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

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

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

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

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

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

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

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

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

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 \( N - 1 \):
\[
I_n^N = \{ x = (x_1, \ldots, x_n) : x_i \in \{0, 1, \ldots, N - 1\} \}.
\]

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 \( u_1, \ldots, u_n \) be \( n \) linearly independent vectors over the field of the real numbers such that the \( i \)th coordinate of \( u_i \) is a positive integer and the other coordinates of \( u_i \) are 0, so that \( u_i \) is of the form \((0, \ldots, 0, z_i, 0, \ldots, 0)\) (with \( z_i \in \mathbb{Z}^+ \)). Let \( t_1, \ldots, t_n \) be integers with \( 0 \leq t_1, \ldots, t_n < N \). Then we call the set
\[
B_n^N = \{ x = x_1u_1 + \cdots + x_nu_n : 0 \leq x_i|u_i| \leq t_i \ (\ < N) \ \text{for} \ i = 1, \ldots, n \}
\]
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 \( x = (x_1, \ldots, x_n) \) so that \( \eta(x) = \eta((x_1, \ldots, x_n)) \) we will simply write \( \eta(x) = \eta(x_1, \ldots, x_n) \). 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
Measures of pseudorandomness of lattices, I

\[ Q_l(\eta) = \max_{B,d_1,\ldots,d_l} \left| \sum_{x \in B} \eta(x + d_1) \cdots \eta(x + d_l) \right|, \]

where the maximum is taken over all distinct \(d_1,\ldots,d_l \in I^n_N\) and all box \(N\)-lattices \(B\) such that \(B + d_1, \ldots, B + d_l \subseteq I^n_N\). Note that in the one-dimensional special case, \(Q_1(\eta)\) is the same as the well-distribution measure \(\mathcal{D}\), and for every \(k \in \mathbb{N}\), \(Q_k(\eta)\) is the combined measure \(\mathcal{D}\).

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 \(k,l,N \in \mathbb{N}, k \mid l, E_N \in \{-1, +1\}^N\) we have

\[ C_k(E_N) \leq N \left( \frac{(l!)^{k/l}}{k!} \left( \frac{C_l(E_N)}{N} \right)^{k/l} + \left( \frac{2}{N} \right)^{k/l} \right). \]

It follows that if \(k,l \in \mathbb{N}, k \mid l, N \to \infty\) 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 \(k \mid l\) 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 \( k \leq N \), then there is a sequence \( E_N \in \{-1, +1\}^N \) such that if \( l \in \mathbb{N}, l \leq N/2 \), then
\[
C_l(E_N) > \frac{N - l}{k} - 54k^2N^{1/2}\log N \quad \text{if } k \mid l
\]
and
\[
C_l(E_N) < 27k^2lN^{1/2}\log N \quad \text{if } k \nmid l.
\]

In \cite{22} and \cite{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
\[
Q_k(E_N) \leq N^2 \left( \left( \frac{l}{N} \right)^{2k/l} + \frac{4(l!)^{k/l}}{k!} \left( \frac{Q_l(\eta)}{N^2} \right)^{k/l} \right).
\]

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 \cite{5} it suffices to prove that for all distinct \( d_1, \ldots, d_k \in I_N^2 \) and box \( N \)-lattices \( B \) with \( B + d_1, \ldots, B + d_k \subseteq I_N^2 \) we have
\[
(\sum_{x \in B} \eta(x + d_1) \cdots \eta(x + d_k))^t \leq N^2 \left( \left( \frac{l}{N} \right)^{2k/l} + \frac{4(l!)^{k/l}}{k!} \left( \frac{Q_l(\eta)}{N^2} \right)^{k/l} \right).
\]

