Measures of pseudorandomness of finite binary lattices, I

(The measures Q_k, normality.)

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 Hubert, Mauduit and Sárközy defined the notion of binary lattice, they introduced the measures of pseudorandomness of binary lattices, and they constructed a binary lattice with strong pseudorandom properties with respect to these measures. Later further constructions of this type have been given by different authors.

In this series we will study the measures of pseudorandomness of binary lattices. In particular, here in Part I first the connection between the pseudorandom measures Q_k of different order is studied. Then a further measure of pseudorandomness of binary lattices, called normality measure, is introduced and studied.

2010 Mathematics Subject Classification: Primary 11K45.
Key words and phrases: binary lattice, pseudorandom, normality.

1 Introduction

Recently in a series of papers a new constructive approach has been developed to study pseudorandomess of binary sequences

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

In particular in [47] Mauduit and Sárközy first introduced the following measures of pseudorandomness: the *well-distribution measure* of E_N is defined by

$$W(E_N) = \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right| \tag{2}$$

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

$$C_k(E_N) = \max_{M,\mathbf{D}} \left| \sum_{n=1}^{M} e_{n+d_1} \dots e_{n+d_k} \right| \tag{3}$$

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

$$Q_k(E_N) = \max_{a,b,t,\mathbf{D}} \left| \sum_{j=0}^{t} e_{a+jb+d_1} \ldots e_{a+jb+d_k} \right| \tag{4}$$

where the maximum is taken over all a, b, t and $\mathbf{D} = (d_1, \ldots, d_k)$ such that all the subscripts $a + jb + d_\ell$ belong to $\{1, 2, \ldots, N\}$. 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 [11] showed that this terminology is justified since for almost all $E_N \in \{-1, +1\}^N$ both $W(E_N)$ and $C_k(E_N)$ are less than $N^{1/2}(\log N)^c$. (See also [3].) It was also shown in [47] that the Legendre symbol forms a "good" pseudorandom sequence. Later many further sequences were tested for pseudorandomness [6], [7], [8], [9], [10], [16], [17], [19], [21], [41], [44], [45], [48], [49], [50], [60], [62], [63], and further constructions were given for sequences with good pseudorandom properties by using multiplicative characters [12], [13], [14], [15], [20], [23], [26], [29], [39], [55], [59], [61], [65], [66], [68], additive characters [18], [37], [38], [43], [46], [52], [57], and both additive and multiplicative characters [42], [58], [64].

In order to encrypt a 2-dimensional digital map or picture via the analog of the Vernam cipher, instead of a pseudorandom binary sequence (as a key stream) one needs the n-dimensional extension of the theory of pseudorandomness. Such a theory has been developed recently by Hubert, Mauduit and Sárközy [31]. They introduced the following definitions:

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

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

This set is called an *n-dimensional N-lattice* or briefly an *N-lattice*. In [30] 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 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 $0 \leq t_1, t_2, \dots, t_n < N$. Then we call the set

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

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

In [31] 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 [31] 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 [30]): Let

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

Define the pseudorandom measure of order ℓ of η by

$$Q_\ell(\eta) = \max_{B, \mathbf{d_1}, \dots, \mathbf{d}_\ell} \left| \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d_1}) \cdots \eta(\mathbf{x} + \mathbf{d}_\ell) \right|, \tag{5}$$

where the maximum is taken over all distinct $\mathbf{d_1}, \dots, \mathbf{d}_\ell \in I_N^n$ and all box N-lattices B such that $B + \mathbf{d_1}, \dots, B + \mathbf{d}_\ell \subseteq I_N^n$. Note that in the one dimensional special case $Q_1(\eta)$ is the same as the well-distribution measure (2), and for every $k \in \mathbb{N}$, $Q_k(\eta)$ is the combined measure (4).

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 [31], 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. Constructions for binary lattices, resp. large families of binary lattices with strong pseudorandom properties were presented in [27], [28], [31], [40], [53], [54], [56].

In the one-dimensional case further related notions were also introduced and studied: the normality measure [47]; the symmetry measure [24]; the properties of the measures of pseudorandomess and the connection between them [1], [2], [3], [4], [5], [8], [22], [25], [51], [69]. (See [67] for a survey of the early work in this field.) In this series of papers our goal is to introduce and study the *n-dimensional analogs* of these notions. More precisely, we will restrict ourselves to the special case $n = 2$, since the case of general n could be handled similarly but then the formulas would be much more lengthy and complicated. In particular, in this Part I of the series we will study the *connection between the measures Q_k and Q_ℓ for $k \neq \ell$, and we will introduce and study the normality measure.*

2 Connection between the measures Q_k and Q_ℓ

In [11] we wrote "...one might like to know whether it suffices to study correlation of order, say, 2, or correlations of higher order must be studied as well. This question can be answered by analyzing the connection between $C_k(E_N)$ and $C_\ell(E_N)$ for $k \neq \ell \ldots$" Indeed, we proved in [11]:

Theorem A *For $k, \ell, N \in \mathbb{N}$, $k \mid \ell$, $E_N \in \{-1, +1\}^N$ we have*

$$C_k(E_N) \leq N \left(\frac{(\ell!)^{k/\ell}}{k!} \left(\frac{C_\ell(E_N)}{N} \right)^{k/\ell} + \left(\frac{\ell^2}{N} \right)^{k/\ell} \right).$$

It follows that if $k, \ell \in \mathbb{N}$, $k \mid \ell$, $N \longrightarrow \infty$ and $C_\ell(E_N)$ is "small", more exactly, $C_\ell(E_N) = o(N)$, then $C_k(E_N)$ is also small ($= o(N)$). We also showed that here the condition $k \mid \ell$ is necessary and, indeed, for fixed k and for $N \longrightarrow \infty$ there is an $E_N \in \{-1,+1\}^N$ such that $C_\ell(E_N)$ is small when $k \nmid \ell$, while $C_k(E_N)$ is large ($\gg N$):

Theorem B *If $k, N \in \mathbb{N}$ and $k \leq N$, then there is a sequence $E_N \in \{-1,+1\}^N$ such that if $\ell \in \mathbb{N}$, $\ell \leq N/2$, then*

$$C_\ell(E_N) > \frac{N-\ell}{k} - 54k^2 N^{1/2} \log N \qquad \text{if } k \mid \ell$$

and

$$C_\ell(E_N) < 27k^2 \ell N^{1/2} \log N \qquad \text{if } k \nmid \ell.$$

In [22] and [51] we also analyzed the connection between $W(E_N)(= Q_1(E_N))$ and $C_k(E_N)$, but we have never studied the connection between $Q_k(E_N)$ and $Q_\ell(E_N)$.

Here first we will study the connection between $Q_k(\eta)$ and $Q_\ell(\eta)$ for two dimensional binary lattices η (but our results and proofs could be adapted to the cases when the dimension is 1 or greater than 2).

Theorem 1 *For $k, \ell, N \in \mathbb{N}$, $k < N$, $\ell < N$, $k \mid \ell$ and every binary lattice $\eta: I_N^2 \longrightarrow \{-1,+1\}$ we have*

$$Q_k(E_N) \leq N^2 \left(\left(\frac{\ell}{N}\right)^{2k/\ell} + \frac{4(\ell!)^{k/\ell}}{k!} \left(\frac{Q_\ell(\eta)}{N^2}\right)^{k/\ell} \right).$$

It follows that if $k \mid \ell$, $N \longrightarrow \infty$ and $Q_\ell(\eta) = o(N^2)$, then $Q_k(\eta)$ is also $o(N^2)$.

