On new measures of pseudorandomness of binary lattices

Katalin Gyarmati

Abstract

Hubert, Mauduit and Sárközy introduced the pseudorandom measure of order ℓ of binary lattices. This measure studies the pseudorandomness only on box lattices of very special type. In certain applications one may need measures covering a more general situation. In this paper the line measure and the convex measure are introduced.

2000 AMS Mathematics Subject Classification: 11K45.

List of keywords and phrases: pseudorandom, binary lattice.

1 Introduction

In [10] Mauduit and Sárközy initiated a new constructive approach to study pseudorandomness of binary sequences

$$E_N = \{e_1, \dots, e_N\} \in \{-1, +1\}^N. \tag{1}$$

Research partially supported by Hungarian National Foundation for Scientific Research, Grants No. K67676 and PD72264 and the János Bolyai Research Fellowship.

They introduced several different measures of pseudorandomness of sequences of this type: the well-distribution measure; the correlation measure of order k; the combined pseudorandom measure of order k; the normality measure of order k. They also showed that the Legendre symbol forms a "good" pseudorandom sequence in terms of these measures. Later many related papers have been written in which these pseudorandom measures are studied, further sequences are tested for pseudorandomness, or further constructions are given for sequences with good pseudorandom properties. In [6] with Mauduit and Sárközy we surveyed some further details of the related work, and we also presented a list of references.

In [9] Hubert, Mauduit and Sárközy extended this theory of pseudorandomness of binary sequences 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*.

They extended the definition of binary sequences to n dimensions by considering functions of type

$$\eta(\mathbf{x}) : \ I_N^n \to \{-1, +1\}. \tag{2}$$

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 [8] the definition of I_N^n was extended to more general lattices in the following way: Let $\mathbf{u_1}, \mathbf{u_2}, \ldots, \mathbf{u_n}$ be n linearly independent 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 $(0, \ldots, 0, z_i, 0, \ldots, 0)$ (with $z_i \in \mathbb{N}$). Let $t_1, t_2, \ldots, t_n$ be integers with $0 \le t_1, t_2, \ldots, t_n < N$. Then we call the set

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

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

In [9] 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 [8]):

Definition 1 *The* pseudorandom measure of order ℓ *of the binary lattice η of form* (2) *is defined by*

$$Q_\ell(\eta) = \max_{B, \mathbf{d_1}, \ldots, \mathbf{d}_\ell} \left| \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d_1}) \cdots \eta(\mathbf{x} + \mathbf{d}_\ell) \right|, \tag{3}$$

where the maximum is taken over all distinct $\mathbf{d_1}, \ldots, \mathbf{d}_\ell \in I_N^n$ and all box N-lattices B such that $B + \mathbf{d_1}, \ldots, B + \mathbf{d}_\ell \subseteq I_N^n$.

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 ℓ and "large" N the measure $Q_\ell(\eta)$ is "small" (much smaller, than the trivial upper bound N^n). This terminology is justified by the fact that, as it was proved in [9], for a truly random binary lattice defined on I_N^n and for fixed ℓ the measure $Q_\ell(\eta)$ is "small"; more precisely, it is less than $N^{n/2}$ multiplied by

a logarithmic factor (see [3] and [4] for more precise results concerning the one-dimensional case). The construction of a binary N-lattice η for which $Q_\ell(\eta)$ is so small (for every fixed ℓ) was also presented in [9]. Later further binary lattices with strong pseudorandom properties have been constructed, a list of related references is given in [6].

Based on these facts we may say that η possesses strong pseudorandom properties if $Q_\ell(\eta)$ is small at least for small values of ℓ. However, it may occur that this measure is not sufficient to study pseudorandomness of binary lattices. In certain applications one may need more general measures and indeed in (3) the box lattice B is of very special form.

In [7] we introduced three different types of symmetry measures in order to study the symmetry properties of binary lattices. All these measures were extensions of the one-dimensional symmetry measure introduced and studied in [5]. Other one-dimensional measures can be generalized to higher dimensions similarly. Note that the measure $Q_\ell(\eta)$ in Definition 1 is the n-dimensional generalization of the one-dimensional combined measure $Q_\ell(E_N)$ introduced in [10]:

Definition 2 *The* combined (well-distribution-correlation) measure *of* E_N *is defined by*

$$Q_\ell(E_N) = \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \dots e_{a+jb+d_\ell} \right|$$

where the maximum is taken over all $a, b, t, D = (d_1, d_2, \dots, d_\ell)$ *such that all the subscripts* $a + jb + d_i$ *belong to* $\{1, 2, \dots, N\}$.

Here we will present two further several dimensional generalizations of this measure $Q_\ell(E_N)$. Then we will show that for truly random binary lattices

these measures are small. Then we will present a construction with strong pseudorandom properties.

