Measures of pseudorandomness of finite binary lattices, II.

(The symmetry measures.)

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

Research partially supported by Hungarian National Foundation for Scientific Research, Grants No. K67676, K72731 and PD72264, French-Hungarian exchange program F-48/06, and the János Bolyai Research Fellowship.

Abstract

In an earlier paper Gyarmati introduced and studied the *symmetry measure* of pseudorandomness of binary *sequences*. The goal of this paper is to extend this definition to two dimensions, i.e., to binary lattices. Three different definitions are proposed to do this extension. The connection between these definitions is analyzed. It is shown that these new symmetry measures are independent of the other measures of pseudorandomness of binary lattices. A binary lattice is constructed for which both the pseudorandom measures of order ℓ (for every fixed ℓ) and the symmetry measures are small. Finally, the symmetry measures are estimated for truly random binary lattices.
2000 Mathematics Subject Classification: Primary 11K45.
Key words and phrases: binary lattice, pseudorandom, symmetry.

1 Introduction

In [15] Mauduit and Sárközy initiated a new constructive approach to study pseudorandomness of binary sequences

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

First they introduced the following 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. Then they 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 Part I [9] we surveyed some further details of the related work, and we also presented a list of references. Here we recall only the definition of the correlation measure which we will need later:

Definition 1 *The* correlation measure of order ℓ *of the sequence* E_N *in* (1) *is defined as*

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

where the maximum is taken over all $\mathbf{D} = (d_1, \dots, d_\ell)$ *and* M *such that* $0 \le d_1 < \dots < d_\ell \le N - M$.

In [11] 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

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

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 [10] the definition of I_N^n 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 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 $z_i \in \mathbb{Z}^+$). 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

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

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

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]):

Definition 2 *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 [11], 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 [7] 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 [11]. Later further binary lattices with strong pseudorandom properties have been constructed, a list of related references is given in [9].

As we mentioned earlier, in the one dimensional case there are several papers written on the measures of pseudorandomness (see [9]). This series of papers is devoted to the study of questions of this type in the n-dimensional case (focusing on the case $n = 2$). In particular, in this paper our goal is to introduce and study the *symmetry measures* in n dimensions.

Starting out from a remark in [15] (Example 2 on p. 372), Gyarmati [8] introduced the symmetry measure of binary sequences:

Definition 3 *The symmetry measure of the sequence E_N in* (1) *is defined as*

$$S(E_N) = \max_{1 \le a < b \le N} \left| \sum_{j=0}^{[(b-a)/2]-1} e_{a+j} e_{b-j} \right|.$$

Clearly, $S(E_N)$ is "large" if and only if E_N has a large part which is "nearly" symmetric or antisymmetric, more precisely, if there are integers a, b such that $1 \le a < b \le N$, b is "much greater", then a (we have $b - a \gg N$), and either

$$e_{a+j} = e_{b-j}$$

or

$$e_{a+j} = -e_{b-j}$$

holds for "much more", than half of the j's with $0 \le j \le \frac{b-a}{2} - 1$. If this is the case, then, as Gyarmati writes, "this sequence certainly cannot be "typical" random sequence, and this symmetric structure may lead difficulties in certain applications. This observation inspired us to propose a new measure of pseudorandomness". Besides, the symmetry measure may help to study symmetry properties of sets which is a subject of independent interest (see e.g., [5], [6], [13], [14], [18], [19], [20], [22]).

In [8] Gyarmati showed that $S(E_N)$ is around $\sqrt{N}$ for almost all $E_N \in \{-1, +1\}^N$. Thus for a "good" pseudorandom sequence E_N the symmetry measure must be "small" (certainly $o(N)$, ideally $O(N^{1/2+\varepsilon})$). She also proved that the symmetry measure of the half of the Legendre symbol sequence (i.e., of the sequence $\left\{\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \dots, \left(\frac{(p-1)/2}{p}\right)\right\}$) is small (it follows from the results in [15]) that the other pseudorandom measures of this sequence are also small), and that the symmetry measure and the other measures of pseudorandomness are independent.

It is not at all clear how to extend Definition 3 to two dimensions and, indeed, here we will present three different definitions (and the case of more than two dimensions would be even more complicated).

2 The rectangle-symmetry measure

It is a natural idea to study the symmetry only on rectangles whose sides are vertical or horizontal. We will call these rectangles parallel rectangles.

Definition 4 *$R \subseteq I_N^2$ is a* parallel rectangle *if R is of the form*

$$R = \{\mathbf{x} = (x_1, x_2) : \ x_1, x_2 \in \mathbb{N}_0, \ a_1 \le x_1 \le b_1, \ a_2 \le x_2 \le b_2\}. \tag{4}$$

Clearly a parallel rectangle R of the form (4) which is not a square has two symmetry axis: the lines $x_1 = \frac{a_1+b_1}{2}$ and $x_2 = \frac{a_2+b_2}{2}$. The rectangle R also has a symmetry center $\left(\frac{a_1+b_1}{2}, \frac{a_2+b_2}{2}\right)$. Let $H(R)$ denote the set of symmetry transformations which leave R in its original position, so that if R is not a a square then for $\tau \in H(R)$ we have either

$$\tau((x_1, x_2)) = (a_1 + b_1 - x_1, x_2) \text{ for all } (x_1, x_2) \in I_N^2,$$
$$\tau((x_1, x_2)) = (x_1, a_2 + b_2 - x_2) \text{ for all } (x_1, x_2) \in I_N^2$$

or

$$\tau((x_1, x_2)) = (a_1 + b_1 - x_1, a_2 + b_2 - x_2) \text{ for all } (x_1, x_2) \in I_N^2.$$

If R is a square then there are two further symmetry transformations: reflections with respect to the diagonals; these rather special transformations are of slightly different nature, than the others, and it would make the discussions much lengthier to cover them as well. Thus we exclude these special transformations, and in $H(R)$ we include only the three transformations τ presented above.

We define the rectangle-symmetry measure by the following:

Definition 5 *Let $\eta : \ I_N^2 \to \{-1, +1\}$ be a binary lattice. The* rectangle-symmetry measure of η *is defined by*

$$S_r(\eta) = \max_{R, \tau \in H(R)} \left| \sum_{\mathbf{x} \in R} \eta(\mathbf{x}) \eta(\tau(\mathbf{x})) \right|$$

where the maximum is taken over all parallel rectangles R of I_N^2 and all symmetry transformations $\tau \in H(R)$.

Then η is considered to have good rectangle-symmetry property if $S_r(\eta)$ is "small". (In a sequel to this paper we will show that for a truly random η $S_r(\eta)$ is "small".)

The first important question is whether this new symmetry measure is independent of the pseudorandom measures $Q_k(\eta)$.

Gyarmati, Sárközy and Stewart [10] gave the following construction:

Construction 1 *Let p be an odd prime, $f(x_1,x_2) \in \mathbb{F}_p[x_1,x_2]$ be a polynomial in two variables. Define the two dimensional binary lattice $\eta : I_p^2 \to \{-1,+1\}$ by*

$$\eta(x_1,x_2) = \begin{cases} \left(\frac{f(x_1,x_2)}{p}\right) & \text{if } (f(x_1,x_2),p) = 1, \\ +1 & \text{if } p \mid f(x_1,x_2) \end{cases} \tag{5}$$

(where $\left(\frac{n}{p}\right)$ denotes the Legendre symbol). They proved that under certain conditions on the polynomial $f(x)$, the binary lattice η has small Q_ℓ pseudorandom measures. Now we will present a construction of this type where the binary lattice η has small Q_ℓ pseudorandom measures but the rectangle-symmetry measure is large.

