ACTA ARITHMETICA
144.3 (2010)

# Measures of pseudorandomness of finite binary lattices, I. The measures $Q_k$, normality

by

Katalin Gyarmati (Budapest), Christian Mauduit (Marseille)
and András Sárközy (Budapest)

**1. Introduction.** Recently in a series of papers a new constructive approach has been developed to study pseudorandomness 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

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

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

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

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

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

where the maximum is taken over all $a, b, t$ and $\mathbf{D} = (d_1, \dots, d_k)$ such that all the subscripts $a+jb+d_l$ belong to $\{1, \dots, N\}$. 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

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

 

$o(N)$ as $N \to \infty$). 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]–[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]–[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 $N-1$:

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

This set is called an *$n$-dimensional $N$-lattice* or briefly an *$N$-lattice*. In [30] this definition was extended to more general lattices in the following way: Let $\mathbf{u}_1, \dots, \mathbf{u}_n$ 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 $t_1, \dots, t_n$ be integers with $0 \le t_1, \dots, t_n < N$. Then we call the set

$$B_N^n = \{\mathbf{x} = x_1\mathbf{u}_1 + \dots + x_n\mathbf{u}_n : 0 \le x_i|\mathbf{u}_i| \le t_i \ (< N) \text{ for } i = 1, \dots, n\}$$

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

In [31] the definition of binary sequences was extended to more dimensions by considering functions of the type

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

If $\mathbf{x} = (x_1, \dots, x_n)$ so that $\eta(\mathbf{x}) = \eta((x_1, \dots, x_n))$ we will simply write $\eta(\mathbf{x}) = \eta(x_1, \dots, x_n)$. 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 present the definition in a slightly modified but equivalent form as in [30]): Let $\eta : I_N^n \to \{-1, +1\}$. Define the pseudorandom measure of order $l$ of $\eta$ by

$$Q_l(\eta) = \max_{B,\mathbf{d}_1,\ldots,\mathbf{d}_l} \Big| \sum_{\mathbf{x}\in B} \eta(\mathbf{x}+\mathbf{d}_1)\cdots\eta(\mathbf{x}+\mathbf{d}_l) \Big|, \tag{5}$$

where the maximum is taken over all distinct $\mathbf{d}_1,\ldots,\mathbf{d}_l \in I_N^n$ and all box $N$-lattices $B$ such that $B+\mathbf{d}_1,\ldots,B+\mathbf{d}_l \subseteq I_N^n$. 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 $\eta$ 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 $Q_l(\eta)$ 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 $Q_l(\eta)$ is "small", or 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 pseudorandomness and the connection between them [1]–[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 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 study the connection between the measures $Q_k$ and $Q_l$ for $k\neq l$, 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 $C_l(E_N)$ for $k\neq l$ (…)." Indeed, we proved in [11]:

THEOREM A. *For $k,l,N\in\mathbb{N}$, $k\,|\,l$, $E_N\in\{-1,+1\}^N$ we have*

$$C_k(E_N) \le N\biggl(\frac{(l!)^{k/l}}{k!}\biggl(\frac{C_l(E_N)}{N}\biggr)^{k/l} + \biggl(\frac{l^2}{N}\biggr)^{k/l}\biggr).$$

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

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

$$C_l(E_N) > \frac{N-l}{k} - 54k^2 N^{1/2} \log N \quad \text{if } k \mid l$$

*and*

$$C_l(E_N) < 27k^2 l N^{1/2} \log N \quad \text{if } k \nmid l.$$

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

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

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

$$Q_k(E_N) \le N^2 \left( \left(\frac{l}{N}\right)^{2k/l} + \frac{4(l!)^{k/l}}{k!} \left(\frac{Q_l(\eta)}{N^2}\right)^{k/l} \right).$$