Write \( l/k = t \) so that \( t \in \mathbb{N} \) as \( k \mid l \). Then clearly
\[
(\sum_{x \in B} \eta(x + d_1) \cdots \eta(x + d_k))^t = \left( \sum_{x_1 \in B} \eta(x_1 + d_1) \cdots \eta(x_1 + d_k) \right) \cdots \left( \sum_{x_t \in B} \eta(x_t + d_1) \cdots \eta(x_t + d_k) \right) = \sum_{x_1 \in B} \cdots \sum_{x_t \in B} \eta(x_1 + d_1) \cdots \eta(x_1 + d_k) \cdots \eta(x_t + d_1) \cdots \eta(x_t + d_k) = S_1 + S_2,
\]
where \( S_1 \) denotes the contribution of those terms \( \eta(x_1 + d_1) \cdots \eta(x_t + d_k) \) where there are two equal vectors amongst the \( x_i + d_u \)'s:
\[
x_i + d_u = x_j + d_v
\]
(with \( (i, u) \neq (j, v) \)), while in \( S_2 \) all these vectors are distinct.

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

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 $z = (x, y)$): 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 $d_1 < \cdots < d_k$ in terms of this ordering. Consider each of the terms $\eta(x_1 + d_1) \cdots \eta(x_t + d_k)$ in $S_2$, and rearrange the factors $\eta(x_i + d_u)$ so that the vectors are increasing:
\[\eta(x_1 + d_1) \cdots \eta(x_t + d_k) = \eta(w_1) \cdots \eta(w_l) , \quad w_1 < \cdots < w_l.\]

We $t$-colour these factors $\eta(w_1), \ldots, \eta(w_l)$: if the vector $w_u$ is of the form $w_u = x_j + d_v$, then we give $\eta(w_u)$ the $j$th colour. Then to each term $\eta(w_1) \cdots \eta(w_l)$ we may assign the sequence of the colours following each other in the order used to colour $\eta(w_1), \ldots, \eta(w_l)$. 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 $\eta(w_1) \cdots \eta(w_l)$ with this fixed colour pattern. We define an equivalence relation among these terms by
\[\eta(w_1) \cdots \eta(w_l) \sim \eta(v_1) \cdots \eta(v_l) \quad \text{if} \quad v_1 - w_1 = \cdots = v_l - w_l.\]

Clearly, this is indeed an equivalence relation. Fix a colour pattern and an equivalence class, and collect all the terms from this class. Let
\begin{equation}
\eta(a_1) \cdots \eta(a_l)
\end{equation}
be any fixed term taken from this class. Then we have
\begin{equation}
\eta(a_1) < \cdots < \eta(a_l),
\end{equation}
and every term belonging to the class is of the form
\begin{equation}
\eta(a_1 + x) \cdots \eta(a_l + x),
\end{equation}
or equivalently,
\begin{equation}
\eta(y)\eta(y + (a_2 - a_1)) \cdots \eta(y + (a_l - a_1)).
\end{equation}

Now we will determine all vectors $x, y \in \mathbb{N}^2$ for which the product in (12), resp. (13), appears in the sum $S_2$ in (7). First, observe that it follows from (11) that
\[\eta(a_1 + x) < \cdots < \eta(a_l + x),\]
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 $j = 1, \ldots, t$, let $\eta(a_{ij})$ denote the factor in (10) in which the $j$th colour first appears; then clearly $a_{ij}$ is of the form
\[ a_{ij} = z_j + d_1 \]
with some $z_j \in B$ (for $j = 1, \ldots, t$); in particular,
\[ a_1 = a_{ir} = z_r + d_1 \]
for some $r \in \{1, \ldots, t\}$.