Proposition 1 *Let p be an odd prime, $f(x_1,x_2) = x_1x_2 + 1$ and define the binary p-lattice η by (5). Then for $\ell < p$ we have*

$$Q_\ell(\eta) \le 10k\ell p^{3/2} \log p, \tag{6}$$

$$S_r(\eta) \ge (p-1)^2. \tag{7}$$

Proof of Proposition 1. (6) follows immediately from Theorem 1 in [10] since x_1x_2+1 is an irreducible polynomials in $\mathbb{F}_p[x_1,x_2]$. Let R be the parallel rectangle

$$R = \{\mathbf{x} = (x_1,x_2) : \ 1 \le x_1 \le p-1, 1 \le x_2 \le p-1\},$$

and let $\tau \in H(R)$ be the symmetry transformation (reflection) with respect to the center $\left(\frac{p}{2}, \frac{p}{2}\right)$. Then by the definition of the rectangle-symmetry measure we have

$$S_r(\eta) \geq \left|\sum_{\mathbf{x}\in R} \eta(x)\eta(\tau(x))\right| = (p-1)^2.$$

We remark that the statement of Proposition 1 can be reversed, i.e., there is a lattice η such that $Q_2(\eta)$ is large but $S_r(\eta)$ is small:

Example 1 *Let $M \in \mathbb{N}$, $N = 2M$. Then define the binary N-lattice $\eta : I_N^2 \to \{-1,+1\}$ so that the values $\eta(x_1,x_2)(\in \{-1,+1\})$ are chosen independently and in random way for $x_1 \in \{0,1,\dots,M-1\}$ and all x_2, and we have*

$$\eta(x_1,x_2) = \eta(x_1 - M, x_2) \qquad \textit{for } x \in \{M, M+1, \dots, N-1\}.$$

Then trivially we have

$$Q_2(\eta) \gg N^2,$$

and we will sketch the proof of the fact that with probability approaching 1 (as $M \to \infty$) we have

$$S_r(\eta) < N(\log N)^c.$$

We will show that if c is large enough, then for any fixed R and $\tau \in H(R)$ we have

$$P\left(\left|\sum_{\mathbf{x}\in R} \eta(\mathbf{x})\eta(\tau(\mathbf{x}))\right| \geq N(\log N)^c\right) < \frac{4}{N^8}. \tag{8}$$

Assume that τ belongs to the first group of symmetry transformations presented after Definition 4:

$$\tau((x_1,x_2)) = (a_1 + b_1 - x_1, x_2) \text{ for all } (x_1,x_2) \in I_N^2.$$

We may assume that

$$\frac{a_1+b_1}{2} \leq M - 1$$

(since the case $\frac{a_1+b_1}{2} \geq M$ is similar). Define r_i by $\{(i, x_2) : \; a_2 \leq x_2 \leq b_2\}$. Then the sum on the left hand side of (8) can be rewritten as

$$\begin{aligned}
\left| \sum_{\mathbf{x} \in R} \eta(\mathbf{x}) \eta(\tau(\mathbf{x})) \right| &= \left| \sum_{i=a_1}^{b_1} \sum_{\mathbf{x} \in r_i} \eta(\mathbf{x}) \eta(\tau(\mathbf{x})) \right| \\
&= 2 \left| \sum_{a_1 \leq i < \frac{a_1+b_1}{2}} \sum_{\mathbf{x} \in r_i} \eta(\mathbf{x}) \eta(\tau(\mathbf{x})) \right| + O(N) \qquad (9)
\end{aligned}$$

where the $O(N)$ term is added to cover the case when $a_1 + b_1$ is even and $i = \frac{a_1+b_1}{2}$ so that for this i we have

$$\left| \sum_{\mathbf{x} \in r_{(a_1+b_1)/2}} \eta(\mathbf{x}) \eta(\tau(\mathbf{x})) \right| = \sum_{\mathbf{x} \in r_{(a_1+b_1)/2}} (\eta(\mathbf{x}))^2 = \sum_{\mathbf{x} \in r_{(a_1+b_1)/2}} 1 \leq N.$$

Now we split the double sum in (9) in two parts:

$$\begin{aligned}
\sum_{a_1 \leq i < \frac{a_1+b_1}{2}} \sum_{\mathbf{x} \in r_i} \eta(\mathbf{x}) \eta(\tau(\mathbf{x})) = &\sum_{a_1 \leq i \leq -M+a_1+b_1} \sum_{\mathbf{x} \in r_i} \eta(\mathbf{x}) \eta(\tau(\mathbf{x})) \\
&+ \sum_{-M+a_1+b_1 < i < \frac{a_1+b_1}{2}} \sum_{\mathbf{x} \in r_i} \eta(\mathbf{x}) \eta(\tau(\mathbf{x})) = \sum\nolimits_1 + \sum\nolimits_2,
\end{aligned} \qquad (10)$$

say. Assume first that $b_1 \geq M$. By the construction of the lattice η we may rewrite $\sum_1$ as

$$\begin{aligned}
\sum\nolimits_1 &= \sum_{a_1 \leq i \leq -M+a_1+b_1} \sum_{\mathbf{x} \in r_i} \eta(\mathbf{x}) \eta(\tau(\mathbf{x}) - (M, 0)) \\
&= \sum_{a_1 \leq i \leq -M+a_1+b_1} \sum_{\mathbf{x} \in r_i} \eta(\mathbf{x}) \eta(\tau'(\mathbf{x}))
\end{aligned}$$

where

$$\tau'((x_1, x_2)) = (-M + a_1 + b_1 - x_1, x_2).$$

Then writing $\tau'(\mathbf{x}) = \mathbf{y}$, we have $\mathbf{x} = \tau'(\mathbf{y})$, the condition $\mathbf{x} \in r_i$ is equivalent with $\mathbf{y} \in r_j$ where $j = -M + a_1 + b_1 - i$, and the condition $a_1 \leq i \leq$

$-M + a_1 + b_1$ can be replaced by $0 \le j \le -M + b_1$. Thus the last double sum can be replaced by

$$\sum\nolimits_1 = \sum_{0 \le j \le -M+b_1} \sum_{\mathbf{y} \in r_j} \eta(\mathbf{y})\eta(\tau'(\mathbf{y})) = \sum_{0 \le j < a_1} \sum_{\mathbf{y} \in r_j} \eta(\mathbf{y})\eta(\tau'(\mathbf{y}))$$
$$+ 2 \sum_{a_1 \le j < \frac{-M+a_1+b_1}{2}} \sum_{\mathbf{y} \in r_j} \eta(\mathbf{y})\eta(\tau'(\mathbf{y})) + O(N) \tag{11}$$

where (as in (9)) the $O(N)$ term covers the contribution of the terms with $j = \frac{-M+a_1+b_1}{2}$ when $-M + a_1 + b_1$ is even.