2 The convex measure

As we mentioned the form of the box-lattices B in the definition $Q_\ell(\eta)$ is very restricted. Clearly, one needs some assumptions on the shape of the sets B in (3), but one must not be too specific. In the following definition we will take the maximum over convex polytopes, which are natural candidates for defining a new measure.

Definition 3 *Let* $\eta : I_N^n \to \{-1, +1\}$ *be a binary lattice. The* convex measure of order ℓ *of* η *is defined by*

$$X_\ell(\eta) = \max_{K, \mathbf{d_1}, \ldots, \mathbf{d}_\ell} \left| \sum_{\mathbf{x} \in K \cap I_N^n} \eta(\mathbf{x} + \mathbf{d_1}) \ldots \eta(\mathbf{x} + \mathbf{d}_\ell) \right|, \tag{4}$$

where the maximum is taken over all distinct $\mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d}_\ell \in I_N^n$ *and all convex polytopes* $K \subseteq [0, N-1]^n$ *such that* $K + \mathbf{d_1}, \ldots, K + \mathbf{d}_\ell \subseteq [0, N-1]^n$.

The convex measure $X_\ell(\eta)$ and the pseudorandom measure $Q_\ell(\eta)$ are probably independent of each other but it seems very difficult to prove this.

3 The line measure

Both the convex measure and pseudorandom measure can be estimated by the line measure defined in this section. In order to introduce this new measure we need a definition from [7].

Definition 4 *$L \subseteq I_N^n$ is a* segment *if L is of the form*

$$L = \{\mathbf{x} = (x_1, \ldots, x_n) : \ x_1 = a_1 t + b_1, \ldots, x_n = a_n t + b_n, \ t \in \{0, 1, \ldots, M-1\}\}$$

(with $M \leq N$) where $a_i, b_i \in \mathbb{Z}$ for $i = 1, 2, \ldots, n$ and $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$.

Next we introduce the line measure.

Definition 5 *Let $I_N^n \to \{-1, +1\}$ be a binary lattice. The line measure of order ℓ of η is defined by*

$$\begin{aligned} L_\ell(\eta) &= \max_{L, \mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d}_\ell} |V(\eta, L, D)| \\ &= \max_{L, \mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d}_\ell} \left| \sum_{\mathbf{x} \in \mathbf{L}} \eta(\mathbf{x} + \mathbf{d_1}) \ldots \eta(\mathbf{x} + \mathbf{d}_\ell) \right| \end{aligned}$$

where the maximum is taken over all distinct $\mathbf{d_1}, \ldots, \mathbf{d}_\ell$ and all segments L such that $L + \mathbf{d_1}, \ldots, L + \mathbf{d}_\ell \subseteq I_N^n$.

We will show that the measures $X_\ell(\eta)$, $Q_\ell(\eta)$ can be estimated in terms of $L_\ell(\eta)$:

Theorem 1 *For every binary lattice $\eta : \ I_N^n \to \{-1, +1\}$ we have*

$$X_\ell(\eta) \leq N^{n-1} L_\ell(\eta).$$

Theorem 2 *For every binary lattice $\eta : \ I_N^n \to \{-1, +1\}$ we have*

$$Q_\ell(\eta) \leq N^{n-1} L_\ell(\eta).$$

Next we give constructions for which the pseudorandom measure or the convex measure is almost minimal, but the line measure is maximal. Consider

two binary N-lattices such that the first binary lattice has possibly small pseudorandom measure, while the second binary lattice has possibly small convex measure. We take one of these two binary lattices and we denote it by η. Consider the segment

$$L = \{\mathbf{x} = (x_1, x_2, \ldots, x_n) : \ x_1 = x_2 = \cdots = x_n = t, \ t \in \{0, 1, \ldots, N-1\}\}.$$

For $\mathbf{x} \in L$ we change the value of $\eta(\mathbf{x})$, for $\mathbf{x} \in L$ let

$$\eta(\mathbf{x}) = 1,$$

while otherwise the value of η remains unchanged. Then in both cases, the pseudorandom measure or the convex measure is small, it differs from the minimal value at most by N, while the line measure is maximal.

Proof of Theorems 1 and 2 The proof is similar to the one in [7], but for the sake of completeness we present it here. Let K be a convex polygon or a box-lattice. We will prove that in both cases we have

$$\left| \sum_{x \in K \cap I_N^n} \eta(\mathbf{x} + \mathbf{d_1}) \ldots \eta(\mathbf{x} + \mathbf{d}_\ell) \right| \leq N^{n-1} L_\ell(\eta). \tag{5}$$

From this the theorem follows. $K + \mathbf{d_1} \cap I_N^n$ is a disjoint union of segments $K_1, K_2, \ldots, K_S$ lying along the lines $L_{i_1,\ldots,i_{n-1}}$ where $L_{i_1,\ldots,i_{n-1}} = \{(i_1, \ldots, i_{n-1}, t) : t \in \mathbb{R}\})$ for $i_1 = 0, 1, \ldots, N-1, \ldots, i_{n-1} = 0, 1, \ldots, N-1$. Then $S \leq N^{n-1}$.

