( \mathcal{G}^* = \{ \chi \in \mathbb{F}_q^* : \chi^q = \chi_0 \} \setminus \{ \chi_0 \} \). For \( 0 \leq y \leq q - 2 \), the following bound holds

\[
\sum_{\chi \in \mathcal{G}^*} \sum_{j=0}^{x+y} \chi(a^j) < 2d \log(1 + d).
\]

**Proof.** This is Lemma 1 of [14]. \( \square \)

**Lemma 2.6.** Suppose that \( T \) is a field and \( g(x) \in T[x] \) is a non-zero polynomial, then it can be written in the form

\[
g(x) = (h(x))^k g^*(x),
\]

where \( h(x), g^*(x) \in T[x] \) and the multiplicity of each zero of \( g^*(x) \) in \( T \) is less than \( k \).

**Proof.** This is Lemma 6 of [15]. \( \square \)

## 3 Pseudorandom measure of order \( k \)

Now we prove Theorem 1.1.

Let \( \mathbb{F}_q^* \) denote the set of all multiplicative characters of \( \mathbb{F}_q^* \) and \( \mathcal{G} = \{ \chi \in \mathbb{F}_q^* : \chi^d = \chi_0 \} \). For \( (x_1, \ldots, x_n) \) with \( f(\xi_0) = f(x_1 v_1 + \cdots + x_n v_n) \neq 0 \), by the orthogonality relations for characters and Lemma 2.1 we have

\[
f(\xi_0) \in \bigcup_{i=0}^{d-1} C_i^{(d, q)} \iff \text{there exist } 0 \leq i \leq \frac{d}{2} - 1, 0 \leq j \leq \frac{q - 1}{d} - 1 \text{ satisfying } f(\xi_0) = a^{id+i}
\]

\[
\implies \frac{1}{q-1} \sum_{i=0}^{d-1} \sum_{j=0}^{\frac{q-1}{d} - 1} \sum_{\chi \in \mathbb{F}_q^*} \chi(f(\xi_0)) \chi(a^{id+i}) = 1
\]

\[
\implies \frac{1}{d} \sum_{i=0}^{d-1} \sum_{\chi \in \mathcal{G}} \chi(f(\xi_0)) \chi(a^i) = 1.
\]

Write \( \mathcal{G}^* = \mathcal{G} \setminus \{ \chi_0 \} \). Hence,

\[
\eta(x_1, \ldots, x_n) = \frac{2}{d} \sum_{\chi \in \mathcal{G}^*} \sum_{j=0}^{d-1} \chi(a^j) \chi(f(x_1 v_1 + \cdots + x_n v_n)). \tag{3.1}
\]

Define \( B' = \left\{ \sum_{j=1}^{n} l_i(b_i v_i) : 0 \leq j_1 \leq t_1, 0 \leq t_i \leq p - 1, i = 1, 2, \ldots, n \right\} \), where \( b_1, \ldots, b_n \) are positive integers, and write \( d_i = (d_{1i}, \ldots, d_{ni}) \), \( z_i = d_{1i} v_1 + \cdots + d_{ni} v_n, i = 1, 2, \ldots, k \). Thus, we obtain
Let \( \chi^* \) be a generator of the group of multiplicative characters on \( \mathbb{F}_q^* \). For \( u = 1, \ldots, k \), we define \( \delta_u \) by \( \overline{\chi^*_u} = \chi^*_{u\delta_u} \), where \( 0 < \delta_u < q - 1 \). By Lemmas 2.3 and 2.4 we have

\[
\left| \sum_{z \in B'} \overline{\chi^*_i}(f(z + z_i)) \cdots \overline{\chi^*_k}(f(z + z_k)) \right| = \left| \sum_{z \in B'} \chi^*_i(f^k(z + z_i) \cdots f^k(z + z_k)) \right| < k \deg(f) \cdot q^2(1 + \log p)^n.
\]

Then

\[
\left| \sum_{u=1}^{l_u} \cdots \sum_{u=1}^{l_u} \eta(j_1 b_1 u_1 + \cdots + j_n b_n u_n + d_i) \cdots \eta(j_1 b_1 u_1 + \cdots + j_n b_n u_n + d_i) \right|
\]

\[
< \frac{2^k}{d^k} \left( \sum_{\chi \in \mathbb{F}^*} \left| \sum_{j=0}^{k-1} \chi(a^j) \right|^k \right)^k \cdot k \deg(f) \cdot q^2(1 + \log p)^n
\]

\[
< k2^k \deg(f) \cdot q^2(1 + \log p)^n \log^k(1 + d)
\]

by Lemma 2.5. It follows that

\[
Q_k(\eta) < k2^k \deg(f) \cdot q^2(1 + \log p)^n \log^k(1 + d),
\]

which proves Theorem 1.1.