Combining (9), (10) and (11) we get

$$\left| \sum_{\mathbf{x} \in R} \eta(\mathbf{x})\eta(\tau(\mathbf{x})) \right| \le 2 \left| \sum_{0 \le j < a_1} \sum_{\mathbf{y} \in r_j} \eta(\mathbf{y})\eta(\tau'(\mathbf{y})) \right|$$
$$+ 4 \left| \sum_{a_1 \le j < \frac{-M+a_1+b_1}{2}} \sum_{\mathbf{y} \in r_j} \eta(\mathbf{y})\eta(\tau'(\mathbf{y})) \right|$$
$$+ 2 \left| \sum_{-M+a_1+b_1 < i < \frac{a_1+b_1}{2}} \sum_{\mathbf{x} \in r_i} \eta(\mathbf{x})\eta(\tau(\mathbf{x})) \right| + O(N).$$

By this grouping of the terms we have achieved that here all the occurring vectors $\mathbf{y}$, $\tau'(\mathbf{y})$, $\mathbf{x}$, $\tau(\mathbf{x})$ are distinct, and thus all the random variables $\eta(\mathbf{y})$, $\eta(\tau'(\mathbf{y}))$, $\eta(\mathbf{x})$, $\eta(\tau(\mathbf{x}))$ are pairwise independent. Now we select the η-values occurring in these sums so that first we select the values of the first factors $\eta(\mathbf{y})$, $\eta(\mathbf{x})$ occurring in these sums (independently); then we fix the values of these η's, and then we let all the second factors $\eta(\tau'(\mathbf{y}))$, $\eta(\tau(\mathbf{x}))$ assume the values +1, -1 with probability 1/2 independently. Then all the terms $\eta(\mathbf{y})\eta(\tau'(\mathbf{y}))$, $\eta(\mathbf{x})\eta(\tau(\mathbf{x}))$ are independent random variables assuming the values $+1$ and -1 with equal probability $\frac{1}{2}$. Using Bernstein's inequality (Lemma 1 later), it is easy to see that if c is large enough, then uniformly for any choice of the first factors $\eta(\mathbf{y})$, $\eta(\mathbf{x})$, it holds with probability less than, say, $\frac{1}{N^8}$ that any one of the last double sums is $\ge \frac{1}{100} N(\log N)^c$. If $b_1 < M$

we have $\sum_1 = 0$ which simplifies the discussion and we obtain similarly that the same conclusion holds. It follows that for fixed R and τ of the first type we have

$$P\left(\left|\sum_{\mathbf{x}\in R}\eta(\mathbf{x})\eta(\tau(\mathbf{x}))\right| \geq N(\log N)^c\right) < \frac{4}{N^8};$$

for the other two symmetry transformations the same bound could be proved similarly. The rectangle R is uniquely determined by its 3 vertices, and these vertices can be chosen in at most $(N^2)^3 = N^6$ ways, while for fixed R the symmetry transformation τ can be chosen in 3 ways. Thus we have

$$\begin{aligned} P\left(S_r(\eta) \geq N(\log N)^c\right) &= P\left(\max_{R,\ \tau\in H(R)}\left|\sum_{\mathbf{x}\in R}\eta(\mathbf{x})\eta(\tau(\mathbf{x}))\right| \geq N(\log N)^c\right) \\ &\leq \sum_{R,\ \tau\in H(R)} P\left(\left|\sum_{\mathbf{x}\in R}\eta(\mathbf{x})\eta(\tau(\mathbf{x}))\right| \geq N(\log N)^c\right) \\ &\leq \sum_{R,\ \tau\in H(R)} \frac{4}{N^8} = \frac{4}{N^8}\sum_{R,\ \tau\in H(R)} 1 \leq \frac{4}{N^8}3N^6 = \frac{12}{N^2} \\ &= o(1) \end{aligned}$$

so that, indeed,

$$P\left(S_r(\eta) < N(\log N)^c\right) > 1 - o(1).$$

(This construction can be extended from Q_2 to Q_ℓ easily.)

This remark and Proposition 1 show that, indeed, $Q_\ell(\eta)$ and $S_r(\eta)$ are independent.

3 The convex symmetry measure

In certain applications one may need the definition of a more general symmetry-measure. Let us consider an arbitrary binary N-lattice η:

$$\begin{array}{ccccc}
+ & - & - & - & + \\
- & + & + & - & + \\
- & + & - & + & - \\
+ & + & + & - & - \\
- & - & + & + & -
\end{array}$$

Figure 1.
A binary lattice

We assign to this lattice another binary N-lattice η':

$$\eta'(x_1, x_2) = \begin{cases} +1 & \text{if } \eta(x_1, x_2) = \eta(N-1-x_1, N-1-x_2), \\ -1 & \text{if } \eta(x_1, x_2) = -\eta(N-1-x_1, N-1-x_2). \end{cases}$$

Suppose that the lattice η' contains more $+1$'s then -1's. It is easy to see that there is a symmetric polygon S which contains exactly those $(x_1, x_2) \in I_N^2$ for which $\eta'(x_1, x_2) = +1$ (see Figure 2).

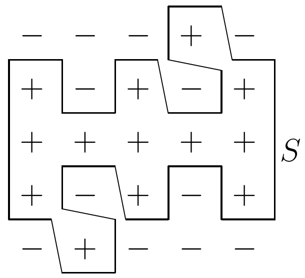

Figure 2.
A symmetric polygon S containing the $+1$'s

Then for $(x_1, x_2) \in I_N^2 \cap S$ we have

$$\eta(x_1, x_2) = \eta(N-1-x_1, N-1-x_2).$$

So S is a large symmetric subset of the binary lattice η. This construction shows that if we want to derive any nontrivial facts related to polygons symmetry we need some additional assumption, for e.g. convexity.

Thus we study the symmetry properties on convex polygons. The idea behind this is that although we showed that usually a binary lattice contains a large symmetric subsets S, the shape of this S can be very "irregular". So we hope that restricting the definition to convex polygons a "typical" random binary lattice has small symmetry measure; we will show later that this is so.

Definition 6 *Let* $K \subseteq \{(x_1, x_2) : \ 0 \leq x_1 \leq N-1, 0 \leq x_2 \leq N-1\}$ *be a convex polygons (the line segments are also included). Let* $H(K)$ *denote the set of symmetry transformations which leave* K *in its original position, so for* $\tau \in H(K)$

$$\tau(K) = K.$$

Now we are ready to introduce a much more general symmetry measure than the rectangle symmetry measure.

Definition 7 *Let* $\eta : \ I_N^2 \to \{-1, +1\}$ *be a binary lattice. The* convex-symmetry measure *of* η *is defined by*

$$S_c(\eta) = \max_{K, \tau \in H(K)} \left| \sum_{\mathbf{x} \in K \cap I_N^2} \eta(\mathbf{x}) \eta(\tau(\mathbf{x})) \right|$$

where the maximum is taken over all convex polygons $K \subseteq \{(x, y) : \ 0 \leq x \leq N-1, 0 \leq y \leq N-1\}$ *and transformations* $\tau \in H(K)$.

It follows trivially from Definition 5 and 7 that

Proposition 2 *For every binary-lattice* η *we have*

$$S_r(\eta) \leq S_c(\eta).$$

Next we would like to give constructions for which the convex-symmetry measure is small. Let $p \geq 5$ be a prime and η be a binary p-lattice defined as in Construction 1. As in [10] there is no hope to prove better bound than

$p^{3/2}\log p$ for $S_c(\eta)$; here the difficulties are the same as it is described in [10, pp. 83-84]. Even the upper bound $p^{3/2}\log p$ is far from trivial.

In order to estimate the convex-symmetry measure, we usually apply the one-dimensional theory of pseudorandomness and we estimate the symmetry measure of lines of η. Since the study of pseudorandom properties with respect to lines is of independent interest, we will introduce a third type symmetry measure in the next paragraph.

4 The line-symmetry measure

Definition 8 *$L \subseteq I_N^2$ is a* segment *if L is of the form*

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

(with $M < N$) where $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ and $(a_1, a_2) \neq (0, 0)$.

