Measures of pseudorandomness of families of binary lattices, II
(A further construction.)

Katalin Gyarmati
Eötvös Loránd University
Department of Algebra and Number Theory
H-1117 Budapest, Pázmány Péter sétány 1/C, Hungary
e-mail: gykati@cs.elte.hu
(corresponding author; fax: 36-13812146)

Christian Mauduit
Institut de Mathématiques de Luminy
CNRS, UMR 6206
163 avenue de Luminy, Case 907
F-13288 Marseille Cedex 9, France
e-mail: mauduit@iml.univ-mrs.fr

András Sárközy
Eötvös Loránd University
Department of Algebra and Number Theory
H-1117 Budapest, Pázmány Péter sétány 1/C, Hungary
e-mail: sarkozy@cs.elte.hu

2010 Mathematics Subject Classification: Primary 11K45.

Keywords and phrases: pseudorandom, binary lattice, family complexity, collision and avalanche effect.

Research partially supported by Hungarian National Foundation for Scientific Research, Grants No. K67676, K72731 and PD72264, French-Hungarian exchange program FR-33/2009, and the János Bolyai Research Fellowship.

Abstract

In Part I of this paper we extended the notions of family complexity, collision and avalanche effect from one dimension to n dimensions, i.e., from binary sequences to binary lattices. Then we considered a large family of binary lattices with strong pseudorandom properties which had been constructed by using quadratic characters of finite fields, and we showed that this family also possesses a nice structure in terms of these notions. In Part I we considered a large family of binary sequences with strong pseudorandom properties constructed by using additive characters and we extended it to n dimensions, i.e., to binary lattices. In this paper we will show that these binary lattices possess strong pseudorandom properties, and their family also possesses a nice structure in terms of family complexity, collision and avalanche effect.

1 Introduction

First we recall those definitions from Part I [9] which we need here. In [14] Mauduit and Sárközy proposed to use the following measures of pseudorandomness of binary sequences

$$(e_1, e_2, \dots, e_N) \in \{-1, +1\}^N :$$

the *well-distribution measure* of E_N is defined by

$$W(E_N) = \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right| \tag{1.1}$$

where the maximum is taken over all $a, b, t \in \mathbb{N}$ with $1 \le a \le a+(t-1)b \le N$, and the *correlation measure of order k* of E_N is defined as

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

where the maximum is taken over all $\mathbf{D} = (d_1, \dots, d_k)$ and M such that $0 \le d_1 < \dots < d_k \le N - M$. The *combined* (well-distribution-correlation) *pseudorandom measure of order* k was also introduced:

$$Q_k(E_N) = \max_{a,b,t,\mathbf{D}} \left| \sum_{j=0}^{t} e_{a+jb+d_1} \dots e_{a+jb+d_k} \right| \tag{1.2}$$

where the maximum is taken over all a, b, t and $\mathbf{D} = (d_1, \dots, d_k)$ such that all the subscripts $a + jb + d_\ell$ belong to $\{1, 2, \dots, N\}$. (Note that $Q_1(E_N) = W(E_N)$ and clearly $C_k(E_N) \le Q_k(E_N)$.) Then 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, in particular, both are $o(N)$ as $N \longrightarrow \infty$. Indeed, later Cassaigne, Mauduit and Sárközy [3] showed that this terminology is justified since for almost all $E_N \in \{-1, +1\}^N$ both $W(E_N)$ and $C_k(E_N)$ (for fixed k) are less than $N^{1/2}(\log N)^c$ (and they are also greater than $\varepsilon N^{1/2}$; see also [2] and [12]). Since that many papers have been written on the pseudorandomness of special binary sequences and on the measures of pseudorandomness.

In [11] Hubert, Mauduit and Sárközy extended this theory of pseudorandomness to n dimensions. They introduced the following definitions:

Denote by I_N^n the set of n-dimensional vectors whose coordinates are integers between 0 and $N-1$:

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

This set is called an *n-dimensional N-lattice* or briefly an *N-lattice*. In [10] this definition was extended to more general lattices in the following way: Let $\mathbf{u_1}, \mathbf{u_2}, \dots, \mathbf{u_n}$ be n linearly independent n-dimensional vectors over the field of the real numbers such that the i-th coordinate of $\mathbf{u_i}$ is a positive integer and the other coordinates of $\mathbf{u_i}$ are 0, so that $\mathbf{u_i}$ is of the form $(0, \dots, 0, z_i, 0, \dots, 0)$ (with $z_i \in \mathbb{N}$). Let $t_1, t_2, \dots, t_n$ be integers with $0 \le t_1, t_2, \dots, t_n < N$. Then we call the set

$$B_N^n = \{\mathbf{x} = x_1\mathbf{u_1} + \cdots + x_n\mathbf{u_n} :,\ x_i \in \mathbb{N} \cup \{0\},\ 0 \le x_i\,|\mathbf{u_i}| \le t_i(< N)$$
$$\text{for } i = 1, \dots, n\}$$

an *n-dimensional box N-lattice* or briefly a *box N-lattice.*

In [11] the definition of binary sequences was extended to more dimensions by considering functions of type

$$\eta(\mathbf{x}):\ I_N^n \to \{-1, +1\}.$$

If $\mathbf{x} = (x_1, \dots, x_n)$ so that $\eta(\mathbf{x}) = \eta((x_1, \dots, x_n))$ then we will simplify the notation slightly by writing $\eta(\mathbf{x}) = \eta(x_1, \dots, x_n)$. Such a function can be visualized as the lattice points of the N-lattice replaced by the two symbols $+$ and $-$, thus they are called *binary N-lattices.*

In [11] Hubert, Mauduit and Sárközy introduced the following measures of pseudorandomness of binary lattices (here we will present the definition in the same slightly modified but equivalent form as in [10]):

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

Define the pseudorandom measure of order k of η by

$$Q_k(\eta) = \max_{B,\mathbf{d_1},\dots,\mathbf{d_k}} \left| \sum_{\mathbf{x}\in B} \eta(\mathbf{x} + \mathbf{d_1}) \cdots \eta(\mathbf{x} + \mathbf{d_k}) \right|,$$

where the maximum is taken over all distinct $\mathbf{d_1}, \dots, \mathbf{d_k} \in I_N^n$ and all box N-lattices B such that $B + \mathbf{d_1}, \dots, B + \mathbf{d_k} \subseteq I_N^n$. Note that in the one dimensional special case $Q_k(\eta)$ is the same as the combined pseudorandom measure (1.2) for every k and, in particular $Q_1(\eta)$ is the well-distribution measure W in (1.1).

Then η is said to have strong pseudorandom properties, or briefly, it is considered as a "good" pseudorandom binary lattice if for fixed n and k and "large" N the measure $Q_k(\eta)$ is "small" (much smaller, than the trivial upper bound N^n). This terminology is justified by the fact that, as it was proved in [11], for a truly random binary lattice defined on I_N^n and for fixed k the measure $Q_k(\eta)$ is "small", more precisely, it is less than $N^{n/2}$ multiplied by a logarithmic factor. As in the one-dimensional case, a list of papers written on pseudorandomness of binary lattices and on the measures of pseudorandomness is presented in [6]; see also the more recent papers [7] and [8].