### 4 Family complexity

We will adopt the methods used in [15, 16] to prove Theorem 1.2. We shall show that for any specification of length \( K \)

\[
\eta(x_i) = \varepsilon_1, \quad \eta(x_2) = \varepsilon_2, \quad \ldots, \quad \eta(x_K) = \varepsilon_K,
\]

(4.1)

where \( x_1, x_2, \ldots, x_K \in \mathbb{F}_q^* \) are \( K \) distinct vectors, there is an \( f \in S \) so that the binary lattice \( \eta = \eta_f \in \mathcal{F} \) satisfies the specification (4.1).

Note that \( K < q \), thus there is an integer \( K + 1 \) satisfying

\[
1 < K + 1 \leq q, \quad x_{K+1} \notin \{x_1, x_2, \ldots, x_K\}.
\]

Let

\[
\varepsilon_{K+1} = -\varepsilon_1,
\]

and let \( \varphi : \mathbb{F}_p^n \to \mathbb{F}_q \) be a mapping defined by

\[
\varphi(x) = \varphi((x_1, \ldots, x_n)) = x_1 v_1 + \cdots + x_n v_n \in \mathbb{F}_q,
\]

where \( x = (x_1, \ldots, x_n) \in \mathbb{F}_p^n \), and let \( \varphi(x_i) = t_i \in \mathbb{F}_q \) for \( i = 1, 2, \ldots, K + 1 \).
For $i = 1, 2, \ldots, K + 1$, we define
\[ y_i \in \begin{cases} \bigcup_{j=0}^{d-1} C_j^{(d,q)}, & \text{if } \varepsilon_i = +1, \\ \bigcup_{j=\frac{d}{2}}^{d-1} C_j^{(d,q)}, & \text{if } \varepsilon_i = -1. \end{cases} \quad (4.2) \]

It is well known that
\[ g(x) = \sum_{i=1}^{K+1} y_i L_i(x), \quad L_i(x) = \prod_{j \neq i} \frac{x - t_j}{t_i - t_j}, \quad i = 1, \ldots, K + 1, \]
\[ g(x) = (h(x))^d g^*(x), \]
is a representation of the unique interpolating polynomial $g(x) \in \mathbb{F}_q[x]$ with $\deg(g) = K$ corresponding to the data $(t_i, y_i)$, $t_i \neq t_j$ for $i \neq j$, $i, j = 1, \ldots, K + 1$.

Note that $g(x) \in \mathbb{F}_q[x]$ with $\deg(g) = K \geq 1$ is a non-zero polynomial, by Lemma 2.6, $g(x)$ can be written in the form
\[ g(x) = (h(x))^d g^*(x), \]
where $h(x), g^*(x) \in \mathbb{F}_q[x]$ and the multiplicity of each zero of $g^*(x)$ in $\mathbb{F}_q$ is less than $d$. Let
\[ f(x) = g^*(x). \]
It follows that
\[ \deg(f) = \deg(g^*) \leq \deg(g) = K. \]