Let now $\mathbf{c} = \left(\frac{c_1}{2}, \frac{c_2}{2}\right)$ be a point with $c_1, c_2 \in \mathbb{N}_0$, $0 \le c_1 \le 2N-2$, $0 \le c_2 \le 2N-2$. Then let $\tau_{\mathbf{c}}$ be the symmetry transformation (reflection) with respect to this center, so that

$$\tau_{\mathbf{c}}(x_1, x_2) = (c_1 - x_2, c_2 - x_2) \qquad \text{for all } (x_1, x_2) \in I_N^2.$$

Finally, let $\mathcal{P}$ denote the set of pairs $(L, \mathbf{c})$ such that L is a segment with $L \subseteq I_N^2$, $\mathbf{c}$ is a point as described above (so that $2\mathbf{c} = \mathbf{c} + \mathbf{c} \in I_{2N-1}^2$), and for every $\mathbf{x} \in L$ we also have $\tau_{\mathbf{c}}(\mathbf{x}) \in I_N^2$. Then

Definition 9 *Let $I_N^2 \to \{-1, +1\}$ be a binary lattice. The* line-symmetry measure *of η is defined by*

$$S_\ell(\eta) = \max_{(L,\mathbf{c}) \in \mathcal{P}} \left| \sum_{\mathbf{x} \in L} \eta(\mathbf{x}) \eta(\tau_{\mathbf{c}}(\mathbf{x})) \right|.$$

The line-symmetry measure is the most demanding of the three symmetry measures and, indeed, if it is "small"$(= o(N))$ then the other two are also small. This follows from Proposition 2 and the following theorem:

Theorem 1 *For every binary N-lattice η we have*

$$S_c(\eta) \leq (2N-1)S_\ell(\eta).$$

Proof of Theorem 1. Let K be a symmetric convex polygon and τ be a symmetry transformation which leaves K in its original position: $\tau(K) = K$. We will prove that

$$\left| \sum_{\mathbf{x} \in K \cap I_N^2} \eta(\mathbf{x}) \eta(\tau(\mathbf{x})) \right| \leq (2N-1) S_\ell(\eta),$$

from this the theorem follows.

There are two different cases:

Case I: τ is a symmetry transformation with respect to a line L defined by $x_2 = Ax_1 + B$ or $x_1 = C$.

Then $K \cap I_N^2$ is a disjoint union of the non-empty segments $K_1, K_2, \ldots, K_t$ lying along the lines $L_1, L_2, \ldots, L_t$ which are perpendicular to the axis L of the symmetry transformation τ (L is the line $x_2 = Ax_1 + B$ or $x_1 = C$). Let M_i be the intersection of L and L_i (see Figure 3). Then for $\mathbf{x} \in K_i$ we have $\tau(\mathbf{x}) = \tau_{M_i}(\mathbf{x})$.

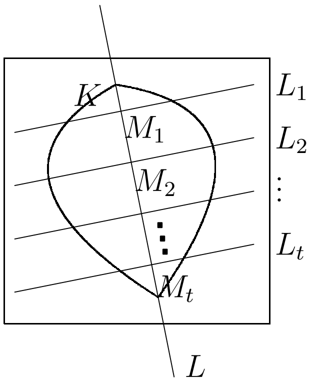

Figure 3.

Dissection of $K \cap I_N^2$ into segments in Case 1

By $K_i \neq \emptyset$, $2M_i$ has integer coordinates between 0 and $2N-2$, since if $x \in K_i$, then $2M_i = \mathbf{x} + \tau(\mathbf{x})$. Thus $2M_i$ may assume $2N-1$ different values, so that $t \leq 2N-1$. Then by this and the triangle inequality

$$\left| \sum_{\mathbf{x} \in K \cap I_N^2} \eta(\mathbf{x})\eta(\tau(\mathbf{x})) \right| \leq \sum_{i=1}^{t} \left| \sum_{\mathbf{x} \in K_i} \eta(\mathbf{x})\eta(\tau(\mathbf{x})) \right| \leq \sum_{i=1}^{t} S_\ell(\eta) = tS_\ell(\eta)$$
$$\leq (2N-1)S_\ell(\eta)$$

which was to be proved.

Case II: τ is a symmetry transformation with respect to a center C.

Then $K \cap I_N^2$ is a disjoint union of segments $K_1, K_2, \ldots, K_t$ which are lying on lines of the form $x_2 = A$ where $0 \leq A < N$, thus $t \leq N$.

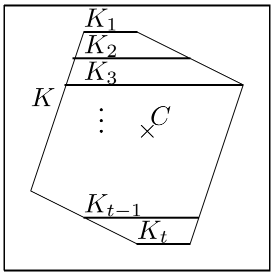

Figure 4.
Dissection of $K \cap I_N^2$ into segments in Case 2

Then

$$\left| \sum_{\mathbf{x} \in K \cap I_N^2} \eta(\mathbf{x})\eta(\tau(\mathbf{x})) \right| \leq \sum_{i=1}^{t} \left| \sum_{\mathbf{x} \in K_i} \eta(\mathbf{x})\eta(\tau_C(\mathbf{x})) \right| \leq \sum_{i=1}^{t} S_\ell(\eta) \leq NS_\ell(\eta)$$

which was to be proved.

5 The symmetry measures for truly random binary lattices

Now we will show that the symmetry measures of a truly random binary lattice $\eta: \ I_N^2 \to \{-1,+1\}$ are "small". By Proposition 2 and Theorem 1, it suffices to give an upper bound for the line-symmetry measure of η to obtain upper bounds for the other two symmetry measures. 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 2 *For every $\varepsilon > 0$ there is a number $N_0 = N_0(\varepsilon)$ 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*

$$P\left(S_\ell(\eta) < 24(N \log N)^{1/2}\right) > 1 - \varepsilon.$$

Proof of Theorem 2. We will need Bernstein's inequality:

Lemma 1 *Let $\xi_1, \dots, \xi_t$ be independent random variables which have expectation and standard deviation, and write $M(\xi_i) = M_i$ (for $i = 1, \dots, t$), $D(\xi) = D_i$ (for $i = 1, \dots, t$), $\xi = \xi_1 + \cdots + \xi_t$, $M = M_1 + \cdots + M_t$ and $D^2 = D_1^2 + \cdots + D_t^2$. Assume that K is a positive number with*

$$|\xi_i - M_i| \le K \tag{12}$$

and let

$$0 \le \mu \le \frac{D}{K}. \tag{13}$$

Then we have

$$P(|\xi - M| \ge \mu D) \le 2 \exp\left(-\frac{\mu^2}{2\left(1 + \frac{\mu K}{2D}\right)^2}\right).$$

Proof of Lemma 1. See [17, p. 324].

Lemma 2 *Let $\xi_1, \dots, \xi_t$ be independent random variables with distribution*

$$P(\xi_i = +1) = P(\xi_i = -1) = \frac{1}{2} \quad (\textit{for } i = 1, \dots, t), \tag{14}$$

and let

$$0 \le \mu \le t^{1/2}. \tag{15}$$

Then we have

$$P\left(|\xi_1 + \dots + \xi_t| \ge \mu t^{1/2}\right) \le 2 \exp\left(-\frac{2}{9}\mu^2\right).$$

Proof of Lemma 2. Using the notations of Lemma 2, now we have $M_i = 0$ and $D_i = 1$ for $i = 1, \dots, t$ whence $M = 0$ and $D = t^{1/2}$, and (12) holds with $K = 1$, so that (13) follows from (15). Thus by Lemma 1 and (15) we have

$$\begin{aligned} P\left(|\xi| \ge \mu t^{1/2}\right) &\le 2 \exp\left(-\frac{\mu^2}{2\left(1 + \frac{\mu}{2t^{1/2}}\right)^2}\right) \le 2 \exp\left(-\frac{\mu^2}{2\left(1 + \frac{1}{2}\right)^2}\right) \\ &\le 2 \exp\left(-\frac{2}{9}\mu^2\right), \end{aligned}$$

which was to be proved.

Now we will show that for a truly random binary lattice $\eta : I_N^2 \to \{-1, +1\}$, i.e., choosing every binary lattice $\eta : I_N^2 \to \{-1, +1\}$ with probability 2^{-N^2}, writing again

$$S_{L,\mathbf{c}} = \left| \sum_{x \in L} \eta(\mathbf{x}) \eta(\tau_{\mathbf{c}}(\mathbf{x})) \right|,$$

for every $(L, \mathbf{c}) \in \mathcal{P}$ we have

$$P\left(S_{L,\mathbf{c}} \ge 24(N \log N)^{1/2}\right) < \frac{4}{N^8} \quad (\text{for } N > N_0). \tag{16}$$

We have to distinguish two cases.