Proof. By (5) it suffices to prove that for all distinct $\mathbf{d_1}, \dots, \mathbf{d_k} \in I_N^2$ and box N-lattices B with $B + \mathbf{d_1}, \dots, B + \mathbf{d_k} \subseteq I_N^2$ we have

$$\left| \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d_1}) \dots \eta(\mathbf{x} + \mathbf{d_k}) \right| \leq N^2 \left(\left(\frac{\ell}{N}\right)^{2k/\ell} + \frac{4(\ell!)^{k/\ell}}{k!} \left(\frac{Q_\ell(\eta)}{N^2}\right)^{k/\ell} \right). \tag{6}$$

Write $\ell/k = t$ so that $t \in \mathbb{N}$ by $k \mid \ell$. Then clearly

$$\begin{aligned}
&\left(\sum_{\mathbf{x}\in B} \eta(\mathbf{x}+\mathbf{d_1})\dots\eta(\mathbf{x}+\mathbf{d_k})\right)^t \\
&= \left(\sum_{\mathbf{x_1}\in B} \eta(\mathbf{x_1}+\mathbf{d_1})\dots\eta(\mathbf{x_1}+\mathbf{d_k})\right)\dots\left(\sum_{\mathbf{x_t}\in B} \eta(\mathbf{x_t}+\mathbf{d_t})\dots\eta(\mathbf{x_t})+\mathbf{d_k})\right) \\
&= \sum_{\mathbf{x_1}\in B}\cdots\sum_{\mathbf{x_t}\in B} \eta(\mathbf{x_1}+\mathbf{d_1})\dots\eta(\mathbf{x_1}+\mathbf{d_k})\dots\eta(\mathbf{x_t}+\mathbf{d_1})\dots\eta(\mathbf{x_t}+\mathbf{d_k}) \\
&= S_1 + S_2 \qquad (7)
\end{aligned}$$

where S_1 denotes the contribution of those terms $\eta(\mathbf{x_1}+\mathbf{d_1})\dots\eta(\mathbf{x_t}+\mathbf{d_k})$ where there are two equal vectors amongst the $\mathbf{x_i}+\mathbf{d_u}$'s:

$$\mathbf{x_i}+\mathbf{d_u} = \mathbf{x_j}+\mathbf{d_v} \tag{8}$$

(with $(i,u) \neq (j,v)$) while in S_2 all these vectors are distinct.

First we estimate S_1. In (8), u and v can be chosen in at most k ways, i, j both in t ways, $\mathbf{x_j}$ (for fixed j) in $|B|$ (=number of lattice points in B)$\leq N^2$ ways, and $u, v, \mathbf{x_j}$ determine $\mathbf{x_i}$ uniquely. Each of the $t-2$ remaining $\mathbf{x}_h$'s can be chosen in at most N^2 ways, so that S_1 has at most $k^2t^2N^2(N^2)^{t-2} = \ell^2N^{2(t-1)}$ terms and thus

$$|S_1| \leq \ell^2 N^{2(t-1)}. \tag{9}$$

Now we estimate S_2. We will use the lexicographical ordering of the lattice points $(x,y) \in \mathbb{N}^2$ (i.e., the vectors $\mathbf{z} = (x,y)$): we write $(x,y) < (u,v)$ if either $x < u$, or $x = u$ and $y < v$. Then clearly we have $(x,y)+(c,d) < (u,v)+(c,d)$ if $(x,y),(u,v),(c,d) \in \mathbb{N}^2$ and $(x,y) < (u,v)$.

We may assume that we have $\mathbf{d_1} < \mathbf{d_2} < \cdots < \mathbf{d_k}$ in terms of this ordering. Consider each of the terms $\eta(\mathbf{x_1}+\mathbf{d_1})\dots\eta(\mathbf{x_t}+\mathbf{d_k})$ in S_2, and rearrange the order of the factors $\eta(\mathbf{x_i}+\mathbf{d_u})$ so that the vectors should be increasing:

$\eta(\mathbf{x_1}+\mathbf{d_1})\dots\eta(\mathbf{x_t}+\mathbf{d_k}) = \eta(\mathbf{w_1})\dots\eta(\mathbf{w_\ell})$, $\mathbf{w_1} < \cdots < \mathbf{w_\ell}$. We t-colour these factors $\eta(\mathbf{w_1}),\dots,\eta(\mathbf{w_\ell})$: if the vector $\mathbf{w_u}$ is of the form $\mathbf{w_u} = \mathbf{x_j}+\mathbf{d_v}$, then we colour the factor $\eta(\mathbf{w_u})$ by the j-th colour. Then to each term $\eta(\mathbf{w_1})\dots\eta(\mathbf{w_\ell})$ we may assign the sequence of the colours following each other in the order used to colour $\eta(\mathbf{w_1}),\dots,\eta(\mathbf{w_\ell})$. In this way we get colour patterns of length ℓ where each of the t colours occurs k times, so that the number of these colour patterns is $\ell!/(k!)^t$.

Now fix any of the colour patterns, and consider each of the terms $\eta(\mathbf{w_1})\dots\eta(\mathbf{w_\ell})$ with this fixed colour pattern. We define an equivalence relation among these terms: we say that

$$\eta(\mathbf{w_1})\dots\eta(\mathbf{w_\ell}) \sim \eta(\mathbf{v_1})\dots\eta(\mathbf{v_\ell}) \quad \text{if } \mathbf{v_1}-\mathbf{w_1}=\dots=\mathbf{v_\ell}-\mathbf{w_\ell}.$$

Clearly, this is indeed an equivalence relation. Fix a colour pattern and an equivalence class, and collect all the terms from this class. Let

$$\eta(\mathbf{a_1})\dots\eta(\mathbf{a_\ell}) \tag{10}$$

be any fixed term taken from this class. Then we have

$$\eta(\mathbf{a_1})<\dots<\eta(\mathbf{a_\ell}), \tag{11}$$

and every term belonging to the class is of the form

$$\eta(\mathbf{a_1}+\mathbf{x})\dots\eta(\mathbf{a_\ell}+\mathbf{x}), \tag{12}$$

or equivalently,

$$\eta(\mathbf{y})\eta(\mathbf{y}+(\mathbf{a_2}-\mathbf{a_1}))\dots\eta(\mathbf{y}+(\mathbf{a_\ell}-\mathbf{a_1})). \tag{13}$$

Now we will determine all vectors $\mathbf{x},\mathbf{y}\in\mathbb{N}^2$ for which the product in (12), resp. (13) appears in the sum S_2 in (7). First, observe that it follows from (11) that

$$\eta(\mathbf{a_1}+\mathbf{x})<\dots<\eta(\mathbf{a_\ell}+\mathbf{x}),$$

so that if the product (12) appears in (7), then it certainly belongs to S_2. So the question is: when does the product (12), resp. (13) appear in (7)? For

$j = 1, 2, \ldots, t$, let $\eta(\mathbf{a_{i_j}})$ denote the factor in (10) in which the j-th colour first appears; then clearly $\mathbf{a_{i_j}}$ is of the form

$$\mathbf{a_{i_j}} = \mathbf{z_j} + \mathbf{d_1} \quad \text{with some } \mathbf{z_j} \in B \quad (\text{for } j = 1, 2, \ldots, t),$$

in particular,

$$\mathbf{a_1} = \mathbf{a_{i_r}} = \mathbf{z_r} + \mathbf{d_1} \quad \text{for some } r \in \{1, 2, \ldots, t\}.$$

Then the i_j-th factor in (13) is

$$\eta(\mathbf{y} + (\mathbf{a_{i_j}} - \mathbf{a_1})) = \eta(\mathbf{y} + (\mathbf{z_j} - \mathbf{z_r})).$$

Since this is of the same colour as $\eta(\mathbf{a_{i_j}})$, thus $\mathbf{y} + (\mathbf{z_j} - \mathbf{z_r})$ must be of the form

$$\mathbf{y} + (\mathbf{z_j} - \mathbf{z_r}) = \mathbf{x_j} + \mathbf{d_1} \quad \text{with the } x_j \in B \text{ in (7)},$$

whence

$$\mathbf{y} = \mathbf{x_j} + \mathbf{d_1} + \mathbf{z_r} - \mathbf{z_j} \in B + \mathbf{d_1} + \mathbf{z_r} - \mathbf{z_j} \text{ for } j = 1, 2, \ldots, t,$$

in particular, for $j = r$ we have

$$\mathbf{y} \in B + \mathbf{d_1}.$$

It follows that we must have

$$y \in (B + \mathbf{d_1}) \bigcap \Big(\bigcap_{\substack{1 \le j \le t \\ j \ne r}} (B + \mathbf{d_r} + \mathbf{z_r} - \mathbf{z_j}) \Big). \tag{14}$$

On the other hand, reversing this argument it can be shown that if y satisfies (14), then the product in (13) belongs to the given equivalence class.