In the applications one may need not just a single binary sequence resp. lattice with strong pseudorandom properties but a large family of them. Moreover, in many applications it is not enough if our family $\mathcal{F}$ is large; it can be much more important to know that $\mathcal{F}$ has a "rich", "complex" structure, there are many "independent" sequences, resp. lattices in it which are "far apart". Thus one needs quantitative measures for these properties of families of binary sequences, resp. lattices. In the one dimensional case there are tools of this type appearing in the literature: family complexity, collision, avalanche effect. In Part I we presented their definitions, and then we extended them to n dimensions, i.e., to binary lattices. These definitions in the n dimensional case are the following:

Let $\mathcal{F}$ be a family of binary lattices $\eta: \ I_N^n \rightarrow \{-1,+1\}$, let $j \leq N^n$, let $\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_j}$ be j distinct vectors from I_N^n, and let $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_j) \in \{-1,+1\}^j$. If we consider binary lattices $\eta: \ I_N^n \rightarrow \{-1,+1\}$ with

$$\eta(\mathbf{x_1}) = \varepsilon_1, \ \eta(\mathbf{x_2}) = \varepsilon_2, \ldots, \eta(\mathbf{x_j}) = \varepsilon_j, \tag{1.3}$$

then

Definition 1 (1.3) *is said to be a specification of length j of η.*

Definition 2 *The* family complexity *or* f-complexity *of a family $\mathcal{F}$ of binary lattices $\eta: \ I_N^n \rightarrow \{-1,+1\}$, denoted by $\Gamma(\mathcal{F})$, is defined as the greatest integer j so that for any specification* (1.3) *of length j there is at least one $\eta \in \mathcal{F}$ which satisfies it.*

Then it is easy to see that

$$\Gamma(\mathcal{F}) \leq \frac{\log |\mathcal{F}|}{\log 2}. \tag{1.4}$$

(Indeed, this is Proposition 1 in [9].)

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

$$\mathcal{F} = \mathcal{F}(\mathcal{S}) = \{\eta_s : \ s \in \mathcal{S}\}. \tag{1.5}$$

Definition 3 *If $s \in \mathcal{S}$, $s' \in \mathcal{S}$, $s \neq s'$ and $\eta_s = \eta_{s'}$, then this is said to be a* collision *in $\mathcal{F} = \mathcal{F}(\mathcal{S})$. If there is no collision in $\mathcal{F} = \mathcal{F}(\mathcal{S})$, then $\mathcal{F}$ is said to be* collision free.

Definition 4 *If $\mathcal{F}$ is of form* (1.5)*, and for any $s \in \mathcal{S}$ changing any element of s changes "many" elements of $\eta_s : \ I_N^n \to \{-1, +1\}$, then we speak about* avalanche effect*, and we say that $\mathcal{F} = \mathcal{F}(\mathcal{S})$ possesses the* avalanche property*. If for any $s \in \mathcal{S}$, $s' \in \mathcal{S}$, $s \neq s'$ at least $\left(\frac{1}{2} - o(1)\right) N^n$ elements of η_s and $\eta_{s'}$ are different, then $\mathcal{F}$ is said to possess the* strict avalanche property*.*

Definition 5 *If $N \in \mathbb{N}$, $n \in \mathbb{N}$, $\eta : \ I_N^n \to \{-1, +1\}$ and $\eta' : \ I_N^n \to \{-1, +1\}$, then the distance $d(\eta, \eta')$ between η and η' is defined by*

$$\begin{aligned} d(\eta, \eta') = |\{(x_1, x_2, \dots, x_n) : (x_1, \dots, x_n) \in \mathbb{I}_N^n,& \\ \eta(x_1, \dots, x_n) \neq \eta'(x_1, \dots, x_n)\}|.& \end{aligned}$$

If $\mathcal{F}$ is a family of form (1.5)*, then the* distance minimum $m(\mathcal{F})$ *is defined by*

$$m(\mathcal{F}) = \min_{\substack{s, s' \in \mathcal{S} \\ s \neq s'}} d(\eta_s, \eta_{s'}).$$

(So that $\mathcal{F}$ is collision free if $m(\mathcal{F}) > 0$, and it possesses the strict avalanche property if

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

After introducing these definitions in Part I, the rest of the paper was devoted to the study of a family of binary lattices. In [16] Mauduit and Sárközy constructed a large family of binary lattices by using the quadratic character of finite fields and they proved that these lattices have strong pseudorandom properties in terms of the measures Q_k. In Part I we also showed that a variant of this family also possesses nice pseudorandom structure in terms of family complexity, collisions and avalanche effect.

The quadratic character based constructions certainly belong to the best ones in both one and n dimensions. However, there are a few further constructions which are (nearly) equally good or just slightly inferior to these quadratic character constructions. It may occur that these other constructions have certain advantages (e.g., fast and simple implementation, flexibility of certain type, better control of a special pseudorandom property) which pay in some applications. Thus it is worth to continue the work by analyzing the pseudorandom properties of families generated by other important constructions. In this paper our goal is to analyze two closely related further constructions, and then combining certain elements of the two constructions we will be able to construct a further large family of binary lattices such that each of them has strong pseudorandom properties and their family also possesses a nice pseudorandom structure.

2 Two further constructions

The first construction is a one dimensional-one which was presented by Mauduit, Rivat and Sárközy in [13]: let p be an odd prime, $f(x) \in \mathbb{F}_p[x]$, and define the binary sequence $E_p = (e_1, \dots, e_p)$ by

$$e_n = \begin{cases} +1 & \text{if } 0 \le r_p(f(n)) < p/2 \\ -1 & \text{if } p/2 \le r_p(f(n)) < p \end{cases} \tag{2.1}$$

(for $n = 1, 2, \dots, p$) where $r_p(n)$ denotes the unique $r \in \{0, 1, \dots, p-1\}$ such that $n \equiv r \pmod p$. They proved:

Theorem A *If $f \in \mathbb{F}_q[x]$ is of degree $\ell \geq 2$ and $E_p = (e_1, e_2, \dots, e_p)$ is defined as above, then we have*

$$W(E_p) \ll \ell p^{1/2} (\log p)^2,$$

and for

$$2 \leq k \leq \ell - 1, \tag{2.2}$$

$$C_k(E_p) \leq \ell p^{1/2} (\log p)^{k+2}.$$

(The expression "additive characters" appears in the title of their paper [13] since this result is proved by using additive characters.) However, they also showed that the correlation of large order can be large:

Theorem B *For any $\ell = 2^s$ there exists a constant $c = c(\ell) > 0$ such that if p is a prime number large enough, $f \in \mathbb{F}_p[x]$ is of degree ℓ and $E_p = (e_1, \dots, e_p)$ is defined as above, then*

$$\max_{\substack{U,V \\ 1 \leq U < U+V \leq p+1-\ell}} \left| \sum_{n=U}^{U+V} e_n e_{n+1} \dots e_{n+\ell-1} \right| \geq cp.$$

Thus condition (2.2) in Theorem A is necessary, and the correlation of order k can be large if $k \geq \deg f$. This slight weakness of construction (2.1) explains that, apart from a rather simplified and crude construction in [5] (which did not use finite fields) it has not been extended to n dimensions (to binary lattices). However, in the most applications this small problem does not lead to any difficulties: it is usually enough to know that the correlation of small order are small. If we want C_k to be small, for say $k \leq K$, then it is enough to take polynomials of degree greater than K. Taking the degrees of the polynomial higher makes the computation longer but, on the other hand, it means more freedom in the choice of the coefficients and it makes the size of the family greater, which pays in cryptography and elsewhere.