Case 1. Assume that L and $\tau_{\mathbf{c}}(L) = \{\tau_{\mathbf{c}}(\mathbf{x}) : \mathbf{x} \in L\}$ are disjoint. We write

$$L = \{\mathbf{x}(t) = (x_1(t), x_2(t)) : x_1(t) = a_1 t + b_1,\ x_2(t) = a_2 t + b_2, t = 0, 1, \dots, M\} \tag{17}$$

(with $M < N$). Then we have

$$S_{L,\mathbf{c}} = \left| \sum_{t=0}^{M} \eta(\mathbf{x}(t))\eta(\tau_{\mathbf{c}}(\mathbf{x}(t))) \right|. \tag{18}$$

By our assumption here the points $\mathbf{x}(0), \dots, \mathbf{x}(M)$, $\tau_{\mathbf{c}}(\mathbf{x}(0)), \dots, \tau_{\mathbf{c}}(\mathbf{x}(M))$ are pairwise distinct. It follows that the terms of this sum, i.e.,

$$\xi_0 \overset{\text{def}}{=} \eta(\mathbf{x}(0))\eta(\tau_{\mathbf{c}}(\mathbf{x}(0))), \dots, \xi_M \overset{\text{def}}{=} \eta(\mathbf{x}(M))\eta(\tau_{\mathbf{c}}(\mathbf{x}(M)))$$

are independent random variables, and each of them is of distribution (14). Write $\mu = 6(\log N)^{1/2}$. If $\mu = 6(\log N)^{1/2} \leq (M+1)^{1/2}$ then by Lemma 2 we have

$$\begin{aligned} P\left(S_{L,\mathbf{c}} \geq 6\left(N \log N\right)^{1/2}\right) &= P\left(S_{L,\mathbf{c}} \geq \mu N^{1/2}\right) \leq P\left(S_{L,\mathbf{c}} \geq \mu(M+1)^{1/2}\right) \\ &= P\left(|\xi_0 + \dots + \xi_M| \geq \mu(M+1)^{1/2}\right) \\ &\leq 2\exp\left(-\frac{2}{9}\mu^2\right) = 2\exp(-8\log N) = \frac{2}{N^8}. \end{aligned}$$

If $\mu = 6(\log N)^{1/2} > (M+1)^{1/2}$, trivially we have

$$S_{L,\mathbf{c}} = |\xi_0 + \dots + \xi_M| \leq M+1 < 36\log N < 6(N\log N)^{1/2}$$

for large enough N, whence

$$P\left(S_{L,\mathbf{c}} \geq 6\left(N\log N\right)^{1/2}\right) \leq P\left(S_{L,\mathbf{c}} \geq 36\log N\right) = 0.$$

Thus in both cases we have

$$P\left(S_{L,\mathbf{c}} \geq 6\left(N\log N\right)^{1/2}\right) < \frac{2}{N^8} \quad \text{for } L \cap \tau_{\mathbf{c}}(L) = \emptyset. \tag{19}$$

Case 2. Assume that $L \cap \tau_{\mathbf{c}}(L) \neq \emptyset$. Let $\mathbf{x}(t_1) \in L$, $\tau_{\mathbf{c}}(\mathbf{x}(t_2)) \in \tau_{\mathbf{c}}(L)$ and $\mathbf{x}(t_1) = \tau_{\mathbf{c}}(\mathbf{x}(t_2))$. Then writing again $\mathbf{c} = \left(\frac{c_1}{2}, \frac{c_2}{2}\right)$ and using the notation (17), we have

$$\begin{aligned} 2\mathbf{c} = (c_1, c_2) &= \mathbf{x}(t_2) + \tau_{\mathbf{c}}(x(t_2)) = \mathbf{x}(t_2) + \mathbf{x}(t_1) \\ &= (a_1t_2 + b_1, a_2t_2 + b_2) + (a_1t_1 + b_1, a_2t_1 + b_2) \\ &= (a_1(t_1+t_2) + 2b_1, a_2(t_1+t_2) + 2b_2) \end{aligned}$$

whence

$$a_1\frac{t_1+t_2}{2}+b_1=\frac{c_1}{2},$$
$$a_2\frac{t_1+t_2}{2}+b_2=\frac{c_2}{2},$$

so that writing $t_{\mathbf{c}}=\frac{t_1+t_2}{2}$ we have

$$\mathbf{c}=\mathbf{x}(t_{\mathbf{c}})=(a_1t_{\mathbf{c}}+b_1,a_2t_{\mathbf{c}}+b_2)$$

and, clearly $0\le t_{\mathbf{c}}\le M$. Then either

$$0\le t_{\mathbf{c}}\le\frac{M}{2} \tag{20}$$

or

$$\frac{M}{2}<t_{\mathbf{c}}\le M; \tag{21}$$

we may assume that (20) holds ((21) could be handled similarly). Then, writing

$$\delta(\mathbf{c})=\begin{cases}1 & \text{if } t_{\mathbf{c}}\in\mathbb{Z}\\ 1 & \text{if } t_{\mathbf{c}}\notin\mathbb{Z}\end{cases}$$

(note that $2t_{\mathbf{c}}=t_1+t_2\in\mathbb{Z}$) we have

$$\begin{aligned}S_{L,\mathbf{c}}&=\left|\sum_{t=0}^{M}\eta(\mathbf{x}(t))\eta(\tau_{\mathbf{c}}(\mathbf{x}(t)))\right|\\&=\left|\sum_{t=0}^{2t_{\mathbf{c}}}\eta(\mathbf{x}(t))\eta(\tau_{\mathbf{c}}(\mathbf{x}(t)))+\sum_{t=2t_{\mathbf{c}}+1}^{M}\eta(\mathbf{x}(t))\eta(\tau_{\mathbf{c}}(\mathbf{x}(t)))\right|\\&=\left|2\sum_{0\le t<t_{\mathbf{c}}}\eta(\mathbf{x}(t))\eta(\tau_{\mathbf{c}}(\mathbf{x}(t)))+\delta(\mathbf{c})\mu^2(\mathbf{x}(t_{\mathbf{c}}))+\sum_{t=2t_{\mathbf{c}}+1}^{M}\eta(\mathbf{x}(t))\eta(\tau_{\mathbf{c}}(\mathbf{x}(t)))\right|\\&\le 2\left|\sum_{0\le t<t_{\mathbf{c}}}\eta(\mathbf{x}(t))\eta(\tau_{\mathbf{c}}(\mathbf{x}(t)))\right|+1+\left|\sum_{t=2t_{\mathbf{c}}+1}^{M}\eta(\mathbf{x}(t))\eta(\tau_{\mathbf{c}}(\mathbf{x}(t)))\right|.\end{aligned}$$

Thus it follows from

$$S_{L,\mathbf{c}}\ge 24(N\log N)^{1/2}$$

that at least one of the inequalities

$$\left|\sum_{0\le t<t_{\mathbf{c}}} \eta(\mathbf{x}(t))\eta(\tau_{\mathbf{c}}(\mathbf{x}(t)))\right| \ge 6(N\log N)^{1/2},$$

$$1 \ge 6(N\log N)^{1/2} \tag{22}$$

and

$$\left|\sum_{t=2t_{\mathbf{c}}+1}^{M} \eta(\mathbf{x}(t))\eta(\tau_{\mathbf{c}}(\mathbf{x}(t)))\right| \ge 6(N\log N)^{1/2}$$

holds. But (22) does not hold for $N > 2$, so that

$$\begin{aligned} P\left(S_{L,\mathbf{c}} \ge 24(N\log N)^{1/2}\right) \le\ & P\left(\left|\sum_{0\le t<t_{\mathbf{c}}} \eta(\mathbf{x}(t))\eta(\tau_{\mathbf{c}}(\mathbf{x}(t)))\right| \ge 6(N\log N)^{1/2}\right) \\ & + P\left(\left|\sum_{t=2t_{\mathbf{c}}+1}^{M} \eta(\mathbf{x}(t))\eta(\tau_{\mathbf{c}}(\mathbf{x}(t)))\right| \ge 6(N\log N)^{1/2}\right). \end{aligned}$$