On the right hand side of (14) we have t translates of the same box B; let $B = \{(au, bv) : \ 0 \le u \le U, \ 0 \le v \le V\}$. Then it is easy to see by induction on t that the intersection of t translates is also a translate of a similar box $B' = \{(au, bv) : \ 0 \le u \le U', \ 0 \le v \le V'\}$ (with U', V' in place of U, V);

denote this translate by $B' + \mathbf{d}'$. Then the sum of the terms (13) belonging to the given equivalence class is

$$\sum_{\mathbf{y} \in B' + \mathbf{d}'} \eta(\mathbf{y})\eta(\mathbf{y} + (\mathbf{a_2} - \mathbf{a_1})) \dots \eta(\mathbf{y} + (\mathbf{a}_\ell - \mathbf{a_1}))$$
$$= \sum_{\mathbf{x} \in B'} \eta(\mathbf{x} + \mathbf{d}')\eta(\mathbf{x} + \mathbf{d}' + \mathbf{a_2} - \mathbf{a_1}) \dots \eta(\mathbf{x} + \mathbf{d}' + \mathbf{a}_\ell - \mathbf{a_1}).$$

By the definition of Q_ℓ, it follows that for any fixed equivalence class the absolute value of this sum is

$$\left| \sum_{\mathbf{y} \in B + \mathbf{d}'} \eta(\mathbf{y})\eta(\mathbf{y} + (\mathbf{a_2} - \mathbf{a_1})) \dots \eta(\mathbf{y} + (\mathbf{a}_\ell - \mathbf{a_1})) \right| \leq Q_\ell(\eta).$$

It remains to estimate the number of equivalence classes. An equivalence class is uniquely determined by the colour pattern, which can be chosen in $\ell!/(k!)^t$ ways, and by the box B' formed by the vectors $\mathbf{y}$ in (14). This box is uniquely determined by the $t-1$ vectors $\mathbf{z_r} - \mathbf{z_j}$ with $j \neq t$ (r is fixed). Each of these vectors is of the form (u, v) with $-(N-1) \leq u, v \leq N-1$, thus each of them can be chosen in less than $(2N)^2$ ways, so that B' can be chosen in less than $(2N)^{2(t-1)}$ ways. We may conclude that

$$|S_2| \leq \frac{\ell!}{(k!)^t} (2N)^{2(t-1)} Q_\ell(\eta). \tag{15}$$

It follows from (7), (9) and (15) that

$$\begin{aligned} \left| \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d_1}) \dots \eta(\mathbf{x} + \mathbf{d_k}) \right| &= (S_1 + S_2)^{1/t} \leq |S_1|^{1/t} + |S_2|^{1/t} \\ &\leq \ell^{2/t} N^2 N^{-2/t} + \frac{(\ell!)^{1/t}}{k!} 2^2 N^2 N^{-2/t} Q_\ell(\eta)^{1/t} \\ &= N^2 \left(\left(\frac{\ell}{N} \right)^{2k/\ell} + \frac{4(\ell!)^{k/\ell}}{k!} \left(\frac{Q_\ell(\eta)}{N} \right)^{k/\ell} \right) \end{aligned}$$

which proves (6) and this completes the proof of Theorem 1.

Now we will show that the condition $k \mid \ell$ is necessary in Theorem 1:

Theorem 2 *If $k, N \in \mathbb{N}$ and $k \le N$, then there is a binary N-lattice η such that if $\ell \in \mathbb{N}$, $\ell \le N/2$, then*

$$Q_\ell(\eta) \ge \frac{N(N-\ell)}{k} \qquad \text{if } k \mid \ell \tag{16}$$

and

$$Q_\ell(\eta) \ll k^2 \ell N (\log N)^2 \qquad \text{if } k \nmid \ell \tag{17}$$

Proof. Let p denote the smallest prime with $p > N$ so that, by Chebyshev's theorem,

$$N < p \le 2N$$

(whence $N - 1 \le p - 2$).

Write $q = p^2$, and the quadratic character of $\mathbb{F}_q$ will be denoted by γ. Let $\mathbf{v_1}, \mathbf{v_2}$ be a basis of the vector space formed by $\mathbb{F}_q$ over $\mathbb{F}_p$.

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

$$\eta(x_1, x_2) = \begin{cases} \gamma((x_1+1)\mathbf{v_1} + (x_2+1)\mathbf{v_2}) & \text{for } x_1 \not\equiv k-1 \pmod{k}, \\ \prod_{j=1}^{k-1} \gamma((x_1+j-1)\mathbf{v_1} + (x_2+1)\mathbf{v_2}) & \text{for } x_1 \equiv k-1 \pmod{k}. \end{cases}$$

Since $0 \le x_1, x_2 \le p-2$, η always assumes $+1$ or -1 here. First we will prove (16). Define the 2-dimensional box N-lattice B by

$$B = \{(x_1, x_2) :\ 0 \le x_1 < N - \ell,\ x_1 \equiv 0 \pmod{k},\ 0 \le x_2 < N\}.$$

Define the vectors $\mathbf{d_1}, \mathbf{d_2}, \dots, \mathbf{d_\ell}$ by

$$\mathbf{d_i} = (i-1, 0).$$

Then by the definition of the pseudorandom measure of order ℓ we have

$$\begin{aligned} Q_\ell(\eta) &\ge \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d_1}) \dots \eta(\mathbf{x} + \mathbf{d_\ell}) \\ &= \sum_{x_2=0}^{N-1} \sum_{\substack{0 \le x_1 < N-\ell \\ x_1 \equiv 0 \pmod{k}}} \eta(x_1, x_2)\eta(x_1+1, x_2) \dots \eta(x_1+\ell-1, x_2) \end{aligned}$$

Since now $k \mid \ell$, here we have

$$\begin{aligned}&\eta(x_1, x_2)\eta(x_1+1, x_2)\dots\eta(x_1+\ell-1, x_2)\\ &= \prod_{i=0}^{\ell/k-1} \eta(x_1+ik, x_2)\eta(x_1+ik+1, x_2)\dots\eta(x_1+ik+k-1, x_2).\end{aligned}$$

By the definition of η, for $x_1 \equiv 0 \pmod k$ we have

$$\eta(x_1+ik, x_2)\eta(x_1+ik+1, x_2)\dots\eta(x_1+ik+k-1, x_2) = 1.$$

It follows that

$$Q_\ell(\eta) \geq \sum_{x_2=0}^{N-1} \sum_{\substack{0\leq x_1<N-\ell\\ x_1\equiv 0 \pmod k}} 1 \geq \frac{N(N-\ell)}{k}.$$

Next we prove (17). Let B_1 be a box lattice of the form

$$B_1 = \{(x_1z_1, x_2z_2) :\ 0 \leq x_1z_1 \leq t_1(< N),\ 0 \leq x_2z_2 \leq t_2(< N),\ x_1, x_2 \in \mathbb{N}\},$$

and let $\mathbf{d_1}, \mathbf{d_2}, \dots, \mathbf{d}_\ell \in I_N^2$ be distinct vectors such that $B+\mathbf{d_1}, \dots, B+\mathbf{d}_\ell \subseteq I_N^2$.