Then the $ij$th factor in (13) is
\[ \eta(y + (a_{ij} - a_1)) = \eta(y + (z_j - z_r)). \]

Since this is of the same colour as $\eta(a_{ij})$, we see that $y + (z_j - z_r)$ must be of the form
\[ y + (z_j - z_r) = x_j + d_1 \]
with the $x_j \in B$ in (7), whence
\[ y = x_j + d_1 + z_r - z_j \in B + d_1 + z_r - z_j \]
in particular, for $j = r$ we have
\[ y \in B + d_1. \]

It follows that we must have
\[ y \in (B + d_1) \cap \bigcap_{1 \leq j \leq t} (B + d_r + z_r - z_j). \tag{14} \]

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 $B = \{(au, bv) : 0 \leq u \leq U, 0 \leq v \leq V\}$. Then it is easy to see by induction on $t$ that the intersection of $t$ translates is also a translate of a similar box $B' = \{(au, bv) : 0 \leq u \leq U', 0 \leq v \leq V'\}$ (with $U', V'$ in place of $U, V$); denote this translate by $B' + d'$. Then the sum of the terms (13) belonging to the given equivalence class is
\[ \sum_{y \in B' + d'} \eta(y)\eta(y + (a_2 - a_1)) \ldots \eta(y + (a_t - a_1)) \]
\[ = \sum_{x \in B'} \eta(x + d')\eta(x + d' + a_2 - a_1) \ldots \eta(x + d' + a_t - a_1). \]

By the definition of $Q_l$, it follows that for any fixed equivalence class the absolute value of this sum is
\[ \left| \sum_{y \in B + d'} \eta(y)\eta(y + (a_2 - a_1)) \ldots \eta(y + (a_t - a_1)) \right| \leq Q_l(\eta). \]

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

\[ l!/(k!)^t \] ways, and by the box \( B' \) formed by the vectors \( y \) in (14). This box is uniquely determined by the \( t - 1 \) vectors \( z_r - z_j \) 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

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

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

\[
\left| \sum_{x \in B} \eta(x + d_1) \ldots \eta(x + d_k) \right| = (S_1 + S_2)^{1/t} \leq |S_1|^{1/t} + |S_2|^{1/t}
\]
\[
\leq N^2 \left( \frac{l}{N} \right)^{2k/l} + 4 \frac{(l!)^{k/l}}{k!} \left( \frac{Q_l(\eta)}{N} \right)^{k/l},
\]
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

\[
Q_l(\eta) \geq \frac{N(N - l)}{k} \quad \text{if } k \mid l
\]

and

\[
Q_l(\eta) \ll k^2 l N (\log N)^2 \quad \text{if } k \nmid l.
\]

**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 $d_1, \ldots, d_l$ by
\[ d_i = (i - 1, 0). \]

Then by the definition of the pseudorandom measure of order $l$ we have
\[
Q_l(\eta) \geq \sum_{x \in B} \eta(x + d_1) \cdots \eta(x + d_l)
= \sum_{x_2=0}^{N-1} \sum_{0 \leq x_1 < N - l} \sum_{x_1 \equiv 0 (\text{mod } k)} \eta(x_1, x_2) \eta(x_1 + 1, x_2) \cdots \eta(x_1 + l - 1, x_2).
\]

Since now $k \mid l$, we have
\[
\eta(x_1, x_2) \eta(x_1 + 1, x_2) \cdots \eta(x_1 + l - 1, x_2)
= \prod_{i=0}^{l/k-1} \eta(x_1 + ik, x_2) \eta(x_1 + ik + 1, x_2) \cdots \eta(x_1 + ik + k - 1, x_2).
\]

By the definition of $\eta$, for $x_1 \equiv 0 (\text{mod } k)$ we have
\[
\eta(x_1 + ik, x_2) \eta(x_1 + ik + 1, x_2) \cdots \eta(x_1 + ik + k - 1, x_2) = 1.
\]

It follows that
\[
Q_l(\eta) \geq \sum_{x_2=0}^{N-1} \sum_{0 \leq x_1 < N - l} 1 \geq \frac{N(N - l)}{k}.
\]

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 $d_1, \ldots, d_l \in \mathbb{Z}^2$ be distinct vectors such that $B + d_1, \ldots, B + d_l \subseteq \mathbb{Z}^2$. Let
\[
S = \sum_{x \in B_1} \eta(x + d_1) \cdots \eta(x + d_l).
\]