Both these last two cases are the type considered in Case 1, i.e., the points $\mathbf{x}(t), \tau_{\mathbf{c}}(\mathbf{x}(t))$ are distinct. Thus we may apply (19). Then we obtain for large enough N that

$$P\left(S_{L,\mathbf{c}} \ge 24(N\log N)^{1/2}\right) < \frac{4}{N^8} \quad \text{for } L\cap\tau_{\mathbf{c}}(L) \ne \emptyset. \tag{23}$$

For N large enough (16) follows from (19) and (23). By (16), for large N we have

$$\begin{aligned} P\left(S_\ell(\eta) \ge 24(N\log N)^{1/2}\right) &= P\left(\max_{(L,\mathbf{c})\in\mathcal{P}} S_{L,\mathbf{c}} \ge 24(N\log N)^{1/2}\right) \\ &\le \sum_{(L,\mathbf{c})\in\mathcal{P}} P\left(S_{L,\mathbf{c}} \ge 24(N\log N)^{1/2}\right) \\ &< \frac{4}{N^8}\sum_{(L,\mathbf{c})\in\mathcal{P}} 1. \end{aligned} \tag{24}$$

L is uniquely determined by $a_1, b_1.a_2, b_2$ and M, and since all these integers belong to the interval $[-N, +N]$, thus L can be chosen in at most $(2N+1)^5$ ways, while $\mathbf{c}$ can be chosen from the $(2N-1)^2$ points in I^2_{2N-1} so that

$$\sum_{(L,\mathbf{c})\in\mathcal{P}} 1 \le (2N+1)^7. \tag{25}$$

If $N > N_0(\varepsilon)$ then it follows from (24) and (25) that

$$P\left(S_\ell(\eta) \geq 24(N \log N)^{1/2}\right) < \varepsilon$$

which completes the proof of Theorem 2.

6 The minimum of the rectangle symmetry measure of binary lattices

In the one dimensional case the minimum of the correlation measures has been studied in [2] (see also [4] and [12]) and Gyarmati proved in [8] that for every binary sequence $E_N \in \{-1,+1\}^N$ we have $S(E_N) \gg \sqrt{N}$. Now we will prove the two dimensional analogue of Gyarmati's result (the n-dimensional case could be handled in the same way easily) and we will study the minima of the other pseudorandom measures in a sequel of this paper:

Theorem 3 *For every $N \in \mathbb{N}$ and binary N-lattice η we have*

$$S_r(\eta) \geq \frac{N}{2}.$$

Proof of Theorem 3. We will write $e^{2\pi i a/N} = e_N(a)$. Using the Cauchy-Schwarz inequality and Parseval formula we obtain

$$\begin{aligned}
\mathcal{J} &\stackrel{\text{def}}{=} \sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\left|\sum_{n=0}^{N-1}\sum_{m=0}^{N-1}\eta(n,m)e_N(ni)e_N(mj)\right|^4 \\
&\geq \frac{1}{N^2}\left(\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\left|\sum_{n=0}^{N-1}\sum_{m=0}^{N-1}\eta(n,m)e_N(ni)e_N(mj)\right|^2\right)^2 \\
&= \frac{1}{N^2}\Bigg(\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\sum_{n=0}^{N-1}\sum_{m=0}^{N-1}\sum_{n'=0}^{N-1}\sum_{m'=0}^{N-1}\eta(n,m)\overline{\eta(n',m')} \\
&\qquad e_N((n-n')i)e_N((m-m')j)\Bigg)^2 \\
&= \frac{1}{N^2}\Bigg(\sum_{n=0}^{N-1}\sum_{m=0}^{N-1}\sum_{n'=0}^{N-1}\sum_{m'=0}^{N-1}\eta(n,m)\overline{\eta(n',m')} \\
&\qquad \sum_{i=0}^{N-1}e_N((n-n')i)\sum_{j=0}^{N-1}e_N((m-m')j)\Bigg)^2 \\
&= \frac{1}{N^2}\left(N^2\sum_{n=0}^{N-1}\sum_{m=0}^{N-1}|\eta(n,m)|^2\right)^2 = \frac{1}{N^2}\left(N^2\cdot N^2\right)^2 \\
&= N^6.
\end{aligned}$$

Using the Parseval formula again we get

$$\begin{aligned}
\mathcal{J} &\stackrel{\text{def}}{=} \sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\left|\left(\sum_{n=0}^{N-1}\sum_{m=0}^{N-1}\eta(n,m)e_N(ni)e_N(mj)\right)^2\right|^2 \\
&= \sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\left|\sum_{n=0}^{N-1}\sum_{m=0}^{N-1}\sum_{n'=0}^{N-1}\sum_{m'=0}^{N-1}\eta(n,m)\eta(n',m')\right. \\
&\qquad\qquad \left. e_N((n+n')i)e_N((m+m')j)\right|^2 \\
&= \sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\left|\sum_{k=0}^{2N-2}\sum_{\ell=0}^{2N-2}\left(\sum_{\substack{\max\{k-N+1,0\}\le n\\ \le\min\{k,N-1\}}}\ \sum_{\substack{\max\{\ell-N+1,0\}\le m\\ \le\min\{\ell,N-1\}}}\right.\right. \\
&\qquad\qquad \left.\left.\eta(n,m)\eta(k-n,\ell-m)\right)e_N(ki)e_N(\ell j)\right|^2 \\
&= N^2\sum_{k=0}^{2N-2}\sum_{\ell=0}^{2N-2}\left|\sum_{\substack{\max\{k-N+1,0\}\le n\\ \le\min\{k,N-1\}}}\ \sum_{\substack{\max\{\ell-N+1,0\}\le m\\ \le\min\{\ell,N-1\}}}\eta(n,m)\eta(k-n,\ell-m)\right|^2 \\
&= N^2\sum_{k=0}^{2N-2}\sum_{\ell=0}^{2N-2}\left(S_r(\eta)\right)^2 \le N^4\left(S_r(\eta)\right)^2.
\end{aligned}$$

Thus

$$N^6 \le \mathcal{J} \le 4N^4\left(S_r(\eta)\right)^2,$$

so that,

$$\frac{N}{2} \le S_r(\eta),$$

which was to be proved.

7 A universally good construction

Next we will present a construction for which all the pseudorandom measures we have defined are small.

Theorem 4 *Let $p \geq 5$ be a prime, $a, b \in \mathbb{F}_p$, $a \neq \pm b$ such that the polynomials $x^3 + x + a$ and $x^3 + x + b \in \mathbb{F}_p[x]$ are irreducible over $\mathbb{F}_p$, and let $n_1, n_2, \dots, n_r \in \mathbb{F}_p$ be non-quadratic residues modulo p. Define*

$$f(x_1, x_2) = (x_1^3 + x_1 + a)(x_2^3 + x_2 + b) \prod_{i=1}^{r} (x_1^2 - n_i x_2^2) \in \mathbb{F}_p[x_1, x_2].$$

Let $k = \deg f(x_1, x_2) = 2r + 6$. Then for a binary p-lattice defined by (5) we have

$$Q_\ell(\eta) \leq 11k\ell p^{3/2} \log p \tag{26}$$

and

$$S_\ell(\eta) \leq 18kp^{1/2} \log p. \tag{27}$$

Note that it follows from (27), Proposition 2 and Theorem 1 that the rectangle and convex symmetry measures are also small:

$$S_r(\eta) \leq S_c(\eta) \ll pS_\ell(\eta) \ll kp^{3/2} \log p.$$

Proof of Theorem 4. First we prove (26). In order to estimate $Q_\ell(\eta)$ we will need two lemmas.