It follows that if $k \mid l$, $N \to \infty$ and $Q_l(\eta) = o(N^2)$, 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

$$\left| \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d}_1) \dots \eta(\mathbf{x} + \mathbf{d}_k) \right| \le N^2 \left( \left(\frac{l}{N}\right)^{2k/l} + \frac{4(l!)^{k/l}}{k!} \left(\frac{Q_l(\eta)}{N^2}\right)^{k/l} \right). \tag{6}$$

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

$$\begin{aligned} &\Big( \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d}_1) \dots \eta(\mathbf{x} + \mathbf{d}_k) \Big)^t \\ &= \Big( \sum_{\mathbf{x}_1 \in B} \eta(\mathbf{x}_1 + \mathbf{d}_1) \dots \eta(\mathbf{x}_1 + \mathbf{d}_k) \Big) \dots \Big( \sum_{\mathbf{x}_t \in B} \eta(\mathbf{x}_t + \mathbf{d}_1) \dots \eta(\mathbf{x}_t + \mathbf{d}_k) \Big) \\ &= \sum_{\mathbf{x}_1 \in B} \cdots \sum_{\mathbf{x}_t \in B} \eta(\mathbf{x}_1 + \mathbf{d}_1) \dots \eta(\mathbf{x}_1 + \mathbf{d}_k) \dots \eta(\mathbf{x}_t + \mathbf{d}_1) \dots \eta(\mathbf{x}_t + \mathbf{d}_k) \\ &= S_1 + S_2, \end{aligned} \tag{7}$$

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 $(i, u) \ne (j, v)$), 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 each, $i, j$ in $t$ ways each, $\mathbf{x}_j$ (for fixed $j$) in $|B|$ (= number of lattice points in $B$) $\le N^2$ 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 $k^2t^2N^2(N^2)^{t-2} = l^2N^{2(t-1)}$ terms and thus

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

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 $\mathbf{d}_1 < \cdots < \mathbf{d}_k$ in terms of this ordering. Consider each of the terms $\eta(\mathbf{x}_1 + \mathbf{d}_1) \ldots \eta(\mathbf{x}_t + \mathbf{d}_k)$ in $S_2$, and rearrange the factors $\eta(\mathbf{x}_i + \mathbf{d}_u)$ so that the vectors are increasing:

$$\eta(\mathbf{x}_1 + \mathbf{d}_1) \ldots \eta(\mathbf{x}_t + \mathbf{d}_k) = \eta(\mathbf{w}_1) \ldots \eta(\mathbf{w}_l), \qquad \mathbf{w}_1 < \cdots < \mathbf{w}_l.$$

We $t$-colour these factors $\eta(\mathbf{w}_1), \ldots, \eta(\mathbf{w}_l)$: if the vector $\mathbf{w}_u$ is of the form $\mathbf{w}_u = \mathbf{x}_j + \mathbf{d}_v$, then we give $\eta(\mathbf{w}_u)$ the $j$th colour. Then to each term $\eta(\mathbf{w}_1) \ldots \eta(\mathbf{w}_l)$ we may assign the sequence of the colours following each other in the order used to colour $\eta(\mathbf{w}_1), \ldots, \eta(\mathbf{w}_l)$. 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 $l!/(k!)^t$.

Now let us fix any of the colour patterns, and consider each of the terms $\eta(\mathbf{w}_1) \ldots \eta(\mathbf{w}_l)$ with this fixed colour pattern. We define an equivalence relation among these terms by

$$\eta(\mathbf{w}_1) \ldots \eta(\mathbf{w}_l) \sim \eta(\mathbf{v}_1) \ldots \eta(\mathbf{v}_l) \quad \text{if } \mathbf{v}_1 - \mathbf{w}_1 = \cdots = \mathbf{v}_l - \mathbf{w}_l.$$