Let

$$S = \sum_{\mathbf{x}\in B_1} \eta(\mathbf{x}+\mathbf{d_1})\dots\eta(\mathbf{x}+\mathbf{d}_\ell).$$

We will prove that

$$|S| \ll k^2\ell N(\log N)^2 \tag{18}$$

from which (17) follows. Write

$$\mathbf{d_i} = (d_1^{(i)}, d_2^{(i)}).$$

Then

$$S = \sum_{x_1=0}^{t_1/z_1}\sum_{x_2=0}^{t_2/z_2}\prod_{i=1}^{\ell} \eta(x_1z_1+d_1^{(i)}, x_2z_2+d_2^{(i)}).$$

Define

$$S(r) \stackrel{\text{def}}{=} \sum_{\substack{0\leq x_1\leq t_1/z_1\\ x_1\equiv r \pmod k}} \sum_{x_2=0}^{t_2/z_2}\prod_{i=1}^{\ell} \eta(x_1z_1+d_1^{(i)}, x_2z_2+d_2^{(i)}). \tag{19}$$

Then

$$S = \sum_{r=0}^{k-1} S(r). \tag{20}$$

Next we will prove that

$$|S(r)| \ll k\ell N(\log N)^2. \tag{21}$$

(18) follows from (20) and (21). In (19) we substitute $x_1 = y_1k + r$, so that

$$\begin{aligned} S(r) &= \sum_{0\le y_1\le (t_1/z_1-r)/k} \sum_{x_2=0}^{t_2/z_2} \prod_{i=1}^{\ell} \eta((y_1k+r)z_1 + d_1^{(i)}, x_2z_2 + d_2^{(i)}) \\ &= \sum_{0\le y_1\le (t_1/z_1-r)/k} \sum_{x_2=0}^{t_2/z_2} \prod_{i=1}^{\ell} \eta((y_1kz_1, x_2z_2) + (rz_1 + d_1^{(i)}, d_2^{(i)})). \end{aligned} \tag{22}$$

Since $B + \mathbf{d_i} \subseteq I_N^2$, for $0 \le y_1 \le (t_1/z_1 - r)/k$ we have

$$0 \le (y_1k + r)z_1 + d_1^{(i)} \le N - 1 \le p - 2.$$

For $y_1 = 0$ we get

$$1 \le rz_1 + d_1^{(i)} + 1 \le p - 1.$$

If $rz_1 + d_1^{(i)} \equiv k - 1 \pmod k$ also holds, then for $1 \le j \le k - 1$ we have

$$1 \le rz_1 + d_1^{(i)} + 1 - j \le p - 2. \tag{23}$$

We will use (23) later in the proof.

By the definition of η we have

$$\begin{aligned} &\eta((y_1kz_1, x_2z_2) + (rz_1 + d_1^{(i)}, d_2^{(i)})) \\ &= \gamma(y_1kz_1\mathbf{v_1} + x_2z_2\mathbf{v_2} + (rz_1 + d_1^{(i)} + 1)\mathbf{v_1} + (d_2^{(i)} + 1)\mathbf{v_2}) \end{aligned}$$

for $rz_1 + d_1^{(i)} \not\equiv k - 1 \pmod k$, and

$$\begin{aligned} &\eta((y_1kz_1, x_2z_2) + (rz_1 + d_1^{(i)}, d_2^{(i)})) \\ &= \prod_{j=1}^{k-1} \gamma(y_1kz_1\mathbf{v_1} + x_2z_2\mathbf{v_2} + (rz_1 + d_1^{(i)} + 1 - j)\mathbf{v_1} + (d_2^{(i)} + 1)\mathbf{v_2}) \end{aligned}$$

for $rz_1 + d_1^{(i)} \equiv k-1 \pmod{k}$.

Let $\mathcal{A}$ and $\mathcal{B}$ be the following multisets:

$$\begin{aligned}
\mathcal{A} = \{ & (rz_1 + d_1^{(i)} + 1)\mathbf{v_1} + (d_2^{(i)} + 1)\mathbf{v_2} : \ 1 \le i \le \ell, \\
& rz_1 + d_1^{(i)} \not\equiv k-1 \pmod{k}\}, \\
\mathcal{B} = \{ & (rz_1 + d_1^{(i)} + 1 - j)\mathbf{v_1} + (d_2^{(i)} + 1)\mathbf{v_2} : \ 1 \le i \le \ell, \ 1 \le j \le k-1, \\
& rz_1 + d_1^{(i)} \equiv k-1 \pmod{k}\}.
\end{aligned}$$

Here $|\mathcal{A}| = n$ and $|\mathcal{B}| = (k-1)m$ for some $n, m \in \mathbb{N}$ with

$$n + m = \ell. \tag{24}$$

Let

$$B_2 = \{y_1(kz_1\mathbf{v_1}) + x_2(z_2\mathbf{v_2}) : \ 0 \le y_1 \le (t_1/z_1 - r)/k, \ 0 \le x_2 \le t_2/z_2\}.$$

Then by (22)

$$S(r) = \sum_{\mathbf{z} \in B_2} \prod_{\alpha \in \mathcal{A} \bigcup \mathcal{B}} \gamma(\mathbf{z} + \alpha).$$

Using the multiplicativity of the quadratic character γ, we have

$$S(r) = \sum_{\mathbf{z} \in B_2} \gamma\left(\prod_{\alpha \in \mathcal{A} \bigcup \mathcal{B}} (\mathbf{z} + \alpha) \right).$$

Now we will use the following lemma

Lemma 1 *Let p be an odd prime, $n \in \mathbb{N}$, $q = p^n$ and $v_1, v_2, \ldots, v_n$ be a basis of $\mathbb{F}_q$ as a vector space over $\mathbb{F}_p$. Let χ be a multiplicative character of $\mathbb{F}_q$ of order $d > 1$ and let $f(x) \in \mathbb{F}_q[x]$ be a polynomial which is not of the form $cg(x)^d$ for $c \in \mathbb{F}_q$, $g(x) \in \mathbb{F}_q[x]$. Suppose that $f(x)$ has s distinct zeros in its splitting field over $\mathbb{F}_q$, and $k_1, \ldots, k_n$ are positive integers with $k_1 \le p, \ldots, k_n \le p$. Then writing $B = \left\{ \sum_{i=1}^{n} j_i v_i : \ 0 \le j_i < k_i \right\}$, we have*

$$\left| \sum_{z \in B} \chi(f(z)) \right| < sq^{1/2}(1 + \log p)^n.$$

This is a part of Theorem 2 in [71] (where its proof was based on A. Weil's theorem [70]).