By (4.2) and (4.3), we have
\[ g(t_i) = y_i \in \begin{cases} \bigcup_{j=0}^{d-1} C_j^{(d,q)}, & \text{if } \varepsilon_i = +1, \\ \bigcup_{j=\frac{d}{2}}^{d-1} C_j^{(d,q)}, & \text{if } \varepsilon_i = -1, \end{cases} \quad (4.4) \]
where $i = 1, 2, \ldots, K + 1$. Therefore,
\[ (h(t_i))^d g^*(t_i) = g(t_i) = y_i \in \mathbb{F}_q^*, \]
and thus
\[ f(t_i) = g^*(t_i) \in \mathbb{F}_q^*. \]
Then by (3.1) and (4.2) we have
\[ \eta(x) = \frac{2}{d} \sum_{j=0}^{d-1} \sum_{x \in \mathcal{G}^*} \tilde{\chi}(f(t_i)) \chi(a^j) = \frac{2}{d} \sum_{j=0}^{d-1} \sum_{x \in \mathcal{G}^*} \tilde{\chi}(g^*(t_i)) \chi(a^j) \]
\[ = \frac{2}{d} \sum_{j=0}^{d-1} \sum_{x \in \mathcal{G}^*} \tilde{\chi}((h(t_i))^d g^*(t_i)) \chi(a^j) = \frac{2}{d} \sum_{j=0}^{d-1} \sum_{x \in \mathcal{G}^*} \tilde{\chi}(g(t_i)) \chi(a^j) \]
\[ = \frac{2}{d} \sum_{j=0}^{d-1} \sum_{x \in \mathcal{G}^*} \tilde{\chi}(y_j) \chi(a^j) = \begin{cases} +1, & \text{if } \varepsilon_i = +1, \\ -1, & \text{if } \varepsilon_i = -1, \end{cases} \]
where $i = 1, 2, \ldots, K + 1$, which implies that
\[ \tilde{\chi}(f(t_i)) \neq \tilde{\chi}(f(t_{i-q})), \]
and $\deg(f) > 0$, and thus $f \in \mathcal{S}$ and the binary lattice $\eta = \eta_f \in \mathcal{F}$ satisfies the specification (4.1). This completes the proof of Theorem 1.2.
5 Collision and avalanche effect

Now we study collision and avalanche effect of the family $\mathcal{F}$ of binary lattices defined in Theorem 1.3. Suppose that $f, g \in \mathcal{S}$ and $f \neq g$. By the definition of the distance $d(\eta_f, \eta_g)$ between $\eta_f$ and $\eta_g$, we have

$$d(\eta_f, \eta_g) = |\{x \in \mathbb{F}_p^n : \eta_f(x) \neq \eta_g(x)\}| = \sum_{x \in \mathbb{F}_p^n} \frac{1}{2} (1 - \eta_f(x) \eta_g(x)).$$  \hfill (5.1)

The last part of the sum in Eq. (5.1) can be written as:

$$\left| \sum_{x=0}^{p-1} \cdots \sum_{x=0}^{p-1} \eta_f(x_1, \ldots, x_n) \eta_g(x_1, \ldots, x_n) \right| \leq \left| \sum_{f \in \mathcal{S}, g \in \mathcal{S}} \left( \frac{2}{d} \sum_{i=0}^{d-1} \sum_{x \in \mathbb{F}_p^*} \chi_f \chi_1(a_i) \right) \cdot \left( \frac{2}{d} \sum_{i=0}^{d-1} \sum_{x \in \mathbb{F}_p^*} \chi_g \chi_2(a_i) \right) \right| + 2L$$

$$= \frac{4}{d^2} \sum_{f \in \mathcal{S}, g \in \mathcal{S}} \left| \sum_{i=0}^{d-1} \chi_f(a_i) \sum_{i=0}^{d-1} \chi_g(a_i) \right| \leq (2L - 1) q^4.$$

Let $\chi$ be a generator of the group of multiplicative characters on $\mathbb{F}_q^*$. Define $\chi_1 = \chi^{\delta_1}$ and $\chi_2 = \chi^{\delta_2}$, where $0 < \delta_1, \delta_2 < q - 1$. Note that $f, g \in \mathcal{S}, f \neq g$ and $f, g$ have no multiple zero in $\mathbb{F}_q$, thus $f^{\delta_1} g^{\delta_2}$ is not a constant times of a $(q - 1)^{th}$ power of a polynomial. Applying Lemma 2.2 we obtain

$$\left| \sum_{x \in \mathbb{F}_q^n} \chi_f(f(z)) \chi_2(g(z)) \right| \leq \left| \sum_{x \in \mathbb{F}_q^n} \chi_f(f^{\delta_1}(z) g^{\delta_2}(z)) \right| \leq (2L - 1) q^4.$$

Then

$$\left| \sum_{x \in \mathbb{F}_p^n} \eta_f(x) \eta_g(x) \right| \leq \frac{4}{d^2} \left( \sum_{\chi \in \mathbb{F}_q^*} \left| \sum_{a \in \mathbb{F}_q^*} \chi(a) \right|^2 \right)^2 \cdot (2L - 1) q^4 < 16(2L - 1) q^4 \log^2(1 + d).$$

It follows that

$$d(\eta_f, \eta_g) \geq \frac{q}{2} - 8(2L - 1) q^4 \log^2(1 + d) - L$$

and

$$m(\mathcal{F}) = \min_{f, g \in \mathcal{S}} d(\eta_f, \eta_g) \geq \frac{q}{2} - 8(2L - 1) q^4 \log^2(1 + d) - L,$$

which proves Theorem 1.3.