Lemma 3 *If $\mathbb{F}$ is a field and $n \in \mathbb{N}$ then in $\mathbb{F}[x_1, x_2, \dots, x_n]$ every polynomial has a factorization into irreducible polynomials which is unique apart from constant factors and reordering.*

Proof of Lemma 3. See, for example, [16, Theorem 207].

Lemma 4 *Suppose that $f \in \mathbb{F}_p[x_1, x_2]$ is a polynomial such that there are no distinct $\mathbf{d_1}, \mathbf{d_2}, \dots, \mathbf{d}_\ell \in \mathbf{F}_p^2$ with the property that $f(\mathbf{x} + \mathbf{d_1}) \cdots f(\mathbf{x} + \mathbf{d}_\ell)$ is of the form $cg(\mathbf{x})^2$ with $c \in \mathbb{F}_p$, $g \in \mathbb{F}_p[x_1, x_2]$. Let k be the degree of the polynomial $f(x_1, x_2)$. Then for the binary p-lattice η defined in (5) we have*

$$Q_\ell(\eta) < 11k\ell p^{3/2} \log p.$$

Proof of Lemma 4. This is Lemma 5 in [10].

Let $f(x_1, x_2)$ be a polynomial as it is described in Theorem 4. We will prove that if $\mathbf{d_1}, \mathbf{d_2}, \dots, \mathbf{d}_\ell \in \mathbf{F}_p^2$ are distinct elements then $f(\mathbf{x}+\mathbf{d_1}) \cdots f(\mathbf{x}+\mathbf{d}_\ell)$ is not of the form $cg(\mathbf{x})^2$ with $c \in \mathbb{F}_p$, $g \in \mathbb{F}_p[x_1, x_2]$. Then using Lemma 4 we get (26).

Let $\mathbf{d_i} = (d_i', d_i'')$ for $1 \le i \le \ell$ and let

$$h(\mathbf{x}) = f(\mathbf{x} + \mathbf{d_1}) \cdots f(\mathbf{x} + \mathbf{d}_\ell).$$

Then $h(\mathbf{x})$ is a product of the following irreducible polynomials:

$$\begin{aligned} p_i(x_1, x_2) &= (x_1 + d_i')^3 + (x_1 + d_i') + a \quad \text{for } 1 \le i \le \ell, \\ q_i(x_1, x_2) &= (x_2 + d_i'')^3 + (x_2 + d_i'') + b \quad \text{for } 1 \le i \le \ell, \\ g_{i,j}(x_1, x_2) &= (x_1 + d_i')^2 - n_j(x_2 + d_i'')^2 \quad \text{for } 1 \le i \le \ell,\ 1 \le j \le r. \end{aligned}$$

Clearly there is no $1 \le i \le \ell$, $1 \le j \le r$, $1 \le s \le \ell$, $c \in \mathbb{F}_p$ such that

$$g_{i,j}(\mathbf{x}) = cp_s(\mathbf{x})$$

or

$$g_{i,j}(\mathbf{x}) = cq_s(\mathbf{x})$$

since the degree of $g_{i,j}$ is 2 and the degree of both p_s and q_s is 3. It is also easy to see that there are no $1 \le i_1, i_2 \le \ell$, $1 \le j_1, j_2 \le r$, $(i_1, j_1) \neq (i_2, j_2)$ and $c \in \mathbb{F}_p$ such that

$$g_{i_1,j_1}(\mathbf{x}) = cg_{i_2,j_2}(\mathbf{x}). \tag{28}$$

Indeed, we have

$$\begin{aligned} g_{i_1,j_1}(x_1, x_2) &= x_1^2 + 2d_{i_1}' x_1 - n_{j_1} x_2^2 - 2n_{j_1} d_{i_1}'' x_2 + (d_{i_1}')^2 - n_{j_1}(d_{i_1}'')^2, \\ g_{i_2,j_2}(x_1, x_2) &= x_1^2 + 2d_{i_2}' x_1 - n_{j_2} x_2^2 - 2n_{j_2} d_{i_2}'' x_2 + (d_{i_2}')^2 - n_{j_2}(d_{i_2}'')^2, \end{aligned}$$

thus it would follow from (28) that

$$\begin{aligned} 1 &= c, \\ 2d'_{i_1} &= 2cd'_{i_2}, \\ n_{j_1} &= cn_{j_2}, \\ 2n_{j_1}d''_{i_1} &= 2cn_{j_2}d''_{i_1} \end{aligned}$$

Then $1 = c$, $d'_{i_1} = d'_{i_2}$, $n_{j_1} = n_{j_2}$, $d''_{i_1} = d''_{i_2}$. Thus $n_{j_1} = n_{j_2}$, $d_{i_1} = d_{i_2}$. But then $i_1 = i_2$ and $j_1 = j_2$, which contradicts $(i_1, j_1) \neq (i_2, j_2)$.

Thus the irreducible factor $g_{1,1}(\mathbf{x})$ appears exactly once in the factorization of $h(\mathbf{x})$. By Lemma 3, $h(\mathbf{x})$ can not be of the form $cg(\mathbf{x})^2$ with $c \in \mathbb{F}_p$, $g \in \mathbb{F}_p[x_1, x_2]$. This completes the proof of (26).

Next we prove (27). Let L be a segment of I_p^2, thus

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

(with $M \leq p$) where $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ and $(a_1, a_2) \neq (0, 0)$. Since $L \subseteq I_p^2$ we may assume that $0 \leq a_1 < p$, $0 \leq a_2 < p$.

Let $\mathbf{c} = \left(\frac{c_1}{2}, \frac{c_2}{2}\right)$ be a point with $c_1, c_2 \in \mathbb{N}$, $0 \leq c_1, c_2 < 2p$, and $(L, \mathbf{c}) \in \mathcal{P}$. We will prove that

$$S_{L,\mathbf{c}} \stackrel{\text{def}}{=} \left| \sum_{x \in L} \eta(\mathbf{x}) \eta(\tau_{\mathbf{c}}(\mathbf{x})) \right| \leq 18kp^{1/2} \log p,$$

and from this the theorem immediately follows.

This sum can be rewritten as

$$S_{L,\mathbf{c}} = \sum_{t=0}^{M} \eta((a_1 t + b_1, a_2 t + b_2)) \eta(\tau_{\mathbf{c}}(a_1 t + b_1, a_2 t + b_2)).$$

Here

$$\tau_{\mathbf{c}}(a_1 t + b_1, a_2 t + b_2) = (-a_1 t + c_1 - b_1, -a_2 t + c_2 - b_2) = (-a_1 t + d_1, -a_2 t + d_2)$$

where $d_1 = c_1 - b_1$ and $d_2 = c_2 - b_2$. We have

$$\begin{aligned}
f(a_1t+b_1, a_2t+b_2) &= \big((a_1t+b_1)^3 + (a_1t+b_1) + a\big) \\
&\quad \big((a_2t+b_2)^3 + (a_2t+b_2) + b\big) \\
&\quad \prod_{i=1}^{r} \big((a_1t+b_1)^2 - n_i(a_2t+b_2)^2\big)\,, \\
f(\tau_{\mathbf{c}}(a_1t+b_1, a_2t+b_2)) &= \big((-a_1t+d_1)^3 + (-a_1t+d_1) + a\big) \\
&\quad \big((-a_2t+d_2)^3 + (-a_2t+d_2) + b\big) \\
&\quad \prod_{i=1}^{r} \big((-a_1t+d_1)^2 - n_i(-a_2t+d_2)^2\big)\,.
\end{aligned}$$

Here all polynomials

$$\begin{aligned}
&(a_1t+b_1)^3 + (a_1t+b_1) + a, \\
&(a_2t+b_2)^3 + (a_2t+b_2) + b, \\
&(a_1t+b_1)^2 - n_i(a_2t+b_2)^2, \\
&(-a_1t+d_1)^3 + (-a_1t+d_1) + a, \\
&(-a_2t+d_2)^3 + (-a_2t+d_2) + b, \\
&(-a_1t+d_1)^2 - n_i(-a_2t+d_2)^2 \in \mathbb{F}_p[t] \qquad (29)
\end{aligned}$$

are irreducible. Indeed the third degree polynomials are shifted version of the irreducible polynomials t^3+t+a, t^3+t+b, and the second degree polynomials are of the form $(A_1t+B_1)^2 - n_i(A_2t+B_2)^2 \in \mathbb{F}_p[t]$ whose discriminant is $4n_i(A_1B_2+B_2A_1)^2$ which is a quadratic non-residue.