Let $f(\mathbf{x}) = \prod_{\alpha \in \mathcal{A} \bigcup \mathcal{B}} (\mathbf{x} + \alpha)$. Then

$$S(r) = \sum_{\mathbf{z} \in B_2} \gamma(f(\mathbf{z})). \tag{25}$$

Here we may use Lemma 1, since $\mathbf{v_1}, \mathbf{v_2}$ is a basis of $\mathbb{F}_q$ as a vector space over $\mathbb{F}_p$, thus $kz_1\mathbf{v_1}, z_2\mathbf{v_2}$ is also such a basis. Thus the box B_2 is of the same type as B in Lemma 1. If we prove that $f(x) = \prod_{\alpha \in \mathcal{A} \bigcup \mathcal{B}} (x + \alpha) \in \mathbf{F}_q[x]$ is not of the form $cg(x)^d$ with $c \in \mathbb{F}_q$, $g(x) \in \mathbb{F}_q[x]$, then by Lemma 1, (24) and (25) we have

$$\begin{aligned}
|S(r)| &\le (|\mathcal{A}| + |\mathcal{B}|)\, q^{1/2}(1 + \log p)^2 \\
&\le (|\mathcal{A}| + |\mathcal{B}|)\, 2N(1 + \log(2N))^2 \\
&\le (k-1)(n+m)2N(1 + \log(2N))^2 \ll k\ell N(\log N)^2,
\end{aligned}$$

so that (21) holds and this was to be proved. Since $\mathbf{d_1}, \mathbf{d_2}, \dots, \mathbf{d}_\ell$ are distinct vectors, the elements of $\mathcal{A}$ are distinct. Similarly, the elements of $\mathcal{B}$ are also distinct: suppose that $\mathcal{B}$ has two identical elements, i.e., for $(i_1, j_1) \neq (i_2, j_2)$, $1 \le i_1, i_2 \le \ell$ and $1 \le j_1, j_2 \le k-1$ we have

$$(rz_1 + d_1^{(i_1)} + 1 - j_1)\mathbf{v_1} + (d_2^{(i_1)} + 1)\mathbf{v_2} = (rz_1 + d_1^{(i_2)} + 1 - j_2)\mathbf{v_1} + (d_2^{(i_2)} + 1)\mathbf{v_2}.$$

Then

$$rz_1 + d_1^{(i_1)} + 1 - j_1 \equiv rz_1 + d_1^{(i_2)} + 1 - j_2 \pmod p$$

and

$$d_2^{(i_1)} \equiv d_2^{(i_2)} \pmod p.$$

Since $0 \le d_2^{(i_1)}, d_2^{(i_2)} < N < p$ and by (23)

$$1 \le rz_1 + d_1^{(i_1)} + 1 - j_1,\ rz_1 + d_1^{(i_2)} + 1 - j_2 \le p$$

we also have

$$r z_1 + d_1^{(i_1)} + 1 - j_1 = r z_1 + d_1^{(i_2)} + 1 - j_2, \tag{26}$$

$$d_2^{(i_1)} = d_2^{(i_2)}. \tag{27}$$

Since $(rz_1+d_1^{(i_1)}+1-j_1)\mathbf{v_1}+(d_2^{(i_1)}+1)\mathbf{v_2}$, $(rz_1+d_1^{(i_2)}+1-j_2)\mathbf{v_1}+(d_2^{(i_2)}+1)\mathbf{v_2} \in B$, it follows from (26) that

$$j_2 - j_1 = (rz_1 + d_1^{(i_1)} + 1) - (rz_1 + d_1^{(i_2)} + 1) \equiv (k-1) - (k-1) \equiv 0 \pmod{k}.$$

But $1 \le j_1, j_2 \le k-1$, thus

$$j_1 = j_2. \tag{28}$$

By this and (26) we get

$$d_1^{(i_1)} = d_1^{(i_2)}. \tag{29}$$

It follows from (27) and (29) that

$$\mathbf{d_{i_1}} = \mathbf{d_{i_2}}.$$

But then by this and (28) we have $(i_1, j_1) = (i_2, j_2)$ which is a contradiction.

Since $\mathcal{A}$ and $\mathcal{B}$ contain different elements, thus $\prod\limits_{\alpha \in \mathcal{A} \bigcup \mathcal{B}} (x+\alpha)$ is a constant multiple of the perfect square of a polynomial if and only if $\mathcal{A} = \mathcal{B}$. Then

$$|\mathcal{A}| = |\mathcal{B}|,$$

i.e.,

$$n = (k-1)m,$$

thus by (24)

$$\ell = n + m = km.$$

But in (17) we assumed that $k \nmid \ell$. This contradiction proves that $f(x)$ is not of the form $cg(x)^2$ with $c \in \mathbb{F}_q$, $g(x) \in \mathbb{F}_q[x]$. Then (21) indeed holds. By (20) and (21)

$$S \ll k^2 \ell N (\log N)^2$$

which was to be proved.

3 The normality measure

In one dimension consider the binary sequence (1), and for $k \in \mathbb{N}$, $M \in \mathbb{N}$ and $X = \{x_1, \dots, x_k\} \in \{-1, +1\}^k$ let

$$T(E_N, M, X) = |\{n : \ 0 \le n < M, \ \{e_{n+1}, e_{n+2}, \dots, e_{n+k}\} = X\}| \,. \tag{30}$$

Definition 1 **([47])** *The* normality measure of order k *of* E_N *is defined as*

$$N_k(E_N) = \max_{X \in \{-1,+1\}^k} \max_{0 < M \le N+1-k} \left| T(E_N, M, X) - \frac{M}{2^k} \right| .$$

Definition 2 **([47])** *The* normality measure *of* E_N *is defined as*

$$N(E_N) = \max_{k \le (\log N)/\log 2} N_k(E_N).$$

It was proved in [47] that

Theorem C *For all* N, E_N *and* $k < N$ *we have*

$$N_k(E_N) \le \max_{1 \le t \le k} C_t(E_N).$$

Thus the estimate of the normality measure of order k can be reduced to the estimate of the correlation of order $\le k$.

Now we will introduce the analogous notations in 2 dimensions. For $k, \ell \in \mathbb{N}$ let $\mathcal{M}(k, \ell)$ denote the set of the $(k \times \ell)$ matrices $A = (a_{ij})$ with $a_{ij} \in \{-1, +1\}$ for $1 \le i \le k$, $1 \le j \le \ell$, let $\eta(x, y) : \ I_N^2 \to \{-1, +1\}$ be a binary lattice, and for $X = (x_{ij}) \in \mathcal{M}(k, \ell)$ let

$$\begin{aligned} Z(\eta, U, V, X) = |\{(m, n) : \ & 0 \le m < U, \ 0 \le n < V, \\ & \eta(m-1+i, n-1+j) = x_{ij} \text{ for } 1 \le i \le k, \ 1 \le j \le \ell\}|. \end{aligned} \tag{31}$$

Definition 3 *The* normality measure of order (k, ℓ) *of* η *is defined as*

$$N_{(k,\ell)}(\eta) = \max_{X \in \mathcal{M}(k,\ell)} \max_{\substack{0 < U \le N+1-k \\ 0 < V \le N+1-\ell}} \left| Z(\eta, U, V, X) - \frac{UV}{2^{k\ell}} \right| .$$

(This definition can be generalized to d dimensions easily; then, of course, we have to replace the matrices $X \in \mathcal{M}(k,\ell)$ by mappings $X:\ \{1,2,\dots,k_1\}\times \cdots \times \{1,2,\dots,k_1\} \to \{-1,+1\}$.)