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

$$\eta(\mathbf{a}_1) \ldots \eta(\mathbf{a}_l) \tag{10}$$

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

$$\eta(\mathbf{a}_1) < \cdots < \eta(\mathbf{a}_l), \tag{11}$$

and every term belonging to the class is of the form

$$\eta(\mathbf{a}_1 + \mathbf{x}) \ldots \eta(\mathbf{a}_l + \mathbf{x}), \tag{12}$$

or equivalently,

$$\eta(\mathbf{y})\eta(\mathbf{y} + (\mathbf{a}_2 - \mathbf{a}_1)) \ldots \eta(\mathbf{y} + (\mathbf{a}_l - \mathbf{a}_1)). \tag{13}$$

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

$$\eta(\mathbf{a}_1 + \mathbf{x}) < \cdots < \eta(\mathbf{a}_l + \mathbf{x}),$$

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 $j = 1, \dots, t$, 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

$$\mathbf{a}_{i_j} = \mathbf{z}_j + \mathbf{d}_1 \quad \text{with some } \mathbf{z}_j \in B \qquad (\text{for } j = 1, \dots, t);$$

in particular,

$$\mathbf{a}_1 = \mathbf{a}_{i_r} = \mathbf{z}_r + \mathbf{d}_1 \qquad \text{for some } r \in \{1, \dots, t\}.$$

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 $\eta(\mathbf{a}_{i_j})$, we see that $\mathbf{y} + (\mathbf{z}_j - \mathbf{z}_r)$ must be of the form

$$\mathbf{y} + (\mathbf{z}_j - \mathbf{z}_r) = \mathbf{x}_j + \mathbf{d}_1 \qquad \text{with the } x_j \in B \text{ in (7)},$$

whence

$$\mathbf{y} = \mathbf{x}_j + \mathbf{d}_1 + \mathbf{z}_r - \mathbf{z}_j \in B + \mathbf{d}_1 + \mathbf{z}_r - \mathbf{z}_j \qquad \text{for } j = 1, \dots, t;$$

in particular, for $j = r$ we have

$$\mathbf{y} \in B + \mathbf{d}_1.$$

It follows that we must have

$$y \in (B + \mathbf{d}_1) \cap \bigcap_{\substack{1 \le j \le t \\ j \ne r}} (B + \mathbf{d}_r + \mathbf{z}_r - \mathbf{z}_j). \tag{14}$$

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

$$\sum_{\mathbf{y} \in B' + \mathbf{d}'} \eta(\mathbf{y})\eta(\mathbf{y} + (\mathbf{a}_2 - \mathbf{a}_1)) \dots \eta(\mathbf{y} + (\mathbf{a}_l - \mathbf{a}_1))$$
$$= \sum_{\mathbf{x} \in B'} \eta(\mathbf{x} + \mathbf{d}')\eta(\mathbf{x} + \mathbf{d}' + \mathbf{a}_2 - \mathbf{a}_1) \dots \eta(\mathbf{x} + \mathbf{d}' + \mathbf{a}_l - \mathbf{a}_1).$$

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

$$\left| \sum_{\mathbf{y} \in B + \mathbf{d}'} \eta(\mathbf{y})\eta(\mathbf{y} + (\mathbf{a}_2 - \mathbf{a}_1)) \dots \eta(\mathbf{y} + (\mathbf{a}_l - \mathbf{a}_1)) \right| \le Q_l(\eta).$$

It remains to estimate the number of equivalence classes. An equivalence class is uniquely determined by the colour pattern, which can be chosen in

$l!/(k!)^t$ 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

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

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

$$\begin{aligned}
\Big|\sum_{\mathbf{x}\in B} \eta(\mathbf{x}+\mathbf{d}_1)\ldots\eta(\mathbf{x}+\mathbf{d}_k)\Big| &= (S_1+S_2)^{1/t} \leq |S_1|^{1/t} + |S_2|^{1/t} \\
&\leq l^{2/t}N^2N^{-2/t} + \frac{(l!)^{1/t}}{k!}2^2N^2N^{-2/t}Q_l(\eta)^{1/t} \\
&= N^2\bigg(\Big(\frac{l}{N}\Big)^{2k/l} + \frac{4(l!)^{k/l}}{k!}\Big(\frac{Q_l(\eta)}{N}\Big)^{k/l}\bigg),
\end{aligned}$$