In [18] Tóth showed that the family induced by (2.1) and (2.2) is not collision free, but later she showed [19] that this weakness can be corrected by taking a subfamily which is just a slightly smaller but it is collision free and it also possesses the strict avalanche property.

Thus we may conclude that in spite of minor problems arising from Theorem B, construction (2.1) can be adjusted to the majority of the applications, besides it is simple and it can be implemented easily, so that is worth to continue its study and, in particular, to extend it to n dimensions (to binary lattices), by using also finite fields which may lead to sharper estimates.

The difficulties arising from Theorem B can be eliminated by using the notion of the multiplicative inverse and replacing $f(n)$ in (2.1) by its multiplicative inverse. This was shown by Mauduit and Sárközy in [15]:

Theorem C *Assume that p is a prime number, $f \in \mathbb{F}_p[x]$ has degree $(0 <)\ell(< p)$ and no multiple zero in $\overline{\mathbb{F}}_p$. For $(a, p) = 1$, denote the multiplicative inverse of a by a^{-1}:*

$$aa^{-1} \equiv 1 \pmod p.$$

Define the binary sequence $E_p = (e_1, \dots, e_p)$ by

$$e_n = \begin{cases} +1 & \text{if } (f(n), p) = 1,\ r_p(f(n))^{-1} < \frac{p}{2} \\ -1 & \text{if either } (f(n), p) = 1 \text{ and } r_p(f(n))^{-1} > \frac{p}{2} \text{ or } p \mid f(n) \end{cases} \tag{2.3}$$

for $n = 1, 2, \dots, p$ (where $r_p(n)$ is defined as in (2.1)). Then we have

$$W(E_p) \ll \ell p^{1/2} (\log p)^2.$$

Theorem D *Define p, $f(x)$, ℓ and $E_p = (e_1, \dots, e_p)$ in the same way as in Theorem C. Assume also that $k \in \mathbb{N}$ with $2 \leq k \leq p$, and one of the following conditions holds:*

(i) $k = 2$;

(ii) $(4\ell)^k < p$.

Then we also have

$$C_k(E_p) \ll \ell k p^{1/2} (\log p)^{k+1}.$$

Note that for small ℓ (for $\ell \ll \frac{\log p}{\log\log p}$) condition (ii) in Theorem D is weaker, than (2.2) in Theorem A.

In [17] Mauduit and Sárközy extended construction (2.3) to n dimensions (to binary lattices). Let $q = p^n$ be the power of an odd prime. We will consider the field $\mathbb{F}_q$ of order q, its prime field of order p will be denoted by $\mathbb{F}_p$ (and we will identify $\mathbb{F}_p$ with the field of the modulo p residue classes, and we write i for the residue class $\equiv i \pmod{p}$). Fix a basis $v_1, v_2, \dots, v_n$ of the linear vector space formed by $\mathbb{F}_q$ over $\mathbb{F}_p$ (i.e., $v_1, v_2, \dots, v_n$ are linearly independent over $\mathbb{F}_p$). Let $\varphi : I_p^n \to \mathbb{F}_q$ be the mapping defined so that for $\mathbf{x} = (x_1, \dots, x_n) \in I_p^n$ we have

$$\varphi(\mathbf{x}) = \varphi((x_1, x_2, \dots, x_n)) = x_1 v_1 + \cdots + x_n v_n \in \mathbb{F}_q;$$

clearly, this is a bijection.

Assume that $\ell \in \mathbb{N}$, $a_1, \dots, a_\ell$ are distinct elements of $\mathbb{F}_q$, and let

$$f(z) = (z + a_1)(z + a_2) \dots (z + a_\ell) \ (\in \mathbb{F}_q[z]). \tag{2.4}$$

Define the "boxes" $B_1, B_2, \dots, B_n$ by

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

and write

$$\mathcal{B} = \cup_{j=1}^n B_j.$$

Define the binary lattice $I_p^n \to \{-1, +1\}$ by

$$\eta(\mathbf{x}) = \begin{cases} +1 & \text{if } f(\varphi(\mathbf{x})) \neq 0 \text{ and } f(\varphi(\mathbf{x}))^{-1} \in \mathcal{B} \\ -1 & \text{otherwise.} \end{cases} \tag{2.5}$$

(As they write in [17]: "We remark that the definition of $\mathcal{B}$ is made slightly complicated by the fact that we have to balance between two requirements: the structure of $\mathcal{B}$ must be possibly symmetric, easy to handle and, on the other hand, its cardinality must approximate $\frac{q}{2}$ well.")

It was shown that if k is not very large, then $Q_k(\eta)$ is "small" for this binary lattice η:

Theorem E *If $p, q, n, \ell, \mathcal{B}$ and η are defined as above, $k \in \mathbb{N}$*

$$k, \ell < p, \ k + \ell \leq p + 1$$

and

$$k\ell < \frac{q}{2},$$

then we have

$$Q_k(\eta) < \left(2^{k+3} + 1\right) k\ell n^k q^{1/2} (\log p + 2)^{n+k}.$$

We have tried to show that there is a large family of binary lattices of type (2.5) obtained from polynomials of form (2.4) (so that by Theorem E the pseudorandom measures Q_k of the lattices are small for small k) and the complexity of this family is large, it is collision free, and it also possesses the strict avalanche property (as it happens in case of the quadratic character construction studied in Part I). Unfortunately, we have not been able to do this. The difficulty is that the polynomials f appearing in this construction have the very special structure given in (2.4) which can be handled only by multiplicative characters (which appear in the quadratic character construction) but it can be handled neither by additive characters (which is the natural approach in case of construction (2.5)) nor by the interpolation method used in [1].

Since the estimate of the family complexity seems to be so difficult in case of the multiplicative inverse construction (2.3), thus we will return here to construction (2.1) which is slightly simpler and thus it can be handled more easily. First in Section 3 we will extend construction (2.1) to n dimensions by using the same finite fields approach which was used in [17] for extending construction (2.3) to the n dimensional construction (2.5), and we will show that $Q_k(\eta)$ is small for the binary lattice obtained in this way if k is small. Then in Section 4 we will introduce a large subfamily of these lattices, and we will show that its family complexity is also large; we will prove this by using a variant of the interpolation method (introduced in [1]). Finally, in Section 5 we will show that the same subfamily is collision free, and it also possesses the strict avalanche property. Thus this subfamily is composed of lattices each having strong pseudorandom properties, and their family also possesses strong pseudorandom properties.

3 Extension of construction (2.1) to n dimensions and estimate of the pseudorandom measures.

We will use the same notations as in Section 2. Let $f(z) \in \mathbb{F}_q[z]$ be a non-constant polynomial, and define the binary lattice $\eta: \; I_p^n \to \{-1,+1\}$ by

$$\eta(\mathbf{x}) = \eta_f(\mathbf{x}) = \begin{cases} +1 & \text{if } f(\varphi(\mathbf{x})) \in \mathcal{B} \\ -1 & \text{if } f(\varphi(\mathbf{x})) \notin \mathcal{B}. \end{cases} \tag{3.1}$$

Theorem 1 *Let $k, \ell \in \mathbb{N}$ with*

$$2 \le \ell < p \tag{3.2}$$

and

$$2 \le k \le \ell - 1, \tag{3.3}$$

let $f(z) \in \mathbb{F}_q[z]$ be of degree ℓ, and define η by (3.1). Then we have

$$Q_k(E_N) < 2^k \ell n^k q^{1/2} (\log p + 2)^{n+k}. \tag{3.4}$$

As Theorem B shows condition (3.3) is necessary in the special case $n = 1$. This result could be extended to the case of general n (so that (3.3) is also necessary for $n > 1$); we will not go into details of this here.