Definition 4 *The normality measure of η is defined as*

$$N(\eta) = \max_{k\ell \le (2\log N)/\log 2} N_{(k,\ell)}(\eta).$$

We will prove the following 2-dimensional analog of Theorem C:

Theorem 3 *For $N,k,\ell \in \mathbb{N}$, $k < N$, $\ell < N$ and every binary lattice $\eta : I_N^2 \to \{-1,+1\}$ we have*

$$N_{(k,\ell)}(\eta) \le \max_{1\le t\le k\ell} Q_t(\eta). \tag{32}$$

Proof. Writing $\mathbb{N}(k,\ell) = \{(i,j):\ 1\le i\le k,\ 1\le j\le \ell\}$ for $X=(x_{ij}) \in \mathcal{M}(k,\ell)$, $0 < U \le N+1-k$ and $0 < V \le N+1-\ell$ we have

$$\begin{aligned}
&\left| Z(\eta,U,V,X) - \frac{UV}{2^{k\ell}} \right| \\
&= \Bigg| \Big| \{(m,n):\ 0\le m<U,\ 0\le n<V, \eta(m-1+i,n-1+j)=x_{ij} \\
&\qquad\qquad \text{for } 1\le i\le k,\ 1\le j\le \ell\} \Big| - \frac{UV}{2^{k\ell}} \Bigg| \\
&= \left| \sum_{0\le m<U} \sum_{0\le n<V} \frac{1}{2^{k\ell}} \prod_{i=1}^{k} \prod_{j=1}^{\ell} x_{ij}(\eta(m-1+i,n-1+j)+x_{ij}) - \frac{UV}{2^{k\ell}} \right| \\
&= \Bigg| \frac{1}{2^{k\ell}} \prod_{i=1}^{k} \prod_{j=1}^{\ell} x_{ij} \sum_{t=1}^{k\ell} \sum_{(i_1,j_1),\dots,(i_t,j_t)\subseteq \mathbb{N}(k,\ell)} \prod_{(i,j)\in \mathbb{N}(k,\ell)\setminus\{(i_1,j_1),\dots,(i_t,j_t)\}} x_{ij} \\
&\qquad\qquad \sum_{0\le m<U} \sum_{0\le n<V} \prod_{r=1}^{t} \eta(m-1+i_r,n-1+j_r) \Bigg|
\end{aligned}$$

whence writing $\mathbf{d_r} = (i_r, j_r)$ and $\mathbf{d'_r} = (i_r - 1, j_r - 1)$ for $r = 1, \ldots, t$ and $B = \{(m,n):\ 0 \le m < U,\ 0 \le n < V\}$ we obtain

$$\begin{aligned}\left|Z(\eta,U,V,X) - \frac{UV}{2^{k\ell}}\right| &\le \frac{1}{2^{k\ell}}\sum_{t=1}^{k\ell}\sum_{\{\mathbf{d_1},\ldots,\mathbf{d_t}\}\subseteq\mathbb{N}(k,\ell)}\left|\sum_{\mathbf{y}\in B}\eta(\mathbf{y}+\mathbf{d'_1})\ldots\eta(\mathbf{y}+\mathbf{d'_t})\right| \\ &\le \frac{1}{2^{k\ell}}\sum_{t=1}^{k\ell}\sum_{\{\mathbf{d_1},\ldots,\mathbf{d_t}\}\subseteq\mathbb{N}(k,\ell)} Q_t(\eta) = \frac{1}{2^{k\ell}}\sum_{t=1}^{k\ell}\binom{k\ell}{t}Q_t(\eta) \\ &\le \max_{t\le k\ell} Q_t(\eta)\end{aligned}$$

which proves (32).

In [28], [30], [31], [40], [53], [54], 2-dimensional binary N-lattices were constructed for which for every fixed t and $N \longrightarrow \infty$ the measure $Q_t(\eta)$ is "small". It follows from Theorem 3 that in all these cases for fixed k, ℓ and $N \longrightarrow \infty$ the normality measure $N_{(k,\ell)}(\eta)$ is also small. In particular, in this way we get that the binary p-lattice constructed in [31] in the 2-dimensional case satisfies

$$N_{(k,\ell)}(\eta) < k\ell p(1 + \log p)^2.$$

In [31] it was also shown that for a truly random n-dimensional binary N-lattice η, $Q_k(\eta)$ is "small" with probability $> 1 - \varepsilon$. More precisely, in the special case when the dimension is $n = 2$ this result gives that for $N > N_0(k, \varepsilon)$ the inequality

$$Q_k(\eta) \le 3(2k)^{1/2} N \log N$$

holds with probability $> 1 - \varepsilon$. By Theorem 3 this implies that if $N > N_1(k, \ell, \varepsilon)$, then for a truly random 2-dimensional binary N-lattice η,

$$N_{(k,\ell)}(\eta) \le 3(k\ell)^{1/2} N \log N$$

holds with probability $> 1 - \varepsilon$.

Note that in [32], [33], [34], [35] and [36] Levin and Smorodinsky also constructed and studied a 2-dimensional binary lattice of "small" normality.

(They are defining "square normality" and "rectangle normality" and they are estimating these measures of the lattice constructed by them.)

Now we will show that if $k \le r$, $\ell \le s$, and r, s are "small" then $N_{k,\ell}$ cannot be much greater than $N_{r,s}$:

Theorem 4 *For every $N, k, \ell, r, s \in \mathbb{N}$, $k \le r \le N$, $\ell \le s \le N$ and every binary lattice $\eta : \ I_N^2 \to \{-1, +1\}$ we have*

$$N_{k,\ell}(\eta) \le 2((r-k) + (s-\ell))N + N_{r,s}(\eta) 2^{rs-k\ell}. \tag{33}$$

Proof If $A = (a_{ij})$ $(1 \le i \le r,\ 1 \le j \le s)$ is an $r \times s$ matrix and $k \le r$, $\ell \le s$, then let $A(k,\ell)$ denote the "truncated" $k \times \ell$ matrix (a_{ij}) with $i \le k,\ j \le \ell$. Moreover, if $\eta : \ I_N^2 \to \{-1, +1\}$, $k, \ell \in \mathbb{N}$, $m + k \le N$ and $n + \ell \le N$, then let $D(k, \ell, m, n, \eta) = (d_{ij})$ denote the $k \times \ell$ matrix defined by

$$d_{ij} = \eta(m + i - 1, n + j - 1) \quad \text{for } 1 \le i \le k,\ 1 \le j \le \ell.$$

Then a pair (m, n) with $0 \le m < U \le N + 1 - r$, $0 \le n < V \le N + 1 - s$ is counted in the definition of $Z(\eta, U, V, X)$ in (31) (with multiplicity 1) if and only if $D(k, \ell, m, n, \eta) = X$. Then writing $D(r, s, m, n, \eta) = Y$ $(\in \mathcal{M}(r, s))$, clearly we have $X = Y(k, \ell)$. Thus for $U \le N + 1 - r$, $V \le N + 1 - s$ we have

$$\begin{aligned} Z(\eta, U, V, X) &= |\{(m, n) :\ 0 \le m < U,\ 0 \le n < V,\ D(k, \ell, m, n, \eta) = X\}| \\ &= \sum_{\substack{Y \in \mathcal{M}(r,s) \\ Y(k,\ell) = X}} |\{(m, n) :\ 0 \le m < U,\ 0 \le n < V, \\ &\qquad\qquad\qquad\qquad\qquad D(k, \ell, m, n, \eta) = Y\}| \\ &= \sum_{\substack{Y \in \mathcal{M}(r,s) \\ Y(k,\ell) = X}} Z(\eta, U, V, Y) = \sum_{\substack{Y \in \mathcal{M}(r,s) \\ Y(k,\ell) = X}} \left(Z(\eta, U, V, Y) - \frac{UV}{2^{k\ell}} \right) \\ &\quad + \frac{UV}{2^{rs}} \sum_{\substack{Y \in \mathcal{M}(r,s) \\ Y(k,\ell) = X}} 1. \end{aligned} \tag{34}$$