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

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

Theorem 2. *If $k, N \in \mathbb{N}$ and $k \leq N$, then there is a binary $N$-lattice $\eta$ such that if $l \in \mathbb{N}$, $l \leq N/2$, then*

$$Q_l(\eta) \geq \frac{N(N-l)}{k} \quad \text{if } k \mid l \tag{16}$$

*and*

$$Q_l(\eta) \ll k^2 l N (\log N)^2 \quad \text{if } k \nmid l. \tag{17}$$

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

$$N < p \leq 2N$$

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

Write $q = p^2$, and denote by $\gamma$ the quadratic character of $\mathbb{F}_q$. Let $\mathbf{v}_1, \mathbf{v}_2$ be a basis of the vector space $\mathbb{F}_q$ 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 $0 \leq x_1, x_2 \leq p-2$, we see that $\eta$ is always $+1$ or $-1$. First we prove (16). Define the 2-dimensional box $N$-lattice $B$ by

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

Define the vectors $\mathbf{d}_1, \dots, \mathbf{d}_l$ by

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

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

$$\begin{aligned} Q_l(\eta) &\geq \sum_{\mathbf{x}\in B} \eta(\mathbf{x}+\mathbf{d}_1)\dots\eta(\mathbf{x}+\mathbf{d}_l) \\ &= \sum_{x_2=0}^{N-1} \sum_{\substack{0\leq x_1<N-l \\ x_1\equiv 0 \,(\mathrm{mod}\, k)}} \eta(x_1,x_2)\eta(x_1+1,x_2)\dots\eta(x_1+l-1,x_2). \end{aligned}$$

Since now $k \mid l$, we have

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

By the definition of $\eta$, 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

$$Q_l(\eta) \geq \sum_{x_2=0}^{N-1} \sum_{\substack{0\leq x_1<N-l \\ x_1\equiv 0 \,(\mathrm{mod}\, k)}} 1 \geq \frac{N(N-l)}{k}.$$

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 $\mathbf{d}_1, \dots, \mathbf{d}_l \in I_N^2$ be distinct vectors such that $B+\mathbf{d}_1, \dots, B+\mathbf{d}_l \subseteq I_N^2$. Let

$$S = \sum_{\mathbf{x}\in B_1} \eta(\mathbf{x}+\mathbf{d}_1)\dots\eta(\mathbf{x}+\mathbf{d}_l).$$

We will prove that

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

from which (17) follows. Write

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

Then

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

Define

$$S(r)=\sum_{\substack{0\le x_1\le t_1/z_1\\ x_1\equiv r\ (\mathrm{mod}\ k)}}\sum_{x_2=0}^{t_2/z_2}\prod_{i=1}^{l}\eta(x_1z_1+d_1^{(i)},x_2z_2+d_2^{(i)}). \tag{19}$$

Then

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

Next we will prove that

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

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

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

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 also $rz_1+d_1^{(i)}\equiv k-1\ (\mathrm{mod}\ k)$, 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 $\eta$ we have

$$\begin{aligned} &\eta((y_1kz_1,x_2z_2)+(rz_1+d_1^{(i)},d_2^{(i)})) \\ &\qquad=\gamma(y_1kz_1\mathbf{v}_1+x_2z_2\mathbf{v}_2+(rz_1+d_1^{(i)}+1)\mathbf{v}_1+(d_2^{(i)}+1)\mathbf{v}_2) \end{aligned}$$

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

$$\begin{aligned} &\eta((y_1kz_1,x_2z_2)+(rz_1+d_1^{(i)},d_2^{(i)})) \\ &\quad=\prod_{j=1}^{k-1}\gamma(y_1kz_1\mathbf{v}_1+x_2z_2\mathbf{v}_2+(rz_1+d_1^{(i)}+1-j)\mathbf{v}_1+(d_2^{(i)}+1)\mathbf{v}_2) \end{aligned}$$