We will prove that
\[
|S| \ll k^2 lN(\log N)^2
\]
from which (17) follows. Write
\[
d_i = (d_1^{(i)}, d_2^{(i)}).
\]

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

\[(19) \quad S(r) = \sum_{0 \leq x_1 \leq t_1/z_1} \sum_{\substack{x_2=0 \ to\ \infty \mod k}} \prod_{i=1}^{t_2/z_2} \eta(x_1 z_1 + d^{(i)}_1, x_2 z_2 + d^{(i)}_2). \]

Then

\[(20) \quad S = \sum_{r=0}^{k-1} S(r). \]

Next we will prove that

\[(21) \quad |S(r)| \ll klN(\log N)^2. \]

Then (18) follows from (20) and (21). In (19) we substitute \(x_1 = y_1 k + r\), so that

\[(22) \quad S(r) = \sum_{0 \leq y_1 \leq (t_1/z_1 - r)/k} \sum_{x_2=0}^{t_2/z_2} \prod_{i=1}^{l} \eta((y_1 k + r) z_1 + d^{(i)}_1, x_2 z_2 + d^{(i)}_2) \]

\[= \sum_{0 \leq y_1 \leq (t_1/z_1 - r)/k} \sum_{x_2=0}^{t_2/z_2} \prod_{i=1}^{l} \eta((y_1 k z_1, x_2 z_2) + (r z_1 + d^{(i)}_1, d^{(i)}_2)). \]

Since \(B + d_i \subseteq I^2_N\), for \(0 \leq y_1 \leq (t_1/z_1 - r)/k\) we have

\[0 \leq (y_1 k + r) z_1 + d^{(i)}_1 \leq N - 1 \leq p - 2. \]

For \(y_1 = 0\) we get

\[1 \leq r z_1 + d^{(i)}_1 + 1 \leq p - 1. \]

If also \(r z_1 + d^{(i)}_1 \equiv k - 1 \mod k\), then for \(1 \leq j \leq k - 1\) we have

\[(23) \quad 1 \leq r z_1 + d^{(i)}_1 + 1 - j \leq p - 2. \]

We will use (23) later in the proof.

By the definition of \(\eta\) we have

\[\eta((y_1 k z_1, x_2 z_2) + (r z_1 + d^{(i)}_1, d^{(i)}_2)) = \gamma((y_1 k z_1 \mathbf{v}_1 + x_2 z_2 \mathbf{v}_2 + (r z_1 + d^{(i)}_1 + 1) \mathbf{v}_1 + (d^{(i)}_2 + 1) \mathbf{v}_2) \]

for \(r z_1 + d^{(i)}_1 \not\equiv k - 1 \mod k\), and

\[\eta((y_1 k z_1, x_2 z_2) + (r z_1 + d^{(i)}_1, d^{(i)}_2)) = \prod_{j=1}^{k-1} \gamma((y_1 k z_1 \mathbf{v}_1 + x_2 z_2 \mathbf{v}_2 + (r z_1 + d^{(i)}_1 + 1 - j) \mathbf{v}_1 + (d^{(i)}_2 + 1) \mathbf{v}_2) \]

for \(r z_1 + d^{(i)}_1 \equiv k - 1 \mod k\).
Let \( A \) and \( B \) be the following multisets:
\[
A = \{(rz_1 + d_1^{(i)} + 1)v_1 + (d_2^{(i)} + 1)v_2 : 1 \leq i \leq l, \quad rz_1 + d_1^{(i)} \not\equiv k - 1 \pmod{k}\},
\]
\[
B = \{(rz_1 + d_1^{(i)} + 1 - j)v_1 + (d_2^{(i)} + 1)v_2 : 1 \leq i \leq l, 1 \leq j \leq k - 1, \quad rz_1 + d_1^{(i)} \equiv k - 1 \pmod{k}\}.
\]