References

[1] Pascal Hubert, Christian Mauduit, and András Sárközy, On pseudorandom binary lattices, Acta Arith. 125 (2006), no. 1, 51–62, DOI: https://doi.org/10.4064/aa125-1-5.

[2] Katalin Gyarmati, Christian Mauduit, and András Sárközy, Measures of pseudorandomness of families of binary lattices, I (Definitions, a construction using quadratic characters), Publ. Math. Debrecen 79 (2011), no. 3, 445–460, DOI: https://doi.org/10.5486/PMD.2011.5066.
Katalin Gyarmati, Christian Mauduit, and András Sárközy, *Measures of pseudorandomness of families of binary lattices, II* (A further construction), Publ. Math. Debrecen 80 (2012), no. 3, 479–502, DOI: https://doi.org/10.5486/PMD.2012.5197.

Katalin Gyarmati, Christian Mauduit, and András Sárközy, *On finite pseudorandom binary lattices*, Discrete Appl. Math. 216 (2017), 589–597, DOI: https://doi.org/10.1016/j.dam.2015.07.012.

Huaning Liu, *A large family of pseudorandom binary lattices*, Proc. Amer. Math. Soc. 137 (2017), no. 3, 793–803, DOI: https://doi.org/10.1090/S0002-9939-08-08706-2.

Huaning Liu, *Large families of pseudorandom binary sequences and lattices by using the multiplicative inverse*, Acta Arith. 159 (2013), no. 2, 123–131, DOI: https://doi.org/10.4064/aa159-2-3.

Huaning Liu, *Large families of pseudorandom binary lattices by using the multiplicative inverse modulo p*, Int. J. Number Theory 15 (2019), no. 3, 527–546, DOI: https://doi.org/10.1142/S1793042119500271.

Huaning Liu and Jing Gao, *A note on large families of pseudorandom binary sequences and lattices*, J. Inf. Sci. Eng. 30 (2014), no. 5, 1635–1654, DOI: https://doi.org/10.6688/JISE.2014.30.5.19.

Christian Mauduit and András Sárközy, *On large families of pseudorandom binary lattices*, Unif. Distrib. Theory 2 (2007), no. 1, 23–37.

Christian Mauduit and András Sárközy, *Construction of pseudorandom binary lattices by using the multiplicative inverse*, Monatsh. Math. 153 (2008), no. 3, 217–231, DOI: https://doi.org/10.1007/s00605-007-0479-z.

László Mérai, *Construction of pseudorandom binary lattices based on multiplicative characters*, Period. Math. Hungar. 59 (2009), no. 1, 43–51, DOI: https://doi.org/10.1007/s10998-009-9043-z.

Wolfgang M. Schmidt, *Equations over Finite Fields: An Elementary Approach*, Springer-Verlag, New York, 1976.

Arne Winterhof, *Some estimates for character sums and applications*, Des. Codes Cryptogr. 22 (2001), no. 2, 123–131, DOI: https://doi.org/10.1023/A:1008300619004.

Zhixiong Chen, Xiaoni Du, and Rong Sun, *A construction of binary cyclotomic sequences using extension fields*, IEICE Trans. Fund. Electron. Commun. Comput. Sci. E92-A (2009), no. 2, 663–667, DOI: https://doi.org/10.1587/transfun.E92.A.663.

Rudolf Ahlswede, Christian Mauduit, and András Sárközy, *Large families of pseudorandom sequences of k symbols and their complexity, Part II*, Electron. Notes Discrete Math. 21 (2005), 199–201, DOI: https://doi.org/10.1016/j.endm.2005.07.023.

Rudolf Ahlswede, Levon H. Khachatrian, Christian Mauduit, and András Sárközy, *A complexity measure for families of binary sequences*, Period. Math. Hungar. 46 (2003), no. 2, 107–118, DOI: https://doi.org/10.1023/A:1025962825241.