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

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

$$\mathcal{A} = \{(rz_1 + d_1^{(i)} + 1)\mathbf{v}_1 + (d_2^{(i)} + 1)\mathbf{v}_2 : 1 \le i \le l,$$
$$rz_1 + d_1^{(i)} \not\equiv k-1 \pmod{k}\},$$
$$\mathcal{B} = \{(rz_1 + d_1^{(i)} + 1 - j)\mathbf{v}_1 + (d_2^{(i)} + 1)\mathbf{v}_2 : 1 \le i \le l,\ 1 \le j \le k-1,$$
$$rz_1 + d_1^{(i)} \equiv k-1 \pmod{k}\}.$$

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

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

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),

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

Using the multiplicativity of the quadratic character $\gamma$, we have

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

Now we will use the following lemma:

Lemma 1. *Let $p$ be an odd prime, $n \in \mathbb{N}$, $q = p^n$ and $v_1, \dots, v_n$ be a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. Let $\chi$ be a multiplicative character of $\mathbb{F}_q$ of order $d > 1$ and let $f(x) \in \mathbb{F}_q[x]$ 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 $k_1, \dots, k_n$ are positive integers with $k_1 \le p, \dots, k_n \le p$. Then writing $B = \{\sum_{i=1}^n j_i v_i : 0 \le j_i < k_i\}$, we have*

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

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

Let $f(\mathbf{x}) = \prod_{\alpha\in\mathcal{A}\cup\mathcal{B}}(\mathbf{x}+\alpha)$. 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 $\mathbb{F}_q$ 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 $f(x) = \prod_{\alpha\in\mathcal{A}\cup\mathcal{B}}(x+\alpha) \in \mathbf{F}_q[x]$ 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

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

so that (21) holds. Since $\mathbf{d}_1, \dots, \mathbf{d}_l$ are distinct, 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 $(i_1, j_1) \ne (i_2, j_2)$, $1 \le i_1, i_2 \le l$ 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

$$rz_1 + d_1^{(i_1)} + 1 - j_1 \equiv rz_1 + d_1^{(i_2)} + 1 - j_2 \pmod p,$$
$$d_2^{(i_1)} \equiv d_2^{(i_2)} \pmod p.$$

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

$$rz_1 + d_1^{(i_1)} + 1 - j_1 = rz_1 + d_1^{(i_2)} + 1 - j_2, \tag{26}$$

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

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

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

From 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 (28) yields $(i_1, j_1) = (i_2, j_2)$, which is a contradiction.

Since $\mathcal{A}$ and $\mathcal{B}$ contain different elements, $\prod_{\alpha \in \mathcal{A} \cup \mathcal{B}} (x + \alpha)$ 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),

$$l = n + m = km.$$

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

By (20) and (21),

$$S \ll k^2 l N (\log N)^2,$$

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

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

Definition 3. The *normality measure of order* $(k,l)$ of $\eta$ is defined as

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

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

Definition 4. The *normality measure* of $\eta$ is defined as

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

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

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

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

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

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

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

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

which proves (32).

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

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

In [31] it was also shown that for a truly random $n$-dimensional binary $N$-lattice $\eta$, $Q_k(\eta)$ 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 $N > N_1(k,l,\varepsilon)$, then for a truly random 2-dimensional binary $N$-lattice $\eta$,

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

holds with probability $> 1-\varepsilon$.

Note that in [32]–[36] Levin and Smorodinsky also constructed and studied a 2-dimensional binary lattice of "small" normality. (They define "square normality" and "rectangle normality" and they estimate these measures of the lattice constructed by them.)