Proof of Theorem 1. Consider the i-th factor $\eta(\mathbf{x} + \mathbf{d_i})$ in the sum in definition of $Q_k(\eta)$. By (3.1), the value of this is

$$\eta(\mathbf{x} + \mathbf{d_i}) = \begin{cases} +1 & \text{if } f(\varphi(\mathbf{x} + \mathbf{d_i})) \in \mathcal{B} \\ -1 & \text{if } f(\varphi(\mathbf{x} + \mathbf{d_i})) \notin \mathcal{B}. \end{cases} \tag{3.5}$$

Clearly, $\varphi(\mathbf{x} + \mathbf{d_i}) = \varphi(\mathbf{x}) + \varphi(\mathbf{d_i})$, so that writing $\varphi(\mathbf{x}) = z$ and $\varphi(\mathbf{d_i}) = z_i$, (3.5) can be rewritten as

$$\eta(\mathbf{x} + \mathbf{d_i}) = \begin{cases} +1 & \text{if } f(z + z_i) \in \mathcal{B} \\ -1 & \text{if } f(z + z_i) \notin \mathcal{B}. \end{cases} \tag{3.6}$$

Moreover, if $\mathbf{x}$ runs over the elements of the box N-lattice

$$B = \{\mathbf{x} = (x_1 b_1, x_2 b_2, \dots, x_n b_n) : \ 0 \le x_i \le t_i \text{ for } i = 1, 2, \dots, n\}$$

then z runs over the box

$$\begin{aligned} B' &= \{\varphi(\mathbf{x}) : \ \mathbf{x} \in B\} \\ &= \{x_1 b_1 v_1 + x_2 b_2 v_2 + \cdots + x_n b_n v_n : \ x_i \in \mathbb{N} \cup \{0\}, \ 0 \le x_i \le t_i\} \subseteq \mathbb{F}_q. \end{aligned}$$

Clearly, for all $u \in \mathbb{F}_q$ we have

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

where ψ_1 denotes the canonical character of $\mathbb{F}_q$ thus (3.6) can be rewritten as

$$\eta(\mathbf{x} + \mathbf{d_i}) = 2\left(\frac{1}{q}\sum_{b\in\mathcal{B}}\sum_{h\in\mathbb{F}_q}\psi_1\left(h(f(z+z_i)-b)\right) - \frac{1}{2}\right)$$

so that the sum in the definition of $Q_k(\eta)$ can be written as

$$\sum_{\mathbf{x}\in B}\eta(\mathbf{x}+\mathbf{d_1})\ldots\eta(\mathbf{x}+\mathbf{d_k}) = \sum_{z\in B'} 2^k \prod_{i=1}^{k}\left(\frac{1}{q}\sum_{b\in\mathcal{B}}\sum_{h\in\mathbb{F}_q}\psi_1\left(h(f(z+z_i)-b)\right)-\frac{1}{2}\right). \tag{3.7}$$

Separating the $h=0$ term in the general factor of the product we get

$$\begin{aligned}\frac{1}{q}\sum_{b\in\mathcal{B}}\sum_{h\in\mathbb{F}_q}\psi_1\left(h(f(z+z_i)-b)\right)-\frac{1}{2} &= \left(\frac{1}{q}\sum_{b\in\mathcal{B}}1-\frac{1}{2}\right)\\ &\quad+\frac{1}{q}\sum_{b\in\mathcal{B}}\sum_{h\in\mathbb{F}_q^*}\psi_1\left(h(f(z+z_i)-b)\right).\end{aligned}$$

Here we have

$$\begin{aligned}\frac{1}{q}\sum_{b\in\mathcal{B}}1-\frac{1}{2} &= \frac{1}{q}\sum_{j=1}^{n}|\mathcal{B}_j|-\frac{1}{2}=\frac{1}{q}\sum_{j=1}^{n}\frac{p-1}{2}\cdot p^{n-j}-\frac{1}{2}=\frac{1}{2q}(p^n-1)-\frac{1}{2}\\ &= \frac{q-1}{2q}-\frac{1}{2}=-\frac{1}{2q}\end{aligned}$$

so that it follows from (3.7) that

$$
\begin{aligned}
&\left|\sum_{\mathbf{x}\in B}\eta(\mathbf{x}+\mathbf{d_1})\dots\eta(\mathbf{x}+\mathbf{d_k})\right|\\
&=\left|\sum_{z\in B'}2^k\prod_{i=1}^{k}\left(\frac{1}{q}\sum_{b\in\mathcal{B}}\sum_{h\in\mathbb{F}_q^*}\psi_1\left(h(f(z+z_i)-b)\right)-\frac{1}{2q}\right)\right|\\
&=\frac{1}{q^k}\left|\sum_{z\in B'}\left((-1)^k+\sum_{j=1}^{k}(-1)^{k-j}2^j\sum_{(b_1,\dots,b_j)\in\mathcal{B}^j}\ \sum_{(h_1,\dots,h_j)\in\left(\mathbb{F}_q^*\right)^j}\ \sum_{1\le i_1<\dots<i_j\le k}\right.\right.\\
&\qquad\left.\left.\psi_1(h_1(f(z+z_{i_1})-b_1)+\dots+h_j(f(z+z_{i_j})-b_j))\right)\right|\\
&\le 1+\frac{1}{q^k}\sum_{j=1}^{k}2^j\sum_{(h_1,\dots,h_j)\in\left(\mathbb{F}_q^*\right)^j}\ \sum_{1\le i_1<\dots<i_j\le k}\\
&\qquad\left|\sum_{z\in B'}\psi_1(h_1(f(z+z_1))+\dots+h_j(f(z+z_j)))\right|\times\\
&\qquad\times\left|\sum_{(b_1,\dots,b_j)\in\mathcal{B}^j}\psi_1(-h_1b_1-\dots-h_jb_j)\right|. \qquad (3.8)
\end{aligned}
$$

In order to estimate the penultimate sum we will need Weil's theorem [20]:

Lemma 1 *If q is a prime power, ψ is a nontrivial additive character of $\mathbb{F}_q$, and $g(x)\in\mathbb{F}_q[x]$ is a polynomial of degree d with $d\ge 1$, then we have*

$$\left|\sum_{z\in\mathbb{F}_q}\psi(g(z))\right|\le (d-1)q^{1/2}.$$

We will use the incomplete version of this theorem:

Lemma 2 *Assume that $q=p^n$ is a prime power, ψ is a nontrivial additive character of $\mathbb{F}_q$, and $g(x)\in\mathbb{F}_q[x]$ is a polynomial of degree d with $d\ge 2$ and $\overline{B}\subseteq\mathbb{F}_q$ is a box of form*

$$\overline{B}=\{\sum_{j=1}^{n}j_iv_i:\ 0\le j_i\le t_i \textit{ for } i=1,2,\dots,n\}$$

(where $v_1, \dots, v_n$ are linearly independent over the prime field of $\mathbb{F}_q$). Then we have

$$\left| \sum_{z \in \overline{B}} \psi(g(z)) \right| \le (d-1) q^{1/2} (2 + \log p)^n. \tag{3.9}$$