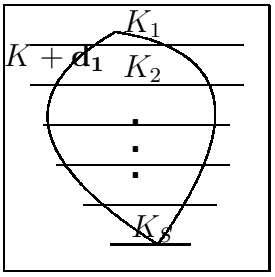

Figure 1.

Using this and the triangle inequality

$$\left| \sum_{x \in K \cap I_N^n} \eta(\mathbf{x} + \mathbf{d_1}) \dots \eta(\mathbf{x} + \mathbf{d}_\ell) \right|$$
$$\leq \sum_{i=1}^{S} \left| \sum_{x \in K_i} \eta(\mathbf{x}) \eta(\mathbf{x} + \mathbf{d_2} - \mathbf{d_1}) \eta(\mathbf{x} + \mathbf{d_3} - \mathbf{d_1}) \dots\dots \eta(\mathbf{x} + \mathbf{d}_\ell - \mathbf{d_1}) \right|$$
$$\leq \sum_{i=1}^{S} L_\ell(\eta) = S L_\ell(\eta) \leq N^{n-1} L_\ell(\eta)$$

which was to be proved.

4 The line measure for truly random binary lattices

In this section we will show that the line measures of a truly random binary lattice $\eta : I_N^2 \to \{-1, +1\}$ are "small". By Theorems 1 and 2 it follows that the convex and pseudorandom measure of a truly random binary lattice are also small (more precisely, we get in this way that they are $< N^{n-1/2+o(1)}$ while the best possible bound is probably $< N^{n/2+o(1)}$). We denote the

probability of an event ξ by $P(\xi)$, and the expectation and standard deviation of a random variable ξ are denoted by $M(\xi)$ and $D(\xi)$, respectively.

Theorem 3 *For every $\varepsilon > 0$ there are numbers $N_0 = N_0(\varepsilon)$ and $\delta = \delta_0(\varepsilon)$ such that if $N > N_0(\varepsilon)$ and we consider a truly random binary lattice $\eta : I_N^2 \to \{-1, +1\}$, i.e., we choose every binary lattice $\eta : I_N^2 \to \{-1, +1\}$ with probability 2^{-N^2}, then we have*

$$P\left(L_\ell(\eta) > \delta N^{1/2}\right) > 1 - \varepsilon \tag{6}$$

and

$$P\left(L_\ell(\eta) < 10(\ell N \log N)^{1/2}\right) > 1 - \varepsilon. \tag{7}$$

Proof of Theorem 3 First we prove (6). Consider the segment $L = \{(0, x_2) : x_2 \in \{0, 1, \ldots, N-1\}\}$. The intersection of this segment and the binary lattice is a binary sequence $E_N = \{e_1, e_2, \ldots, e_N\}$ where

$$e_i = \eta(0, i-1).$$

By Theorem 2 in [4] and using also $Q_\ell(E_N) \geq C_\ell(E_N)$ we have

$$P(Q_\ell(E_N) > \delta N^{1/2}) > 1 - \varepsilon.$$

From this immediately follows (6).

Note that Alon, Kohayakawa, Mauduit, Moreira and Rödl proved in Theorem 1 in [2] that if ℓ is even then $Q_\ell(E_N) \geq C_\ell(E_N) \gg \sqrt{N}$, and from this

Proposition 1 *For every binary lattice η and even ℓ we have*

$$L_\ell(\eta) \gg \sqrt{N},$$

where the implied constant factor depends only on ℓ.

Next we prove (7). We will adapt the method used in the one dimensional case in [4]. This will be a consequence of an upper bound for

$$S_{N,\ell}(v) = \sum_{\eta:\ I_N^2 \to \{-1,+1\}} \sum_{D=(\mathbf{d_1},\ldots,\mathbf{d}_\ell)} \sum_{\substack{L:\ L+\mathbf{d_i}\subseteq I_N^2 \\ \text{for } 1\le i\le \ell}} \left| \sum_{x\in L} \eta(\mathbf{x}+\mathbf{d_1})\ldots(\mathbf{x}+\mathbf{d}_\ell) \right|^{2v}, \tag{8}$$

where the first sum is taken over all binary lattices $\eta:\ I_N^2 \to \{-1,+1\}$, the second sum is taken over all ℓ-tuples $D=(\mathbf{d_1},\ldots,\mathbf{d}_\ell)$ with different vectors $\mathbf{d_i} \in \{(x,y):\ x,y\in\mathbb{Z},\ -(N-1)<x,y<N-1\}$, and the third sum is taken over all segments L with $L+\mathbf{d_1},\ldots,L+\mathbf{d}_\ell \subseteq I_N^2$. We may rewrite (8) by using the slightly simpler notation:

$$S_{N,\ell}(v) = \sum_{\eta}\sum_{D}\sum_{L} \left| \sum_{x\in L} \eta(\mathbf{x}+\mathbf{d_1})\ldots(\mathbf{x}+\mathbf{d}_\ell) \right|^{2v},$$