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

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

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

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

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

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 $D(k,l,m,n,\eta)=X$. Then writing $D(r,s,m,n,\eta)=Y$ $(\in \mathcal{M}(r,s))$, we clearly have $X=Y(k,l)$. Thus for $U \le N+1-r$, $V \le N+1-s$ we get

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

If $Y=(y_{ij}) \in \mathcal{M}(r,s)$ and $Y(k,l)=X=(x_{ij})$ so that $y_{ij}=x_{ij}$ for $1 \le i \le k$, $1 \le j \le l$, then the number of the remaining entries $y_{ij}$ of $Y$ with

$k < i \le r$ and/or $l < j \le s$ is $rs - kl$, and each of them is in $\{-1, +1\}$ so that it can be chosen in two ways. It follows that $Y$ in the last sum can be chosen in $2^{rs-kl}$ ways. Hence the last term in (34) is

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

Thus from (34) we get

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

Finally, if $N + 1 - r < U \le N + 1 - k$ and/or $N + 1 - s < V \le N + 1 - l$, 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

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

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

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

$$(36)\qquad N_{(k,l)}(\eta) = O(N_{(r,s)}(\eta) + N).$$

Another consequence is that for $k, l = O(1)$, $k \geq l$ the estimate of $N_{(k,l)}(\eta)$ 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 $k \leq r$, $l \leq s$, each of $k, l, r, s$ is $O(1)$, and $N_{(r,s)}(\eta)$ is "small", then by (36), $N_{k,l}(\eta)$ is also small. One may ask whether the converse is also true: under the same assumptions on $k, l, r, s$, if $N_{k,l}(\eta)$ is small, is then $N_{(r,s)}(\eta)$ 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 $E_N^{(1)}, \dots, E_N^{(N)}$ formed by the row vectors of the matrix $(\eta(i,j))$ (with $0 \leq i, j < N$) so that $E_N^{(i)} = \{e_1^{(i)}, \dots, e_N^{(i)}\}$ is defined by $e_j^{(i)} = \eta(i-1, j-1)$ for $i, j = 1, \dots, N$. Is it true that if $N_k(E_N^{(i)})$ is "small" for all $i$ for small $k$, then $N_{k,l}(\eta)$ 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 $E_N^{(1)} = \{e_1^{(1)}, \dots, e_N^{(1)}\}$ 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 $i = 1, \dots, N$, and let $E_N^{(j)} = E_N^{(1)}$ for $j = 1, \dots, N$. Then it follows from [47] that $N_k(E_N^{(i)})$ is small for all $i$ for small $k$, but $N_{(k,l)}(\eta)$ is large for small $k$ and $l$ if $k \geq 2$.

**Acknowledgments.** 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.

## References

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

[2] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, *Measures of pseudorandomness for finite sequences: minimal values*, Combin. Probab. Comput. 15 (2006), 1–29.

[3] —, —, —, —, —, *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*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 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*, Period. Math. Hungar. 52 (2006), no. 2, 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] —, —, —, —, —, *On finite pseudorandom binary sequences. IV. The Liouville function, II*, ibid. 95 (2000), 343–359.

[11] J. Cassaigne, C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences. VII. The measures of pseudorandomness*, ibid. 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. X. Chen and S. Q. Li, *Some notes on generalized cyclotomic sequences of length pq*, J. Comput. Sci. Tech. 23 (2008), 843–850.

[15] Z. X. Chen, S. Q. Li and G. Z. Xiao, *Construction of pseudo-random binary sequences from elliptic curves by using discrete logarithm*, in: Sequences and Their Applications—SETA 2006, Lecture Notes in Comput. Sci. 4086, Springer, 2006, 285–294.

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

[17] —, —, *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($2^k$), Period. Math. Hungar. 57 (2008), 73–81.

[19] É. Fouvry, P. Michel, J. Rivat and A. Sárközy, *On the pseudorandomness of the signs of Kloosterman sums*, J. Austral. 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. 140 (2009), 345–368.

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

[23] —, *On a family of pseudorandom binary sequences*, Period. Math. Hungar. 49 (2004), no. 2, 45–63.