Proof of Lemma 2. This can be derived from the complete version in Lemma 1 in the standard way; for the sake of completeness we sketch the proof. By $\psi \ne \psi_0$ for any $u, b \in \mathbb{F}_q$ we have

$$\frac{1}{q} \sum_{h \in \mathbb{F}_q} \psi(h(u-b)) = \begin{cases} 1 & \text{if } u = b \\ 0 & \text{if } u \ne b, \end{cases}$$

and thus

$$\begin{aligned} \left| \sum_{z \in \overline{B}} \psi(g(z)) \right| &= \left| \sum_{u \in \mathbb{F}_q} \psi(g(u)) \sum_{b \in \overline{B}} \frac{1}{q} \sum_{h \in \mathbb{F}_q} \psi(h(u-b)) \right| \\ &\le \frac{1}{q} \sum_{h \in \mathbb{F}_q} \left| \sum_{u \in \mathbb{F}_q} \psi(g(u) + hu) \right| \left| \sum_{b \in \overline{B}} \psi(hb) \right| \end{aligned} \tag{3.10}$$

By deg $g(u) = d \ge 2$ we have

$$\deg\, (g(u) + hu) = \deg\, g(u) \ge 2$$

for every $h \in \mathbb{F}_q$, thus we may estimate the middle sum by using Lemma 1, and then we obtain

$$\left| \sum_{u \in \mathbb{F}_q} \psi(g(u) + hu) \right| \le (d-1) q^{1/2} \text{ for every } h \in \mathbb{F}_q. \tag{3.11}$$

Moreover, by formula (3.21) in [17], for $\psi \ne \psi_0$ and any box $\overline{B}$ of the given type we have

$$\sum_{h \in \mathbb{F}_q} \left| \sum_{b \in \overline{B}} \psi(hb) \right| \le q (2 + \log p)^n. \tag{3.12}$$

(3.9) follows from (3.10) by (3.11) and (3.12), and this completes the proof of Lemma 2.

To complete the proof of Theorem 1 it suffices to prove

Lemma 3 *In the penultimate sum in* (3.8) *we have*

$$\deg\big(h_1 f(z+z_{i_1})+\dots+h_j f(z+z_{i_j})\big)\geq 2 \tag{3.13}$$

for every $(h_1,\dots,h_j)\in(\mathbb{F}_q^*)^j$ *and* $1\leq i_1<\dots<i_j\leq k$.

First we will show that, indeed, (3.4) follows from (3.8) and Lemma 3, and we will return to the proof of Lemma 3 after this.

By Lemma 3, each of the polynomials $h_1 f(z+z_1)+\dots+h_j f(z+z_j)$ in the penultimate sum in (3.8) is of degree greater than 1, and clearly, each of them has degree at most $\deg f=\ell$. Thus we may use Lemma 2 to estimate these sums, and then we get

$$\left|\sum_{z\in B'}\psi_1(h_1 f(z+z_1)+\dots+h_j f(z+z_j))\right|\leq(\ell-1)q^{1/2}(2+\log p)^n.$$

Thus it follows from (3.8) that

$$\begin{aligned}\left|\sum_{\mathbf{x}\in B}\eta(\mathbf{x}+\mathbf{d_1})\dots\eta(\mathbf{x}+\mathbf{d_k})\right| &\leq 1+\frac{1}{q^k}\sum_{j=1}^{k}2^j\sum_{(h_1,\dots,h_j)\in(\mathbb{F}_q^*)^j}\ \sum_{1\leq i_1<\dots<i_j\leq k}\\ &\qquad(\ell-1)q^{1/2}(2+\log p)^n\prod_{i=1}^{j}\left|\sum_{b\in\mathcal{B}}\psi_1(h_i b)\right|\\ &=1+\frac{1}{q^k}\sum_{j=1}^{k}2^j(\ell-1)q^{1/2}(2+\log p)^n\binom{k}{j}\\ &\qquad\left(\sum_{h\in\mathbb{F}_q^*}\left|\sum_{b\in\mathcal{B}}\psi_1(hb)\right|\right)^j.\end{aligned} \tag{3.14}$$

Here we have

$$\begin{aligned}\sum_{h\in\mathbb{F}_q^*}\left|\sum_{b\in\mathcal{B}}\psi_1(hb)\right| &=\sum_{\psi\neq\psi_0}\left|\sum_{b\in\mathcal{B}}\psi(b)\right|=\sum_{\psi\neq\psi_0}\left|\sum_{i=1}^{n}\sum_{b\in B_i}\psi(b)\right|\\ &\leq\sum_{\psi\neq\psi_0}\sum_{i=1}^{n}\left|\sum_{b\in B_i}\psi(b)\right|=\sum_{i=1}^{n}\sum_{\psi\neq\psi_0}\left|\sum_{b\in B_i}\psi(b)\right|\end{aligned}$$

By (3.29) in [17] we have

$$\sum_{\psi \neq \psi_0} \left| \sum_{b \in B_i} \psi(b) \right| < q \left(\log p + \frac{3}{2} \right)$$

so that

$$\sum_{h \in \mathbb{F}_q^*} \left| \sum_{b \in B} \psi_1(hb) \right| < \sum_{i=1}^{n} q \left(\log p + \frac{3}{2} \right) = nq \left(\log p + \frac{3}{2} \right). \tag{3.15}$$

Thus it follows from (3.14) that

$$\begin{aligned}
\left| \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d_1}) \dots \eta(\mathbf{x} + \mathbf{d_k}) \right| &\le 1 + \frac{1}{q^k} \sum_{j=1}^{k} 2^j (\ell - 1) q^{1/2} (2 + \log p)^n \\
&\quad \binom{k}{j} \left(nq \left(\log p + \frac{3}{2} \right) \right)^j \\
&= 1 + \frac{\ell - 1}{q^k} q^{1/2} (2 + \log p)^n \sum_{j=1}^{k} \binom{k}{j} \\
&\quad \left(2nq \left(\log p + \frac{3}{2} \right) \right)^j \\
&< 1 + \frac{\ell - 1}{q^k} q^{1/2} (2 + \log p)^n \\
&\quad \left(1 + 2nq \left(\log p + \frac{3}{2} \right) \right)^k \\
&< 1 + (\ell - 1) q^{1/2} (2 + \log p)^n \left(2n \left(\log p + 2 \right) \right)^k \\
&< 2^k \ell n^k q^{1/2} (\log p + 2)^{n+k}.
\end{aligned}$$

This holds for every $B, \mathbf{d_1}, \dots, \mathbf{d_k}$ which proves (3.4) in the theorem.

It remains to prove Lemma 3.