The sum above can be rewritten as

$$S_{N,\ell}(v) = \sum_{D}\sum_{L} Z(D,L) \tag{9}$$

where

$$Z(D,L) = \sum_{\eta} \left| \sum_{x\in L} \eta(\mathbf{x}+\mathbf{d_1})\ldots\eta(\mathbf{x}+\mathbf{d}_\ell) \right|^{2v}.$$

If $|L| = |\{x=(x_1,x_2):\ x_1=a_1t+b_1,\ x_2=at_2+b_2,\ t\in\{0,1,\ldots,M-1\}\}| = M \le N^{1/4}$ then clearly

$$Z(D,L) = \sum_{\eta} \left| \sum_{x\in L} \eta(\mathbf{x}+\mathbf{d_1})\ldots\eta(\mathbf{x}+\mathbf{d}_\ell) \right|^{2v} \le \sum_{\eta} M^{2v} \le 2^{N^2} M^{2v}. \tag{10}$$

Assume now that

$$N^{1/4} < M = |L| \le N. \tag{11}$$

Let $\mathbf{d_i} = (d_i^{(1)}, d_i^{(2)})$. For $\mathbf{x}\in L$, $\mathbf{x}=(a_1t+b_1, a_2t+b_2)$ write $\eta(\mathbf{x}+\mathbf{d_1})\ldots\eta(\mathbf{x}+\mathbf{d}_\ell) = \eta(a_1t+b_1+d_1^{(1)}, a_2t+b_2+d_1^{(2)})\ldots\eta(a_1t+b_1+d_\ell^{(1)}, a_2t+b_2+d_\ell^{(2)}) = A_t$.

Then by the multinomial theorem

$$Z(D,L)=\sum_{\eta}\sum_{s=1}^{2v}\sum_{0\le i_1<\cdots<i_s\le M-1}\sum_{\substack{j_1+\cdots+j_s=2v\\ 1\le j_1,\ldots,j_s}}\frac{(2v)!}{j_1!\ldots j_s!}A_{i_1}^{j_1}\ldots A_{i_s}^{j_s}.$$

Observe that each $A_i\in\{-1,+1\}$, and thus the value A_i^j depends only on the parity of j: $A_i^j=1$ if j is even and $A_i^j=A_i$ if j is odd. Let Z_1 denote the contribution of those terms for which at least one of $j_1,\ldots,j_s$ is odd and let Z_2 denote the contribution of the terms such that each of $j_1,\ldots,j_s$ is even, so that

$$Z(D,L)=Z_1+Z_2. \tag{12}$$

All the terms in Z_1 can be replaced by a term of the form constant times $A_{r_1}\ldots A_{r_u}$ where $u\le 2v$, $0\le r_1<\cdots<r_u\le M$. Thus Z_1 can be rewritten in the form

$$Z_1=\sum_{u\le 2v}\sum_{0\le r_1<\cdots<r_u\le M}a(r_1,\ldots,r_u)\sum_{\eta}A_{r_1}\ldots A_{r_u} \tag{13}$$

(where the coefficients $a(r_1,\ldots,r_u)$ are non-negative integers independent of η). Replace A_{r_i} again by $\eta(\mathbf{x_i}+\mathbf{d_1})\eta(\mathbf{x_i}+\mathbf{d_2})\ldots\eta(\mathbf{x_i}+\mathbf{d_k})$ for each of $i=1,2,\ldots,u$ where $\mathbf{x_i}=(a_1r_i+b_1,a_2r_i+b_2)$. Without loss of generality we may assume that $\mathbf{x_1}$ is minimal in lexicographical order among $\mathbf{x_1},\ldots,\mathbf{x_u}$. We may also suppose that $\mathbf{d_1}$ is minimal in lexicographical order among $\mathbf{d_1},\ldots,\mathbf{d}_\ell$. Then each term is of the form

$$A_{r_1}\ldots A_{r_u}=\eta(\mathbf{x_1}+\mathbf{d_1})\eta(\mathbf{v_2})^{q_2}\ldots\eta(\mathbf{v_z})^{q_z}$$