Here \(|A| = n\) and \(|B| = (k - 1)m\) for some \(n,m \in \mathbb{N}\) with
\[
(24) \quad n + m = l.
\]

Let
\[
B_2 = \{y_1(kz_1v_1) + x_2(z_2v_2) : 0 \leq y_1 \leq (t_1/z_1 - r)/k, 0 \leq x_2 \leq t_2/z_2\}.
\]

Then by (22),
\[
S(r) = \sum_{z \in B_2} \prod_{\alpha \in A \cup B} \gamma(z + \alpha).
\]

Using the multiplicativity of the quadratic character \(\gamma\), we have
\[
S(r) = \sum_{z \in B_2} \gamma\left(\prod_{\alpha \in A \cup B} (z + \alpha)\right).
\]

Now we will use the following lemma:

**Lemma 1.** Let \(p\) be an odd prime, \(n \in \mathbb{N}\), \(q = p^n\) and \(v_1, \ldots, v_n\) 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 \(k_1, \ldots, k_n\) are positive integers with \(k_1 \leq p, \ldots, k_n \leq p\). Then writing \(B = \{\sum_{i=1}^n j_i v_i : 0 \leq j_i < k_i\}\), we have
\[
\left|\sum_{z \in B} \chi(f(z))\right| < sq^{1/2}(1 + \log p)^n.
\]

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

Let \(f(x) = \prod_{\alpha \in A \cup B} (x + \alpha)\). Then
\[
(25) \quad S(r) = \sum_{z \in B_2} \gamma(f(z)).
\]

Here we may use Lemma 1, since \(v_1, v_2\) is a basis of \(\mathbb{F}_q\) over \(\mathbb{F}_p\), thus \(kz_1v_1, z_2v_2\) is also such a basis. Thus the box \(B_2\) is of the same type as \(B\) in Lemma 1. If we prove that \(f(x) = \prod_{\alpha \in A \cup B} (x + \alpha) \in \mathbb{F}_q[x]\) 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
\[ |S(r)| \leq (|A| + |B|)q^{1/2}(1 + \log p)^2 \leq (|A| + |B|)2N(1 + \log(2N))^2 \]
\[ \leq (k - 1)(n + m)2N(1 + \log(2N))^2 \ll klN(\log N)^2, \]
so that (21) holds. Since \( d_1, \ldots, d_l \) are distinct, the elements of \( A \) are distinct. Similarly, the elements of \( B \) are also distinct: for \( (i_1, j_1) \neq (i_2, j_2) \), \( 1 \leq i_1, i_2 \leq l \) and \( 1 \leq j_1, j_2 \leq k - 1 \) we have
\[
(rz_1 + d_1^{(i_1)} + 1 - j_1)v_1 + (d_2^{(i_1)} + 1)v_2 = (rz_1 + d_1^{(i_2)} + 1 - j_2)v_1 + (d_2^{(i_2)} + 1)v_2.
\]
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 \( 0 \leq d_2^{(i_1)}, d_2^{(i_2)} < N < p \) and by (23),
\[
1 \leq rz_1 + d_1^{(i_1)} + 1 - j_1, rz_1 + d_1^{(i_2)} + 1 - j_2 \leq p,
\]
we also have
\[
(26) \quad rz_1 + d_1^{(i_1)} + 1 - j_1 = rz_1 + d_1^{(i_2)} + 1 - j_2,
\]
\[
(27) \quad d_2^{(i_1)} = d_2^{(i_2)}.
\]
Since \( (rz_1 + d_1^{(i_1)} + 1 - j_1)v_1 + (d_2^{(i_1)} + 1)v_2, (rz_1 + d_1^{(i_2)} + 1 - j_2)v_1 + (d_2^{(i_2)} + 1)v_2 \in B \), 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 \( 1 \leq j_1, j_2 \leq k - 1 \), thus
\[
(28) \quad j_1 = j_2.
\]
From this and (26) we get
\[
(29) \quad d_1^{(i_1)} = d_1^{(i_2)}.
\]
It follows from (27) and (29) that
\[
\mathbf{d}_i = \mathbf{d}_j.
\]
But then (28) yields \( (i_1, j_1) = (i_2, j_2) \), which is a contradiction.