Proof of Lemma 3 Write

$$F(z) = h_1 f(z + z_{i_1}) + \dots + h_j f(z + z_{i_j}),$$

and assume that contrary to (3.13) we have

$$\deg\ F(z) = 0 \text{ or } 1, \text{ or } F(z) \equiv 0. \tag{3.16}$$

By the assumption $\deg f = \ell < p$ in (3.2), for every $z_i \in \mathbb{F}_q$ we may use the Taylor formula to write

$$f(z+z_i) = \sum_{m=0}^{\ell} \frac{z_i^m}{m!} f^{(m)}(z).$$

(where $f^{(m)}(z)$ denotes the m-th derivative of $f(z)$). By (3.3) we have

$$j \le k \le \ell - 1, \tag{3.17}$$

thus we may rewrite this as

$$f(z+z_i) = \sum_{m=0}^{j-1} \frac{z_i^m}{m!} f^{(m)}(z) + r_i(z)$$

with some polynomial $r_i(z)$ of degree at most $\ell-(j-1)-1 = \ell - j$. Thus $F(z)$ can be written as

$$\begin{aligned} F(z) &= \sum_{t=1}^{j} h_t \sum_{m=0}^{j-1} \frac{z_{i_t}^m}{m!} f^{(m)}(z) + \sum_{t=1}^{j} h_t r_{i_t}(z) \qquad (3.18)\\ &= \sum_{m=0}^{j-1} \left(\sum_{t=1}^{j} h_t z_{i_t}^m \right) \frac{1}{m!} f^{(m)}(z) + R(z) \qquad (3.19) \end{aligned}$$

where $R(z)$ is a polynomial of degree

$$\deg R(z) \le \ell - j \quad (\text{or } R(z) \equiv 0), \tag{3.20}$$

while the polynomials $f^m(z)$ with $0 \le m \le j-1$ are of degree

$$\deg f^{(m)}(z) = \ell - m \ge \ell - j + 1 \tag{3.21}$$

so that by (3.17) we have

$$\deg f^{(m)}(z) \ge 2. \tag{3.22}$$

By our indirect assumption (3.16), it follows from (3.19), (3.20), (3.21) and (3.22) that the coefficient of every $f^{(m)}(z)$ in (3.19) must be 0:

$$\begin{aligned} h_1 + h_2 + \dots + h_j &= 0, \\ z_{i_1}h_1 + z_{i_2}h_2 + \dots + z_{i_j}h_j &= 0, \\ &\vdots \\ z_{i_1}^{j-1}h_1 + z_{i_2}^{j-1}h_2 + \dots + z_{i_j}^{j-1}h_j &= 0. \end{aligned}$$

This is a system of linear equations in the variables $h_1, h_2, \dots, h_j$ whose determinant is a Vandermonde determinant with generating elements $z_{i_1}, z_{i_2}, \dots, z_{i_j}$ which are pairwise distinct, thus it is nonzero. It follows that the system has only the trivial solution

$$h_1 = h_2 = \dots = h_j = 0,$$

which contradicts our assumption $(h_1, h_2, \dots, h_j) \in (\mathbb{F}_q^*)^j$, and this completes the proof of the lemma.

4 The family complexity of a large subfamily of the binary lattices studied in Theorem 1

Suppose that by using construction (3.1) we want to form a large family of n-dimensional binary p-lattices η each of them having strong pseudorandom properties, more precisely, we want $Q_k(\eta)$ to be "small" for every η belonging to the family and every $k \in \mathbb{N}$ less than a certain parameter $K \in \mathbb{N}$. By Theorem 1 the lattice $\eta = \eta_f$ in (3.1) satisfies this requirement if conditions (3.2) and (3.3) in Theorem 1 hold with $\ell = \deg f < p$ and K in place of $k+1$: $K \le \ell < p$. On the other hand, if $\ell = \deg f$ increases then the computational complexity of the construction also increases, thus we have to keep $\ell = \deg f$ possibly small. To balance these two requirements, we take polynomials of degree exactly K, i.e., wee consider the family

$$\mathcal{G}_K = \{\eta : \ \eta = \eta_f \text{ is of form (3.1) with } f \in \mathbb{F}_q[x], \ \deg f = K\}.$$

Note that the coefficients of f can be chosen in $(q-1)q^K$ ways so that

$$|\mathcal{G}_K| = (q-1)q^K. \tag{4.1}$$

Now we will define a subfamily $\mathcal{H}_K$ of $\mathcal{G}_K$ which is just slightly smaller than $\mathcal{G}_K$, and we will show that it is of high family complexity (it follows from $\mathcal{H}_K \subseteq \mathcal{G}_K$ that $\Gamma(\mathcal{H}_K) \le \Gamma(\mathcal{G}_K)$ so that then $\mathcal{G}_K$ is also of high complexity), it is also collision free, and it possesses the strict avalanche property. Thus, indeed, both the lattices belonging to this family $\mathcal{H}_K$ and the family itself will possess all the pseudorandom properties studied by us.

Define S^+ and S^- as the set of the polynomials of the following form:

$$S^+ = \{x^K + x^2 g(x) + x + 1 : \ g(x) \in \mathbb{F}_q[x], \ \deg g(x) \le K-3 \text{ or } g(x) \equiv 0\},$$
$$S^- = \{x^K + x^2 g(x) - x - 1 : \ g(x) \in \mathbb{F}_q[x], \ \deg g(x) \le K-3 \text{ or } g(x) \equiv 0\},$$

and let

$$\mathcal{S} = S^+ \cup S^-$$

and

$$\mathcal{H}_K = \{\eta : \ \eta = \eta_f \text{ with some } f \in \mathcal{S}\}.$$

Note that clearly

$$|\mathcal{S}| = \left|S^+\right| + \left|S^-\right| = 2q^{K-2},$$

and in the next section we will show that $\mathcal{H}_K = \mathcal{H}_K(S)$ is collision free so that

$$|\mathcal{H}_K| = |\mathcal{S}| = 2q^{K-2} \tag{4.2}$$

which is indeed, just slightly smaller than $|\mathcal{G}_K|$ in (4.1).

Now we will prove that $\mathcal{H}_K$ is of high complexity:

Theorem 2 *Define $q = p^n$, $\mathcal{S}$ and $\mathcal{H}_K$ as above, and assume that $K \in \mathbb{N}$ is such that*

$$3 < K < p. \tag{4.3}$$

Then we have

$$\Gamma(\mathcal{H}_K) \geq K - 2. \tag{4.4}$$

Note that by (1.4) and (4.2) we have

$$\Gamma(\mathcal{H}_K) \leq \frac{\log |\mathcal{H}_K|}{\log 2} = \frac{\log 2 + (K-2)\log q}{\log 2} < \frac{2}{\log 2}(K-2)\log q$$

so that our lower bounds (4.4) is worse than the best possible one by at most a factor $c \log q$.

Proof of Theorem 2 We will use a modified and extended version of the interpolation method applied in [1]. While this method gives slightly weaker estimate than the optimal one, it has the advantage that it is more flexible than the method used in [4] and it can be adapted to more general situations. We will use the same notations as in Section 5.

In order to prove (4.4) we have to show that for any specification

$$\eta(\mathbf{x_1}) = \varepsilon_1,\ \eta(\mathbf{x_2}) = \varepsilon_2, \dots, \eta(\mathbf{x_{K-2}}) = \varepsilon_{K-2}, \tag{4.5}$$

of length $K-2$ there is an $f \in S$ such that the associated binary lattice $\eta = \eta_f\ :\ I_p^n \to \{-1, +1\}$ satisfies it. For each of the vectors $\mathbf{x_i} \in I_p^n$ considered in (4.5) we write $\varphi(\mathbf{x_i}) = y_i$ and $\mathcal{Y} = \{y_1, y_2, \dots, y_{K-2}\}$. Then by (3.1),

$$\eta(\mathbf{x_i}) = \varepsilon_i$$

holds for some $\eta = \eta_f$ if and only if (4.6)

$$f(y_i) \in \mathcal{B} \text{ if } \varepsilon_i = +1 \qquad \text{and } f(y_i) \notin \mathcal{B} \text{ if } \varepsilon_i = -1. \tag{4.6}$$

Since clearly $1 \in B_1 \subseteq \mathcal{B}$ for $p > 3$ and $1 \in B_2 \subseteq \mathcal{B}$ for $p = 3$, and $-1 \notin \mathcal{B}$, thus (4.6) follows from

$$f(y_i) = \varepsilon_i \tag{4.7}$$

so that it suffices to show that there is an $f \in \mathcal{S} = S^+ \cup S^-$ such that (4.7) holds for $i = 1, 2, \dots, K-2$.