where $\mathbf{x_1}+\mathbf{d_1}<\mathbf{v_2}<\cdots<\mathbf{v_z}$ follow in lexicographical order and $q_i\in\mathbb{N}$ for $i=2,3,\ldots,z$. Then the innermost sum in (13) is

$$2^{N^2-z}\sum_{\eta(\mathbf{v_2}),\ldots,\eta(\mathbf{v_z})\in\{-1,+1\}^z}\eta(\mathbf{v_2})^{q_2}\ldots\eta(\mathbf{v_z})^{q_z}\sum_{\eta(\mathbf{x_1}+\mathbf{d_1})\in\{-1,+1\}}\eta(\mathbf{x_1}+\mathbf{d_1}). \tag{14}$$

Here the inner sum is 0 so that the innermost sum in (14) is always 0 and thus

$$Z_1 = 0. \tag{15}$$

In Z_2 we may replace each j_i by $2g_i$ and then we may use the fact that the inner sums are independent of η:

$$\begin{aligned} Z_2 &= \sum_{\eta} \sum_{s=1}^{2v} \sum_{0 \le i_1 < \cdots < i_s \le M-1} \sum_{\substack{g_1 + \cdots + g_s = v \\ 1 \le g_1, \ldots, g_s}} \frac{(2v)!}{(2g_1)! \ldots (2g_s)!} \\ &= 2^{N^2} \sum_{s=1}^{2v} \sum_{0 \le i_1 < \cdots < i_s \le M-1} \sum_{\substack{g_1 + \cdots + g_s = v \\ 1 \le g_1, \ldots, g_s}} \frac{(2v)!}{(2g_1)! \ldots (2g_s)!}. \end{aligned}$$

To compute this sum observe that, by a similar argument,

$$\begin{aligned} F(y_1, \ldots, y_M) &\stackrel{\text{def}}{=} \sum_{f_0, \ldots, f_{M-1} \in \{-1, +1\}} (f_0 y_0 + \cdots + f_{M-1} y_{M-1})^{2v} \\ &= 2^M \sum_{s=1}^{2v} \sum_{0 \le i_1 < \cdots < i_s \le M-1} \sum_{\substack{g_1 + \cdots + g_s = v \\ 1 \le g_1, \ldots, g_s}} \frac{(2v)!}{(2g_1)! \ldots (2g_s)!} y_{i_1}^{2g_1} \ldots y_{i_s}^{2g_s}. \end{aligned}$$

Substituting $y_0 = \cdots = y_{M-1} = 1$, we obtain $F(1, 1, \ldots, 1) = 2^{M-N^2} Z_2$. On the other hand, $F(1, 1, \ldots, 1)$ is easy to compute: if

$$|\{f_i : \ 0 \le i \le M-1, \ f_i = -1\}| = h \tag{16}$$

then

$$f_0 + \cdots + f_{M-1} = M - 2h$$

and there are $\binom{M}{h}$ M-tuples satisfying (16). Thus

$$2^{M-N^2} Z_2 = F(1, 1, \ldots, 1) = \sum_{h=0}^{M} \binom{M}{h} (M-2h)^{2v} \le 2 \sum_{h=0}^{[M/2]} \binom{M}{h} (M-2h)^{2v}.$$

Now we fix the value of v: let

$$v = [8\ell \log N]. \tag{17}$$

Write $B_h = \binom{M}{h}(M-2h)^{2v}$ so that $2^{M-N^2}Z_2 \le 2\sum_{h=0}^{[M/2]} B_h$.

A little computation shows that for $h < M/2$ we have

$$\frac{B_{h+1}}{B_h} = \frac{M-h}{h+1}\left(1 - \frac{2}{M-2h}\right)^{2v}$$

and clearly this is decreasing on the interval $0 \le h \le M/2 - 1$. Thus writing $H = M/2 - \sqrt{vM}$, by (11) and (17) for $h \le H$

$$\begin{aligned}\frac{B_{h+1}}{B_h} &\ge \frac{M-H}{H+1}\left(1 - \frac{2}{M-2H}\right)^{2v} = \frac{M/2+\sqrt{vM}}{M/2-\sqrt{vM}+1}\left(1 - \frac{1}{\sqrt{vM}}\right)^{2v} \\ &= \left(1 + (1+o(1))4\sqrt{v/M}\right)\left(1 - (1+o(1))2\sqrt{v/M}\right) > 1.\end{aligned}$$