Since \( A \) and \( B \) contain different elements, \( \prod_{\alpha \in A \cup B}(x + \alpha) \) is a constant multiple of the perfect square of a polynomial if and only if \( A = B \). Then \( |A| = |B| \), 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 \(X = \{x_1, \ldots, x_k\} \in \{-1, +1\}^k\) let
\[ T(E_N, M, X) = |\{n : 0 \leq n < M, \{e_{n+1}, e_{n+2}, \ldots, e_{n+k}\} = X\}|. \]

**Definition 1 ([47]):** The normality measure of order \(k\) of \(E_N\) is defined as
\[ N_k(E_N) = \max_{X \in \{-1, +1\}^k} \max_{0 < M \leq N+1-k} \left| T(E_N, M, X) - \frac{M}{2^k} \right|. \]

**Definition 2 ([47]):** The normality measure of \(E_N\) is defined as
\[ N(E_N) = \max_{k \leq (\log N)/\log 2} N_k(E_N). \]

It was proved in [47] that

**Theorem C.** For all \(N\), \(E_N\) and \(k < N\) we have
\[ N_k(E_N) \leq \max_{1 \leq t \leq k} C_t(E_N). \]

Thus the estimate of the normality measure of order \(k\) can be reduced to the estimate of the correlation of order \(\leq k\).

Now we will introduce the analogous notations in two dimensions. For \(k, l \in \mathbb{N}\) let \(M(k, l)\) denote the set of \(k \times l\) matrices \(A = (a_{ij})\) with \(a_{ij} \in \{-1, +1\}\) for \(1 \leq i \leq k, 1 \leq j \leq l\), let \(\eta(x, y) : I_N^2 \rightarrow \{-1, +1\}\) be a binary lattice, and for \(X = (x_{ij}) \in M(k, l)\) let
\[ Z(\eta, U, V, X) = |\{(m, n) : 0 \leq m < U, 0 \leq n < V, \eta(m - 1 + i, n - 1 + j) = x_{ij} \text{ for } 1 \leq i \leq k, 1 \leq j \leq l\}|. \]

**Definition 3.** The normality measure of order \((k, l)\) of \(\eta\) is defined as
\[ N_{(k, l)}(\eta) = \max_{X \in M(k, l)} \max_{0 < U \leq N+1-k} \max_{0 < V \leq N+1-l} \left| Z(\eta, U, V, X) - \frac{UV}{2^{kl}} \right|. \]

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

**Definition 4.** The normality measure of \(\eta\) is defined as
\[ N(\eta) = \max_{kl \leq (2 \log N)/\log 2} N_{(k, l)}(\eta). \]

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 $\eta: I_N^k \to \{-1, +1\}$ we have

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

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

$$|Z(\eta, U, V, X) - UV| = \left| \left\{ (m, n) : 0 \leq m < U, 0 \leq n < V, \eta(m - 1 + i, n - 1 + j) = x_{ij} \right\} - UV \right|$$

for $1 \leq i \leq k, 1 \leq j \leq l$. Hence, writing $d_r = (i_r, j_r)$ and $d'_r = (i_r - 1, j_r - 1)$ for $r = 1, \ldots, t$ and $B = \{(m, n) : 0 \leq m < U, 0 \leq n < V\}$ we obtain

$$\left| Z(\eta, U, V, X) - \frac{UV}{2^{kl}} \right| \leq \frac{1}{2^{kl}} \sum_{t=1}^{kl} \sum_{\{d_1, \ldots, d_t\} \subseteq \mathbb{N}(k,l)} \left| \sum_{y \in B} \eta(y + d'_1) \ldots (y + d'_t) \right|$$