If $0 \notin \mathcal{Y}$, or $0 \in \mathcal{Y}$ and for the i_0 with $y_{i_0} = 0$ we have

$$\varepsilon_{i_0} = +1, \tag{4.8}$$

then we look for such an f in S^+, i.e., we represent it in the form

$$f(y) = y^K + y^2 g(y) + y + 1. \tag{4.9}$$

Clearly, $f(0) = +1$ for every f of this form, so that if $0 \in \mathcal{Y}$ then by (4.8), (4.7) holds trivially for $i = i_0$. Thus we may restrict ourselves to $i \neq i_0$ in (4.7), i.e., we are looking for a

$$g \in \mathbb{F}_q[y] \text{ with } \deg g(y) \leq K - 3 \text{ or } g(y) \equiv 0 \tag{4.10}$$

such that

$$f(y_i) = y_i^K + y_i^2 g(y_i) + y_i + 1 = \varepsilon_i$$

for $i \neq i_0$. If $i \neq i_0$, i.e., $y_i \neq 0$, then the last equality can be rewritten in the form

$$g(y_i) = -y_i^{K-2} + \frac{\varepsilon_i - y_i - 1}{y_i^2} \text{ (for } i \neq i_0). \tag{4.11}$$

Since i may assume at most $K-2$ values here, thus there is an interpolation polynomial g of form (4.10) which satisfies (4.11) for every $i \neq i_0$ (which can be determined by Lagrange or Newton interpolation) and then the polynomial f defined by (4.9) is of the desired properties.

It remains to consider the case when $0 \in \mathcal{Y}$ and for the i_0 with $y_{i_0} = 0$ we have

$$\varepsilon_{i_0} = -1.$$

Then we look for f in S^-, i.e., we represent it in the form

$$f(y) = y^K + y^2 g(y) - y - 1.$$

Then again (4.7) holds trivially for $i = i_0$. It remains to find a polynomial g of form (4.10) such that

$$f(y_i) = y_i^K + y_i^2 g(y_i) - y_i - 1 = \varepsilon_i$$

or, in equivalent form,

$$g(y_i) = -y_i^{K-2} + \frac{\varepsilon_i + y_i + 1}{y_i^2} \text{ (for } i \neq i_0\text{)}.$$

Again, such a polynomial g can be found by interpolation, and this completes the proof of Theorem 2.

5 The family studied in Section 4 is collision free and it possesses the strict avalanche property

We will prove

Theorem 3 *Using the notations and assumptions of Section 4 we have*

$$m(\mathcal{H}_K) > \frac{1}{2}\left(q - 6(K-1)n^2 q^{1/2}\left(\log p + \frac{3}{2}\right)^2\right). \tag{5.1}$$

Note that if

$$6(K-1)n^2\left(\log p + \frac{3}{2}\right)^2 < q^{3/2} \tag{5.2}$$

then the right hand side of (5.1) is positive so that $m(\mathcal{H}_K) > 0$ and thus $\mathcal{H}_K$ is collision free. This proves

Corollary 1 *If* (5.2) *holds then* $\mathcal{H}_K$ *is collision free.*

Moreover, if $q \to \infty$ and

$$Kn^2(\log p)^2 = o(q^{3/2}) \tag{5.3}$$

then it follows from (5.1) that

$$m(\mathcal{H}_K) > \left(\frac{1}{2} - o(1)\right) q$$

which proves

Corollary 2 *If* (5.3) *holds then* $\mathcal{H}_K$ *possesses the strict avalanche property.*

Proof of Theorem 3 Assume that $f, g \in \mathcal{S}$ and $f \neq g$. Then as at the beginning of the proof of Theorem 2 in [9] we have

$$d(\eta_f, \eta_g) = \frac{1}{2}\left(q - \sum_{\mathbf{x} \in I_p^n} \eta_f(\mathbf{x})\eta_g(\mathbf{x})\right). \tag{5.4}$$

If we write $\varphi(\mathbf{x}) = z$, then in the same way as in the proof of Theorem 1 we get

$$\begin{aligned} \eta_f(\mathbf{x}) &= 2\left(\frac{1}{q}\sum_{b\in\mathcal{B}}\sum_{h\in\mathbb{F}_q} \psi_1(h(f(z)-b)) - \frac{1}{2}\right) \\ &= 2\left(\frac{1}{q}\sum_{b\in\mathcal{B}}\sum_{h\in\mathbb{F}_q^*} \psi_1(h(f(z)-b)) - \frac{1}{2q}\right) \end{aligned} \tag{5.5}$$

and

$$\eta_g(\mathbf{x}) = 2\left(\frac{1}{q}\sum_{b\in\mathcal{B}}\sum_{h\in\mathbb{F}_q^*} \psi_1(h(g(z)-b)) - \frac{1}{2q}\right). \tag{5.6}$$

If $\mathbf{x}$ runs over the elements of I_p^n then $\varphi(\mathbf{x}) = z$ runs over the elements of $\mathbb{F}_q$. Thus by (5.5) and (5.6), the sum in (5.4) can be rewritten as

$$\begin{aligned} \sum_{\mathbf{x}\in I_p^n} \eta_f(\mathbf{x})\eta_g(\mathbf{x}) &= 4\left(\frac{1}{q}\sum_{b\in\mathcal{B}}\sum_{h\in\mathbb{F}_q^*} \psi_1(h(f(z)-b)) - \frac{1}{2q}\right) \times \\ &\qquad \times \left(\frac{1}{q}\sum_{b\in\mathcal{B}}\sum_{h\in\mathbb{F}_q^*} \psi_1(h(g(z)-b)) - \frac{1}{2q}\right) \\ &= 4\left(\sum\nolimits_1 + \sum\nolimits_2 + \sum\nolimits_3\right) + \frac{1}{q^2} \end{aligned} \tag{5.7}$$

where

$$\sum\nolimits_1 = \frac{1}{q^2} \sum_{h_1 \in \mathbb{F}_q^*} \sum_{h_2 \in \mathbb{F}_q^*} \sum_{z \in \mathbb{F}_q} \psi_1(h_1 f(z) + h_2 g(z)) \sum_{b_1 \in \mathcal{B}} \psi_1(-h_1 b_1) \sum_{b_2 \in \mathcal{B}} \psi_1(-h_2 b_2),$$

$$\sum\nolimits_2 = \frac{1}{2q^2} \sum_{h \in \mathbb{F}_q^*} \sum_{z \in \mathbb{F}_q} \psi_1(h(f(z))) \sum_{b \in \mathcal{B}} \psi_1(-hb)$$

and

$$\sum\nolimits_3 = \frac{1}{2q^2} \sum_{h \in \mathbb{F}_q^*} \sum_{z \in \mathbb{F}_q} \psi_1(h(g(z))) \sum_{b \in \mathcal{B}} \psi_1(-hb).$$