Thus $f(a_1t+b_1, a_2t+b_2)$ and $f(\tau_{\mathbf{c}}(a_1t+b_1, a_2t+b_2))$ are never 0. It follows that

$$\begin{aligned}
S_{L,\mathbf{c}} &= \left| \sum_{t=0}^{M} \left(\frac{f(a_1t+b_1, a_2t+b_2)}{p}\right) \left(\frac{f(-a_1t+d_1, -a_2t+d_2)}{p}\right) \right| \\
&= \left| \sum_{t=0}^{M} \left(\frac{f(a_1t+b_1, a_2t+b_2) f(-a_1t+d_1, -a_2t+d_2)}{p}\right) \right|.
\end{aligned}$$

Next we prove that $f(a_1t+b_1, a_2t+b_2)f(-a_1t+d_1, -a_2t+d_2)$ is not of the form $cg(t)^2$. Then by using the following lemma we will prove (27).

Lemma 5 *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 5. This is a consequence of Lemma 2 in [1] which was derived from Weil's theorem [21].

By Lemma 5 we get $S_{L,\mathbf{c}} \le 18kp^{1/2} \log p$, from which Theorem 4 follows. It remains to prove that $f(a_1t+b_1, a_2t+b_2)f(-a_1t+d_1, -a_2t+d_2)$ is not of the form $cg(t)^2$.

Since $(a_, a_2) \ne (0,0)$ by symmetry reasons we may suppose that $a_1 \ne 0$.

Lemma 6 *Let $p \ge 5$ be a prime, $a_1 \ne 0$ and $f \in \mathbb{F}_p[x_1, x_2]$ be a polynomial as it is described in Theorem 4. Then in the factorization of*

$$f(a_1t+b_1, a_2t+b_2)f(-a_1t+d_1, -a_2t+d_2) \in \mathbb{F}_p[t]$$

into irreducible factors, the irreducible polynomial $(a_1t+b_1)^3 + (a_1t+b_1) + a$ has multiplicity 1.

Then by Lemma 3 and Lemma 6 the product

$$f(a_1t+b_1, a_2t+b_2)f(-a_1t+d_1, -a_2t+d_2) \in \mathbb{F}_p[t]$$

can not be of the form $cg(t)^2$ and this was to be proved.

Proof of Lemma 6. In (29) we listed all the irreducible polynomials which appear in the factorization $f(a_1t+b_1, a_2t+b_2)f(-a_1t+d_1, -a_2t+d_2)$. Trivially the second and third degree polynomials are different. Since $a \ne \pm b$ it follows from Lemma 7 below that the irreducible polynomial $(a_1t + b_1)^3 + (a_1t + b_1) + a$ is not a constant multiple of $(a_2t + b_2)^3 + (a_2t + b_2) + b$ or $(-a_1t + d_1)^3 + (-a_1t + d_1) + a$ or $(-a_2t + d_2)^3 + (-a_2t + d_2) + b$. Thus the multiplicity of $(a_1t + b_1)^3 + (a_1t + b_1) + a$ is indeed 1 in the factorization of $f(a_1t + b_1, a_2t + b_2)f(-a_1t + d_1, -a_2t + d_2)$, which was the statement of Lemma 6.

Lemma 7 *Let $p \geq 5$ be a prime, $a_1 \neq 0$ and suppose that the polynomials $(a_1t+b_1)^3+(a_1t+b_1)+a$ and $(At+B)^3+(At+B)+D$ are constant multiple of each other, so there is a $c \in \mathbb{F}_p$ such that*

$$(a_1t + b_1)^3 + (a_1t + b_1) + a = c\left((At + B)^3 + (At + B) + D\right) \tag{30}$$

Then $a_1 = A$, $b_1 = B$ and $a = D$ or $a_1 = -A$, $b_1 = -B$ and $a = -D$.

Proof of Lemma 7. If (30) holds, then comparing the coefficients of the powers of t on the two sides of (30) we get

$$a_1^3 = cA^3, \tag{31}$$

$$3a_1^2b_1 = 3cA^2B, \tag{32}$$

$$3a_1b_1^2 + a_1 = 3cAB^2 + cA, \tag{33}$$

$$b_1^3 + b_1 + a = cB^3 + cB + cD. \tag{34}$$

By (31)

$$c = a_1^3\left(A^{-1}\right)^3. \tag{35}$$

By (32) and (35)

$$b_1 = a_1B\left(A^{-1}\right). \tag{36}$$

By (33), (35) and (36)

$$A^2 = a_1^2$$

whence

$$A = \pm a_1.$$

Case I If $A = a_1$, then by (35)

$$c = 1$$

and by (36)

$$b_1 = B,$$

thus by (34)

$$a = D,$$

and this proves Lemma 7.

Case II If $A = -a_1$, then by (35)

$$c = -1$$

and by (36)

$$b_1 = -B,$$

thus by (34)

$$a = -D,$$

which completes the proof of Lemma 7.

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] V. Anantharam, *A technique to study the correlation measures of binary sequences*, Discrete Math. 308, 24 (2008), 6203 -6209.

[5] T. Banakh and I. Protasov, *Symmetry and colorings: some results and open problems*, arXiv:0901.3356v2.

[6] T. Banakh, O. Verbitsky and Ya. Vorobets, *A Ramsey treatment of symmetry*, Electron. J. Combin. 7 (2000), Research Paper 52, 25pp.

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

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

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

[10] K. Gyarmati, A. Sárközy and C. L. Stewart, *On Legendre symbol lattices*, Unif. Distrib. Theory, 4 (2009), no. 1, 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] G. Martin and K. O'Bryant, *The symmetric subset problems in continous Ramsey theory*, Experiment. Math. 16 (2007), 145-165.

[14] G. Martin and K. O'Bryant, *The supremum of autoconvolutions, with applications to additive number theory*, Illinois J. Math., to appear.

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

[16] L. Rédei, *Algebra*, Pergamon Press, Oxford-New York-Toronto, Ont. 1967.

[17] A. Rényi, *Wahrscheinlichkeitstrechung*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1962.

[18] O. Verbitsky, *Symmetry subsets of lattice paths*, INTEGERS: an Electronic Journal of Combinatorial Number Theory, vol. 0 (2000), A05, 16 pages.

[19] O. Verbitsky, *Ramseyan variations on symmetric subsequences*, Algebra Discrete Math. 2003, no. 1, 111-124.

[20] O. Verbitsky, *Structural properties of extremal asymmetric colorings*, Algebra Discrete Math. 2003, no. 4, 92-117.

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

[22] H. Weyl, *Symmetry*. Reprint of the 1952 original. Princeton Science Library. Princeton, NJ, Princeton University Press, 1989.