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

$$\left| Z(\eta, U, V, X) - \frac{UV}{2^{kl}} \right| \leq \frac{1}{2^{kl}} \sum_{t=1}^{kl} \sum_{\{d_1, \ldots, d_t\} \subseteq \mathbb{N}(k,l)} \left| \sum_{y \in B} \eta(y + d'_1) \ldots (y + d'_t) \right|$$

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

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

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 $\eta$,

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

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 $k \leq r$, $l \leq s$, 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 $k \leq r \leq N$ and $l \leq s \leq N$ and every binary lattice $\eta : I_N^2 \rightarrow \{-1, +1\}$ we have

$$N_{k,l}(\eta) \leq 2((r - k) + (s - l))N + N_{r,s}(\eta)2^{r s - k l}.$$  \hfill (33)

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

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

Then a pair $(m, n)$ with $0 \leq m < U \leq N + 1 - r$, $0 \leq n < V \leq N + 1 - s$ 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 $U \leq N + 1 - r$, $V \leq N + 1 - s$ we get

$$Z(\eta, U, V, X) = \sum_{\substack{Y \in \mathcal{M}(r, s) \\ Y(k, l) = X}} \left| \{(m, n) : 0 \leq m < U, \ 0 \leq n < V, \ D(k, l, m, n, \eta) = X\} \right|$$

$$= \sum_{\substack{Y \in \mathcal{M}(r, s) \\ Y(k, l) = X}} \left( Z(\eta, U, V, Y) - \frac{UV}{2^{k l}} \right) + \frac{UV}{2^{r s}} \sum_{\substack{Y \in \mathcal{M}(r, s) \\ Y(k, l) = X}} 1.$$  \hfill (34)

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

$$\begin{align*}
|Z(\eta, U, V, X) - \frac{UV}{2^{kl}}| &\leq \sum_{Y \in M(r,s)} |Z(\eta, U, V, X) - \frac{UV}{2^{rs}}| \leq N_{(r,s)}(\eta) \sum_{Y \in M(r,s)} 1 \\
&= N_{(r,s)}(\eta)2^{rs - kl} \quad \text{for} \quad U \leq N+1-r, \quad V \leq N+1-s.
\end{align*}$$

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

$$\begin{align*}
|Z(\eta, U, V, X) - \frac{UV}{2^{kl}}| &\leq |Z(\eta, U', V', X) - Z(\eta, U', V', X)| \\
&\quad + \left|Z(\eta, U', V', Y) - \frac{UV'}{2^{kl}}\right| + \frac{1}{2^{kl}}|U'V' - UV|
\end{align*}$$

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

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

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

$$N_{(k,l)}(\eta) = O(N_{(r,s)}(\eta) + N).$$
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 \(N_{(k,k)}(\eta)\). 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 \(E_N^{(1)}, \ldots, E_N^{(N)}\) formed by the row vectors of the matrix \((\eta(i,j))\) (with \(0 \leq i, j < N\)) so that \(E_N^{(i)} = \{e_1^{(i)}, \ldots, e_N^{(i)}\}\) is defined by \(e_j^{(i)} = \eta(i - 1, j - 1)\) for \(i, j = 1, \ldots, N\). 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 \(E_N^{(1)} = \{e_1^{(1)}, \ldots, e_N^{(1)}\}\) of the matrix \((\eta(i,j))\) be a binary sequence such that \(N_k(E_N^{(i)})\) 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 \(i = 1, \ldots, N\), and let \(E_N^{(j)} = E_N^{(1)}\) for \(j = 1, \ldots, N\). 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**


312 K. Gyarmati et al.


[34] —, —, *Explicit construction of normal lattice configurations*, ibid. 102 (2005), 33–47.


[40] —, *A large family of pseudorandom binary lattices*, ibid. 137 (2009), 793–803.


Measures of pseudorandomness of lattices, I


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)