It follows that writing $H_0 = [M/2 - \sqrt{vM} + 1]$ we have $B_0 < B_1 < \cdots < B_{H_0}$, whence

$$\begin{aligned}2^{M+1-N^2}Z_2 &\le 2\sum_{h=0}^{[M/2]} B_h = 2\sum_{h=0}^{H_0} B_h + 2\sum_{h=H_0+1}^{[M/2]} B_h \\ &< 2\left(\sum_{h=0}^{H_0} B_{H_0} + \sum_{h=H_0+1}^{[M/2]} \binom{M}{h}(M-2h)^{2v}\right) \\ &< 2\left(2H_0 B_{H_0} + (M-2H_0)^{2v}\sum_{h=0}^{M}\binom{M}{h}\right) \\ &< 2\left(M\binom{M}{H_0}(M-2H_0)^{2v} + (M-2H_0)^{2v}2^M\right) \\ &< 2^{M+1}(M+1)\left(M - 2\left(\frac{M}{2} - \sqrt{vM}\right)\right)^{2v} \\ &< 2^{M+2}M(4vM)^v \quad \text{for } (N^2)^{1/4} < M \le N. \end{aligned} \tag{18}$$

It follows from (9), (10), (12), (15) and (18) that

$$\begin{aligned}
S_{n,\ell}(v) &= \sum_D \left(\sum_{\substack{L:\ L+\mathbf{d_i}\subseteq I_N^2 \\ \text{for } 1\le i\le \ell \\ |L|=M\le N^{1/4}}} Z(M,D) + \sum_{\substack{L:\ L+\mathbf{d_i}\subseteq I_N^2 \\ \text{for } 1\le i\le \ell \\ N^{1/4}<|L|=M\le N}} Z(M,D) \right) \\
&< \sum_D \left(N^4 \sum_{M\le N^{1/4}} 2^{N^2} M^{2v} + N^4 \sum_{N^{1/4}<v\le N} 2^{N^2+2}(4v)^v N^{v+1} \right) \\
&< N^4 \sum_D \left(\sum_{M\le N^{1/4}} 2^{N^2} N^{v/2} + N^{v+2} 2^{N^2+2}(4v)^v \right) \\
&< 2^{N^2} N^4 \sum_D \left(N^{v/2+1/4} + 4N^{v+2}(4v)^v \right) \\
&< 5\cdot 2^{N^2} N^{v+6}(4v)^v \sum_D 1. \qquad (19)
\end{aligned}$$

Each $\mathbf{d_i}$ in $D = (\mathbf{d_1}, \dots, \mathbf{d}_\ell)$ satisfies $\mathbf{d_i} \in \{(x,y) :\ x,y \in \mathbb{Z},\ -(N-1) < x,y < N-1\}$, thus it can be chosen in at most $4N^2$ ways so that

$$\sum_D 1 \le (2N)^{2\ell}. \qquad (20)$$

It follows from (19) and (20)

$$S_{N,\ell}(v) < 5\cdot 2^{N^2} N^v (2N)^{2\ell+6}(4v)^v. \qquad (21)$$

On the other hand, writing $X = 10(\ell N \log N)^{1/2}$

$$\begin{aligned}
S_{N,\ell}(v) &= \sum_\eta \sum_D \sum_L (V(E_N,L,D))^{2v} \ge \sum_\eta \left(\max_{M,D} |V(E_N,L,D)| \right)^{2v} \\
&= \sum_\eta Q_\ell(\eta)^{2v} \ge X^{2v} \left| \{\eta :\ I_N^2 \to \{-1,+1\} :\ Q_\ell(\eta) > X\} \right|. \qquad (22)
\end{aligned}$$

It follows from (17), (21) and (22) for $N > N_0(\varepsilon)$

$$P(Q_\ell > X) = \frac{1}{2^{N^2}} \left|\{\eta : I_N^2 \to \{-1,+1\} : Q_\ell(\eta) > X\}\right| \le 5N^v (2N)^{2\ell+6} (4v)^v X^{-2v}$$
$$\le 5N^v (2N)^{2\ell+6} (4v)^v (100\ell N \log N)^{-v} < 5(2N)^{2\ell+6} 3^{-v} = 15(2N)^{2\ell+6} 3^{-v-1}$$
$$< 15(2N)^{8\ell} 3^{-9\ell \log N} < 15(2N)^{8\ell(1-\log 3)} < 15(2N)^{1-\log 3}$$

and this is $< \varepsilon$ if N is large enough in terms of ε (since $1 - \log 3 < 0$), which completes the proof of (7).

5 A construction with strong pseudorandom properties

Next we will present a construction for which the line measure of order ℓ is small.