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

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

[26] —, *On a fast version of a pseudorandom generator*, in: General Theory of Information Transfer and Combinatorics, Lecture Notes in Comput. Sci. 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] —, —, —, *Constructions of pseudorandom binary lattices*, Unif. Distrib. Theory 4 (2009), no. 2, 59–80.

[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* $\mathbb{Z}^d$ *generalization of the Davenport–Erdős construction of normal numbers*, Colloq. Math. 84/85 (2000), 431–441.
[34] —, —, *Explicit construction of normal lattice configurations*, ibid. 102 (2005), 33–47.
[35] —, —, *On linear normal lattice configurations*, J. Théor. Nombres Bordeaux 17 (2005), 825–858.
[36] —, —, *On polynomially normal lattice configurations*, Monatsh. Math. 147 (2006), 137–153.
[37] H. N. Liu, *New pseudorandom sequences constructed using multiplicative inverses*, Acta Arith. 125 (2006), 11–19.
[38] —, *A family of pseudorandom binary sequences constructed by the multiplicative inverse*, ibid. 130 (2007), 167–180.
[39] —, *New pseudorandom sequences constructed by quadratic residues and Lehmer numbers*, Proc. Amer. Math. Soc. 135 (2007), 1309–1318.
[40] —, *A large family of pseudorandom binary lattices*, ibid. 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), 305–324.
[45] C. Mauduit, J. Rivat and A. Sárközy, *On the pseudo-random properties of* $n^c$, Illinois J. Math. 46 (2002), 185–197.
[46] —, —, —, *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] —, —, *On finite pseudorandom binary sequences. II. The Champernowne, Rudin–Shapiro, and Thue–Morse sequences, further construction*, J. Number Theory 73 (1998), 256–276.
[49] —, —, *On finite pseudorandom binary sequences. V. On* $(n\alpha)$ *and* $(n^2\alpha)$ *sequences*, Monatsh. Math. 129 (2000), 197–216.
[50] —, —, *On finite pseudorandom binary sequences. VI. On* $(n^k\alpha)$ *sequences*, ibid. 130 (2000), 281–298.
[51] —, —, *On the measures of pseudorandomness of binary sequences*, Discrete Math. 271 (2003), 195–207.
[52] —, —, *Construction of pseudorandom binary sequences by using the multiplicative inverse*, Acta Math. Hungar. 108 (2005), 239–252.
[53] —, —, *On large families of pseudorandom binary lattices*, Unif. Distrib. 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] —, *Construction of pseudorandom binary lattices based on multiplicative characters*, Period. Math. Hungar. 59 (2009), 43–51.
[57] —, *A construction of pseudorandom binary sequences using rational functions*, Unif. Distrib. Theory 4 (2009), 35–49.
[58] —, *A construction of pseudorandom binary sequences using both additive and multiplicative characters*, Acta Arith. 139 (2009), 241–252.
[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, Lecture Notes in Comput. Sci. 4859, Springer, 2007, 48–57.
[60] S.-M. Oon, *Pseudorandom properties of prime factors*, Period. Math. Hungar. 49 (2004), no. 2, 107–118.
[61] —, *On pseudorandom 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 $P(n+1)$*, Period. Math. Hungar. 43 (2001), 121–136.
[64] J. Rivat and A. Sárközy, *Modular constructions of pseudorandom binary sequences with composite moduli*, ibid. 51 (2005), no. 2, 75–107.
[65] —, —, *On pseudorandom binary sequences and their application*, in: General Theory of Information Transfer and Combinatorics, Lecture Notes in Comput. Sci. 4123, Springer, 2006, 343–361.
[66] A. Sárközy, *A finite pseudorandom binary sequence*, Studia Sci. Math. Hungar. 38 (2001), 377–384.
[67] —, *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*, Period. 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 déduisent*, Actualités Sci. Ind. 1041, Hermann, Paris, 1948.
[71] A. Winterhof, *Some estimates for character sums and applications*, Des. Codes Cryptogr. 22 (2001), 123–131.

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

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

*Received on 11.11.2009* (6213)