We have

$$\sum\nolimits_1 = \frac{1}{q^2} \sum_{h_1 \in \mathbb{F}_q^*} \sum_{h_2 \in \mathbb{F}_q^*} \left| \sum_{z \in \mathbb{F}_q} \psi_1(h_1 f(z) + h_2 g(z)) \right| \left| \sum_{b_1 \in \mathcal{B}} \psi_1(-h_1 b_1) \right| \times$$
$$\times \left| \sum_{b_2 \in \mathcal{B}} \psi_1(-h_2 b_2) \right|. \tag{5.8}$$

We will show that for every $h_1, h_2 \in \mathbb{F}_q^*$ we have

$$\deg\ (h_1 f(z) + h_2 g(z)) \geq 1. \tag{5.9}$$

Indeed, if $h_1 \neq -h_2$, then the coefficient of x^K in $h_1 f(z) + h_2 g(z)$ is nonzero. If $h_1 = -h_2$ and both $f(z)$ and $g(z)$ belong to S^+ or both belong to S^-, then, by $f \neq g$ the coefficient of at least one of $x^2, x^3, \ldots, x^{K-1}$ is nonzero. Finally, if $h_1 = -h_2$ and one of f and g belongs to S^+ and the other one to S^- then the coefficient of x is $\pm 2h_1 \neq 0$ (note that $p > 2$). This proves (5.9) so that we may apply Lemma 1 to estimate the middle sum in (5.8). Clearly, the degree of the polynomial in (5.9) is at most K, thus we obtain

$$\left| \sum_{z \in \mathbb{F}_q} \psi_1(h_1 f(z) + h_2 g(z)) \right| \leq (K-1) q^{1/2}$$

(uniformly for $h_1, h_2 \in \mathbb{F}_q^*$). Thus it follows from (5.8) that

$$\left| \sum\nolimits_1 \right| \leq \frac{1}{q^2} (K-1) q^{1/2} \left(\sum_{h \in \mathbb{F}_q^*} \left| \sum_{b \in B} \psi_1(-hb) \right| \right)^2$$

whence, by (3.15),

$$\left|\sum\nolimits_1\right| \le \frac{1}{q^2}(K-1)q^{1/2}\left(nq\left(\log p+\frac{3}{2}\right)\right)^2 = (K-1)n^2q^{1/2}\left(\log p+\frac{3}{2}\right)^2. \tag{5.10}$$

Clearly we have

$$\left|\sum\nolimits_2\right| \le \frac{1}{2q^2}\sum_{h\in\mathbb{F}_q^*}\left|\sum_{z\in\mathbb{F}_q}\psi_1(hf(z))\right|\left|\sum_{b\in B}\psi_1(-hb))\right|.$$

Again we may estimate the middle sum by Lemma 1 and then we may use (3.15):

$$\begin{aligned}\left|\sum\nolimits_2\right| &\le \frac{1}{2q^2}\sum_{h\in\mathbb{F}_q^*}(K-1)q^{1/2}\left|\sum_{b\in B}\psi_1(-hb))\right| \\ &= \frac{1}{2q^2}(K-1)q^{1/2}\sum_{h\in\mathbb{F}_q^*}\left|\sum_{b\in B}\psi_1(-hb))\right| \\ &\le \frac{1}{2q^2}(K-1)q^{1/2}nq\left(\log p+\frac{3}{2}\right) \\ &= \frac{1}{2q^{1/2}}(K-1)n\left(\log p+\frac{3}{2}\right),\end{aligned} \tag{5.11}$$

and in the same way,

$$\left|\sum\nolimits_3\right| \le \frac{1}{2q^{1/2}}(K-1)n\left(\log p+\frac{3}{2}\right). \tag{5.12}$$

It follows from (5.7), (5.10), (5.11) and (5.12) that

$$\begin{aligned}\left|\sum_{\mathbf{x}\in I_p^n}\eta_f(\mathbf{x})\eta_g(\mathbf{x})\right| &\le 4\Bigg((K-1)n^2q^{1/2}\left(\log p+\frac{3}{2}\right)^2 \\ &\quad + \frac{1}{q^{1/2}}(K-1)n\left(\log p+\frac{3}{2}\right)\Bigg)+\frac{1}{q^2} \\ &< 6(K-1)n^2q^{1/2}\left(\log p+\frac{3}{2}\right)^2.\end{aligned} \tag{5.13}$$

(5.1) follows from (5.4) and (5.13) which completes the proof of the theorem.

References

[1] R. Ahlswede, L. H. Khachatrian and C. Mauduit, *A complexity measure for families of binary sequences*, Period. Math. Hungar. 46 (2003), 107-118.

[2] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, *Measures of pseudorandomness for finite sequences: typical values*, Proc. London Math. Soc. 95 (2007), 778-812.

[3] J. Cassaigne, C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences VII: The measures of pseudorandomness*, Acta Arith. 103 (2002), 97-118.

[4] K. Gyarmati, *On the complexity of a family related to the Legendre symbol*, Period. Math. Hungar. 58 (2009), 209-215.

[5] K. Gyarmati, C. Mauduit and A. Sárközy, *Constructions of pseudorandom binary lattices*, Unif. Distrib. Theory 4 (2009), 59-80.

[6] K. Gyarmati, C. Mauduit and A. Sárközy, *Measures of pseudorandomness of finite binary lattices, I. (The measures Q_k, normality.)*, Acta Arith. 144 (2010), 295-313

[7] K. Gyarmati, C. Mauduit and A. Sárközy, *Measures of pseudorandomness of finite binary lattices, II. (The symmetry measures.)*, Ramanujan J. 25 (2011), 155-178.

[8] K. Gyarmati, C. Mauduit and A. Sárközy, *Measures of pseudorandomness of finite binary lattices, III. (Q_k, correlation, normality, minimal values)*, Unif. Distrib. Theory 5 (2010), 183-207.

[9] K. Gyarmati, C. Mauduit and A. Sárközy, *Measures of pseudorandomness of families of binary lattices, I (Definitions, a construction using quadratic characters.)*, Publ. Math. Debrecen 79 (2011).

[10] K. Gyarmati, A. Sárközy and C. L. Stewart, *On Legendre symbol lattices*, Unif. Distrib. Theory 4 (2009), 81-95.

[11] P. Hubert, C. Mauduit and A. Sárközy, *On pseudorandom binary lattices*, Acta Arith. 125 (2006), 51-62.

[12] Y. Kohayakawa, C. Mauduit, C. G. Moreira, V. Rödl, *Measures of pseudorandomness for finite sequences: minimum and typical values*, Proceedings of WORDS'03, 159-169, TUCS Gen. Publ., 27, Turku Cent. Comput. Sci., Turku, 2003.

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

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

[15] C. Mauduit and A. Sárközy, *Construction of pseudorandom binary sequences by using the multiplicative inverse*, Acta Math. Hungar. 108 (2005), 239-252.

[16] C. Mauduit and A. Sárközy, *On large families of pseudorandom binary lattices*, Unif. Distr. Theory 2 (2007), 23-37.

[17] C. Mauduit and A. Sárközy, *Construction of pseudorandom binary lattices by using the multiplicative inverse*, Monatsh. Math. 153 (2008), 217-231.

[18] V. Tóth, *Collision and avalanche effect in families of pseudorandom binary sequences*, Period. Math. Hungar. 55 (2007), 185-196.

[19] V. Tóth, *The study of collision and avalanche effect in a family of pseudorandom binary sequences*, Period. Math. Hungar. 59 (2009), 1-8.

[20] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduissent*, Act. Sci. Ind. 1041, Hermann, Paris, 1948.