Theorem 4 *Let p be a prime. Define*

$$f(x_1, x_2) = \prod_{i=1}^{r} f_i(x_1 + A_i x_2)$$

where $f_i(x) \in \mathbb{F}_p[x]$ is a one-variable irreducible polynomial for $i = 1, 2, \ldots, r$ and $A_1, A_2, \ldots, A_r \in \mathbb{F}_p$ are different. We also suppose that the degrees of the polynomials f_i are different and $p - 1 \ge \deg f_i \ge 2$. Define the binary p-lattice η by

$$\eta(x_1, x_2) = \left(\frac{f(x_1, x_2)}{p}\right). \tag{23}$$

Let $k = \deg f(x_1, x_2)$. Then for $\ell \le (2r-3)^{1/2}$ we have

$$L_\ell(\eta) \ll k\ell p^{1/2} \log p.$$

(Note that by Theorems 1 and 2 this upper bound for $L_\ell(\eta)$ implies that $X_\ell(\eta)$ and $Q_\ell(\eta)$ are also $o(p^2)$.)

(We note that the smallest possible value of k is $2+3+\cdots+(r+1) = \frac{r^2+3r}{2}$.)

Proof of Theorem 3 First we note that $f_i(x) \in \mathbb{F}_p[x]$ is irreducible, thus $f_i(x_1 + A_i x_2)$ is never zero, so that $\eta(x_1, x_2)$ in (23) is well defined. Let L be a segment of I_p^2, thus

$$L = \{\mathbf{x} = (x_1, x_2) : \ x_1 = a_1 t + b_1, \ x_2 = a_2 t + b_2, \ t \in \{0, 1, \ldots, M-1\}\}$$

(with $M \le p$) where $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ and $(a_1, a_2) \neq (0, 0)$. Let $D = (\mathbf{d_1}, \ldots, \mathbf{d}_\ell)$ be an ℓ-tuple such that the $\mathbf{d_i}$'s are different and $L + \mathbf{d_i} \subseteq {I_p}^2$. We will prove that

$$S_{L,D} \stackrel{\text{def}}{=} \left| \sum_{\mathbf{x} \in L} \eta(\mathbf{x} + \mathbf{d_1}) \ldots \eta(\mathbf{x} + \mathbf{d}_\ell) \right| \ll k\ell p^{1/2} \log p.$$

Since $L + \mathbf{d_1} \subseteq I_p^2$ we may assume that $0 \le a_1 < p$, $0 \le a_2 < p$. Let $\mathbf{d_i} = (d_i^{(1)}, d_i^{(2)})$. Then

$$\begin{aligned} S_{L,D} &= \left| \sum_{\mathbf{x} \in L} \left(\frac{f(\mathbf{x} + \mathbf{d_1}) \ldots f(\mathbf{x} + \mathbf{d}_\ell)}{p} \right) \right| \\ &= \left| \sum_{t=0}^{M-1} \left(\frac{f(a_1 t + b_1 + d_1^{(1)}, a_2 t + b_2 + d_1^{(2)}) \cdots f(a_1 t + b_1 + d_\ell^{(1)}, a_2 t + b_2 + d_\ell^{(2)})}{p} \right) \right|. \end{aligned}$$

In the factorization of $f(a_1 t + b_1 + d_1^{(1)}, a_2 t + b_2 + d_1^2) \cdots f(a_1 t + b_1 + d_\ell^{(1)}, a_2 t + b_2 + d_\ell^2)$ the following irreducible factors appear:

$$f_j((a_1 t + b_1 + d_i^{(1)}) - A_j(a_2 t + b_2 + d_i^2)) \quad \text{for } j = 1, \ldots, r, \ i = 1, \ldots, \ell. \ (24)$$

The degree of one of these polynomials in t is 0 if $a_1 - A_j a_2 \equiv 0 \pmod p$ and $\deg f_j$ otherwise. By $\binom{\ell}{2} + 2 \le \frac{\ell^2+3}{2} \le r$ there is an A_j for which

$$a_1 - A_j a_2 \not\equiv 0 \pmod p, \tag{25}$$

$$d_v^{(1)} - d_u^{(1)} - A_j(d_v^{(2)} - d_u^{(2)}) \not\equiv 0 \pmod p \text{ for } 1 \le u, v \le \ell,\ u \ne v. \tag{26}$$

(We used here that $(a_1, a_2) \ne (0, 0)$ and $\mathbf{d_u} \ne \mathbf{d}_v$.) Fix a j for which (25) and (26) holds.