If $Y = (y_{ij}) \in \mathcal{M}(r,s)$ and $Y(k,\ell) = X = (x_{ij})$ so that $y_{ij} = x_{ij}$ for $1 \le i \le k$, $1 \le j \le \ell$, then the number of the remaining entries y_{ij} of Y with $k < i \le r$ and/or $\ell < j \le s$ is $rs - k\ell$, and each of them is $\in \{-1,+1\}$ so that it can be chosen in 2 ways, it follows that Y in the last sum can be chosen in $2^{rs-k\ell}$ ways. It follows that in the last term in (34) is

$$\frac{UV}{2^{rs}} 2^{rs-k\ell} = \frac{UV}{2^{k\ell}}.$$

Thus we get from (34) that

$$\left| Z(\eta, U, V, X) - \frac{UV}{2^{k\ell}} \right| \le \sum_{\substack{Y \in \mathcal{M}(r,s) \\ Y(k,\ell)=X}} \left| Z(\eta, U, V, X) - \frac{UV}{2^{rs}} \right| \le N_{(r,s)}(\eta) \sum_{\substack{Y \in \mathcal{M}(r,s) \\ Y(k,\ell)=X}} 1$$
$$= N_{(r,s)}(\eta) 2^{rs-k\ell} \text{ (for } U \le N+1-r,\ V \le N+1-s). \tag{35}$$

Finally, if $N+1-r < U \le N+1-k$ and/or $N+1-s < V \le N+1-\ell$, then using (35) with $U' = \min\{U, N+1-r\}$, $V' = \min\{V, N+1-s\}$ in place of U and V, respectively, we obtain that

$$
\begin{aligned}
\left|Z(\eta,U,V,X)-\frac{UV}{2^{k\ell}}\right| &\le |Z(\eta,U,V,X)-Z(\eta,U',V',X)| \\
&+\left|Z(\eta,U',V',Y)-\frac{U'V'}{2^{k\ell}}\right|+\frac{1}{2^{k\ell}}\left|U'V'-UV\right| \\
&\le \Bigl| |\{(m,n):\ 0\le m<U,\ 0\le n<V,\ D(k,\ell,m,n,\eta)=X\}| \\
&- |\{(m,n):\ 0\le m<U',\ 0\le n<V',\ D(k,\ell,m,n,\eta)=X\}| \Bigr| \\
&+ N_{(r,s)}(\eta)2^{rs-k\ell}+\frac{1}{2^{k\ell}}\left(|U(V-V')|+|V'(U-U')|\right) \\
&\le |\{(m,n):\ U'\le m<U,\ D(k,\ell,m,n,\eta)=X| \\
&+ |\{(m,n):\ V'\le n<V,\ D(k,\ell,m,n,\eta)=X| \\
&+ N_{(r,s)}(\eta)2^{rs-k\ell}+\frac{1}{2^{k\ell}}\left((V-V')N+(U-U')N\right) \\
&\le (U-U')N+(V-V')N+N_{(r,s)}(\eta)2^{rs-k\ell} \\
&+\frac{1}{2^{k\ell}}\left((V-V')N+(U-U')N\right) \\
&\le 2((r-k)+(s-\ell))N+N_{(r,s)}(\eta)2^{rs-k\ell}
\end{aligned}
$$

whence (33) follows and this completes the proof of Theorem 4.

A consequence of Theorem 4 is that if $k \le r,\ \ell \le s$, and k,ℓ,r,s are all $O(1)$, then

$$N_{(k,\ell)}(\eta) = O\left(N_{(r,s)}(\eta)+N\right). \tag{36}$$

Another consequence of the theorem is that for $k,\ell = O(1),\ k \ge \ell$ the estimate of $N_{(k,\ell)}(\eta)$ can be reduced to the estimate of $N_{(k,k)}$. Thus for "small" k,ℓ, it suffices to estimate the normality measures $N_{(k,k)}(\eta)$.

If $k \le r,\ \ell \le s$ each of k,ℓ,r,s is $O(1)$, and $N_{(r,s)}(\eta)$ is "small", then by (36), $N_{k,\ell}(\eta)$ is also small. One may ask the question whether the converse of this statement is also true, i.e., if we have the same assumptions on k,ℓ,r,s and $N_{k,\ell}(\eta)$ is small, then $N_{(r,s)}(\eta)$ is also small?

One may ask another related question: As in [27], to any lattice $\eta: I_N^2 \to \{-1,+1\}$ we may assign the binary sequences $E_N^{(1)}, E_N^{(2)}, \dots, E_N^{(N)}$ formed by the row vectors of the matrix $(\eta(i,j))$ (with $0 \le i,j < N$) so that $E_N^{(i)} = \{e_1^{(i)}, e_2^{(i)}, \dots, e_N^{(i)}\}$ is defined by $e_j^{(i)} = \eta(i-1, j-1)$ for $i = 1,2,\dots,N$, $j = 1,2,\dots,N$. Is it true that if $N_k(E_N^{(i)})$ is "small" for all i for small k, then $N_{k,\ell}(\eta)$ is also small for small k and ℓ? The answer to both questions is negative as the following example shows.

Example 1 *Let the first row $E_N^{(1)} = \{e_1^{(1)}, e_2^{(1)}, \dots, e_N^{(1)}\}$ of the matrix $(\eta(i,j))$ be a binary sequence such that $N_k(E_N^{(1)})$ is small for every small k; e.g., let $N = p-1$ (p prime) and $e_i^{(1)} = \left(\frac{i}{p}\right)$ (Legendre symbol) for $i = 1,2,\dots,N$, and let $E_N^{(j)} = E_N^{(1)}$ for $j = 1,2,\dots,N$. Then it follows from the results in* [47] *that $N_k(E_N^{(i)})$ is small for all i for small k, however $N_{(k,\ell)}(\eta)$ is large for small k and ℓ if $k \ge 2$.*

References

[1] R. Ahlswede, J. Cassaigne and A. Sárközy, *On the correlation of binary sequences*, Applied Discrete Math. 156 (2008), 1478-1487.

[2] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, *Measures of pseudorandomness for finite seqiuences: minimal values*, Combin., Probab. Comput. 15 (2005), 1-29.

[3] 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.

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

[5] Á. Andics, *On the linear complexity of binary sequences*, Annales Univ. Sci. Budapest. Eötvös 48 (2005), 173-180.

[6] I. Berkes, W. Philipp and R. F. Tichy, *Pseudorandom numbers and entropy conditions*, J. Complexity 23 (2007), 516-527.

[7] I. Berkes, W. Philipp and R. F. Tichy, *Entropy conditions for subsequences of random variables with applications to empirical processes*, Monatsh. Math. 153 (2008), 183-204.

[8] N. Brandstätter and A. Winterhof, *Linear complexity profile of binary sequences with small correlation measure*, Periodica Math. Hungar. 52 (2006), 1-8.

[9] J. Cassaigne, S. Ferenczi, C. Mauduit, J. Rivat and A. Sárközy, *On finite pseudorandom binary sequences III, (The Liouville function, I)*, Acta Arith. 87 (1999), 367-390.

[10] J. Cassaigne, S. Ferenczi, C. Mauduit, J. Rivat and A. Sárközy, *On finite pseudorandom binary sequences IV: The Liouville function, II*, Acta Arith. 95 (2000), 343-359.

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

[12] Z.-X. Chen, *Elliptic curve analogue of Legendre sequences*, Monatsh. Math. 154 (2008), 1-10.

[13] Z. X. Chen, X. N. Du and G. Z. Xiao, *Sequences related to Legendre/Jacobi sequences*, Inform. Sci. 177 (2007), 4820-4831.

[14] Z. Chen and S. Li, *Some notes on generalized cyclomatic sequences of length pq*, J. Comput. Sci. Technology 23 (2008), 843-850.

[15] Z. Chen, S. Li and G. Xiao, *Construction of pseudorandom binary sequences from elliptic curves by using the discrete logarithms*, in: Se-

quences and their applications - SETA 2006, LNCS 4086, Springer, 2006; pp. 285-294.