Consider the irreducible factors

$$f_j((a_1 t + b_1 + d_i^{(1)}) - A_j(a_2 t + b_2 + d_i^2)) \quad \text{for } i = 1, 2, \dots, \ell. \tag{27}$$

The main coefficients of these factors are the same. Their degree is $\deg f_j$, which is different from the degree of other irreducible factors in (24). We will also prove that the irreducible factors in (27) are different. It follows from this that the product $f(a_1 t + b_1 + d_1^{(1)}, a_2 t + b_2 + d_1^{(2)}) \cdots f(a_1 t + b_1 + d_\ell^{(1)}, a_2 t + b_2 + d_\ell^{(2)})$ is not of the form $cg(t)^2$ since the multiplicity of the irreducible factor $f_j((a_1 t + b_1 + d_1^{(1)}) - A_j(a_2 t + b_2 + d_1^{(2)})) \in \mathbb{F}_p[t]$ is 1 in the factorization of $f(a_1 t + b_1 + d_1^{(1)}, a_2 t + b_2 + d_1^{(2)}) \cdots f(a_1 t + b_1 + d_\ell^{(1)}, a_2 t + b_2 + d_\ell^{(2)}) \in \mathbb{F}_p[t]$ into irreducible polynomials.

Suppose that two irreducible factors in (27) are the same:

$$f_j((a_1 t + b_1 + d_u^{(1)}) - A_j(a_2 t + b_2 + d_u^{(2)})) = f_j((a_1 t + b_1 + d_v^{(1)}) - A_j(a_2 t + b_2 + d_v^{(2)}))$$

Let $A = a_1 - A_j a_2$, $B = b_1 + d_u^{(1)} - A_j(b_2 + d_u^{(2)})$, $C = d_v^{(1)} - d_u^{(1)} - A_j(d_v^{(2)} - d_u^{(2)})$. Here $A \not\equiv 0,\ C \not\equiv 0 \pmod p$ by the definition of A_j. Then

$$f_j(At + B) = f_j(At + B + C).$$

Substituting $t = A^{-1}(Z - B)$ we get

$$f_j(Z) = f_j(Z + C),$$

whence

$$f_j(Z) = f_j(Z + C) = f_j(Z + 2C) = \cdots = f_j(Z + (p-1)C).$$

Since $\{aC : \ a \in \mathbb{F}_p\} = \mathbb{F}_p$ we get

$$f_j(Z) = f_j(Z + 1) = f_j(Z + 2) = \cdots = f_j(Z + p - 1).$$

Thus $Z^p - Z \mid f_j(Z) - f_j(1)$ which contradicts $\deg f_j < p$.

Thus we proved that $f(a_1t+b_1+d_1^{(1)}, a_2t+b_2+d_1^{(2)}) \cdots f(a_1t+b_1+d_\ell^{(1)}, a_2t+b_2+d_\ell^{(2)})$ is not of the form $cg(t)^2$. We will use the following lemma.

Lemma 1 *Suppose that p is a prime, χ is a non-principal character modulo p of order d, $f(t) \in \mathbb{F}_p[t]$ has s distinct roots in $\overline{\mathbb{F}}_p$, and it is not a constant multiple of the d-th power of a polynomial in $\mathbb{F}_p[t]$. Let v be a real number with $0 \le v \le p$. Then for any $u \in \mathbb{F}_p$:*

$$\left| \sum_{u \le t \le u+v} \chi(f(t)) \right| \le 9sp^{1/2} \log p.$$

Proof of Lemma 1. This is a consequence of Lemma 1 in [1] which was derived from Weil's theorem [11].

By using Lemma 1 we get

$$|S_{L,D}| \ll k\ell p^{1/2} \log p,$$

which was to be proved.

References

[1] R. Ahlswede, C. Mauduit and A. Sárközy, *Large families of pseudorandom sequences of k symbols and their complexity, Part I*, Lecture Notes in Computer Science 4123, General Theory of Information Transfer and Combinatorics, 2006, 293-307.

[2] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira, V. Rödl, *Measures of pseudorandomness for finite sequences: minimal values*, Combin. Probab. Comput. 15 (2006), no. 1-2, 1-29.

[3] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira, V. Rödl, *Measures of pseudorandomness for finite sequences: typical values*, Proc. Lond. Math. Soc. (3) 95 (2007), no. 3, 778-812.

[4] J. Cassaigne, C. Mauduit, A. Sárközy, *On finite pseudorandom binary sequences. VII. The measures of pseudorandomness*, Acta Arith. 103 (2002), no. 2, 97-118.

[5] K. Gyarmati, *On a pseudorandom property of binary sequences*, Ramanujan J. 8 (2004), 289-302.

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

[7] K. Gyarmati, C. Mauduit, A. Sárközy, *Measures of pseudorandomness of finite binary lattices, II (The symmetry measures.)*, Ramanujan J., to appear.

[8] K. Gyarmati, A. Sárközy and C. L. Stewart, *On Legendre symbol lattices*, Unif. Distrib. Theory, 4 (2009), no. 1, 81-95.

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

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

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

Katalin Gyarmati

Department of Algebra and Number Theory

Eötvös Loránd University

H-1117 Budapest, Pázmány Péter sétány 1/c

Hungary

email: gykati@cs.elte.hu