[16] H. Daboussi, *On pseudorandom properties of multiplicative functions*, Acta Math. Hungar. 98 (2003), 273-300.

[17] H. Daboussi, *On the correlation of the truncated Liouville function*, Acta Arith. 108 (2003), 61-76.

[18] J. Folláth, *Construction of pseudorandom binary sequences using additive characters over $GF(2^k)$*, Periodica Math. Hungar. 57 (2008), 73-81.

[19] E. Fouvry, P. Michel, J. Rivat and A. Sárközy, *On the pseudorandomness of the signs of Kloosterman sums*, J. Australian Math. Soc. 77 (2004), 425-436.

[20] L. Goubin, C. Mauduit and A. Sárközy, *Construction of large families of pseudorandom binary sequences*, J. Number Theory 106 (2004), 56-69.

[21] E. Grant, J. Shallit and T. Stoll, *Bounds for the discrete correlation of infinite sequences on k symbols and generalized Rudin-Shapiro sequences*, Acta Arith., to appear.

[22] K. Gyarmati, *An inequality between the measures of pseudorandomness*, Annales Univ. Sci. Budapest. Eötvös 46 (2003), 157-166.

[23] K. Gyarmati, *On a family of pseudorandom binary sequences*, Periodica Math. Hungar. 49 (2004), 45-63.

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

[25] K. Gyarmati, *On the correlation of binary sequences*, Studia Sci. Math. Hungar. 42 (2005), 79-93.

[26] K. Gyarmati, *On a fast version of a pseudorandom generator*, in: General Theory of Information Transfer and Combinatorics, LNCS 4123, Springer, 2006, 326-342.

[27] K. Gyarmati, C. Mauduit and A. Sárközy, *Pseudorandom binary sequences and lattices*, Acta Arith. 135 (2008), 181-197.

[28] K. Gyarmati, C. Mauduit and A. Sárközy, *Construction of pseudorandom binary lattices*, Unif. Distr. Theory, submitted.

[29] K. Gyarmati, A. Pethő and A. Sárközy, *On linear recursion and pseudorandomness*, Acta Arith. 118 (2005), 359-374.

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

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

[32] M. B. Levin, *On normal lattice configurations and simultaneously normal numbers*, J. Théor. Nombres Bordeaux 13 (2001), 483-527.

[33] M. B. Levin and M. Smorodinsky, *A $\mathbb{Z}^d$ generalisation of the Davenport-Erdős construction of normal numbers*, Colloq. Math. 84/85 (2000), 431-441.

[34] M. B. Levin and M. Smorodinsky, *Explicit construction of normal lattice configurations*, Colloq. Math. 102 (2005), 33-47.

[35] M. B. Levin and M. Smorodinsky, *On linear normal lattice configurations*, J. Théor. Nombres Bordeaux 17 (2005), 825-858.

[36] M. B. Levin and M. Smorodinsky, *On polynomially normal lattice configurations*, Monaths. Math. 147 (2006), 137-153.

[37] H. Liu, *New pseudorandom sequences constructed using multiplicative inverses*, Acta Arith. 125 (2006), 11-19.

[38] H. N. Liu, *A family of pseudorandom binary sequences constructed by the multiplicative inverse*, Acta Arith. 130 (2007), 167-180.

[39] H. Liu, *New pseudorandom sequences constructed by quadratic residues and Lehmer numbers*, Proc. Amer. Math. Soc. 135 (2007), 1309-1318.

[40] H. Liu, *A large family of pseudorandom binary lattices*, Proc. Amer. Math. Soc. 137 (2009), 793-803.

[41] H. N. Liu and W. G. Zhai, *A note on the pseudorandomness of the Liouville function*, Acta Arith. 136 (2009), 101-121.

[42] H. N. Liu, T. Zhan and X. Y. Wang, *On the correlation of pseudorandom binary sequences with composite moduli*, Publ. Math. Debrecen 74 (2009), 195-214.

[43] S. Louboutin, J. Rivat and A. Sárközy, *On a problem of D. H. Lehmer*, Proc. Amer. Math. Soc. 135 (2007), 969-975.

[44] C. Mauduit, H. Niederreiter and A. Sárközy, *On pseudorandom* $[0,1)$ *and binary sequences*, Publ. Math. Debrecen 71 (2007), 305-327.

[45] C. Mauduit, J. Rivat and A. Sárközy, *On the pseudo-random properties of* n^c, Illinois J. Math. 46 (2002), 185-197.

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

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

[48] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences, II. (The Champernowne, Rudin-Shapiro and Thue-Morse sequences. A further construction.)*, J. Number Theory 73 (1998), 256-276.

[49] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences, V. On* $(n\alpha)$ *and* $(n^2\alpha)$ *sequences*, Monatsh. Math. 129 (2000), 197-216.

[50] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences, VI. On* $(n^k\alpha)$ *sequences*, Monatsh. Math. 130 (2000), 281-298.

[51] C. Mauduit and A. Sárközy, *On the measures of pseudorandomness of binary sequences*, Discrete Math. 271 (2003), 195-207.

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

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

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

[55] L. Mérai, *Construction of large families of pseudorandom binary sequences*, Ramanujan J. 18 (2009), 341-349.

[56] L. Mérai, *Construction of pseudorandom binary lattices based on multiplicative characters*, Periodica Math. Hungar., to appear.

[57] L. Mérai, *A construction of pseudorandom binary sequences using rational functions*, Unif. Distrib. Theory 4 (2009), 35-49.

[58] L. Mérai, *A construction of pseudorandom binary sequences using both additive and multiplicative characters*, Acta Arith., submitted.

[59] V. N. Muralidhara and S. Sen, *A result on the distribution of quadratic residues with applications to elliptic curve cryptography*, in: Progress in Cryptology - INDOCRYPT 2007, LNCS 4859, Springer, 2007, pp. 48-57.

[60] S.-M. Oon, *Pseudorandom properties of prime factors*, Periodica Math. Hungar. 49 (2004), 107-118.

[61] S.-M. Oon, *On pseudo-random properties of some Dirichlet characters*, Ramanujan J. 15 (2008), 19-30.

[62] W. Philipp and R. Tichy, *Metric theorems for distribution measures of pseudorandom sequences*, Monatsh. Math. 135 (2002), 321-326.

[63] J. Rivat, *On pseudo-random properties of $P(n)$ and $P(n+1)$*, Periodica Math. Hungar. 43 (2001), 121-136.

[64] J. Rivat and A. Sárközy, *Modular constructions of pseudorandom binary sequences with composite moduli*, Periodica Math. Hungar. 51 (2005), 75-107.

[65] J. Rivat and A. Sárközy, *On pseudo-random binary sequences and their applications*, in: General Theory of Information Transfer and Combinatorics, LNCS 4123, Springer, 2006, pp. 343-361.

[66] A. Sárközy, *A finite pseudorandom binary sequence*, Studia Sci. Math. Hungar. 38 (2001), 377-384.

[67] A. Sárközy, *On finite pseudorandom binary sequences and their applications in cryptography*, Tatra Mt. Math. Publ. 37 (2007), 123-136.

[68] A. Sárközy and C. L. Stewart, *On pseudorandomness in families of sequences derived from the Legendre symbol*, Periodica Math. Hungar. 54 (2007), 163-173.

[69] A. Sárközy and A. Winterhof, *Measures of pseudorandomness for binary sequences constructed using finite fields*, Discrete Math. 309 (2009), 1327-1333.

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

[71] A. Winterhof, *Some estimates for character sums and applications*, Des. Codes Cryptogr. 22 (2001), 123–131.