Measures of pseudorandomness of binary lattices, III.

(Q_k, correlation, normality, minimal values.)

Dedicated to the memory of Edmund Hlawka

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 FR-33/2009, 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 study the measures of pseudorandomness of binary lattices. In particular, in this paper first we study the minimum of the measure Q_k in one dimension. Then we introduce the correlation measure C_k in n dimensions, and we estimate the minima of Q_k, C_k and the normality measures in two dimensions. The connection between the correlation measures of order two and three of binary lattices is also studied.
2000 Mathematics Subject Classification: Primary 11K45.
Key words and phrases: binary lattice, pseudorandom, correlation, normality.

1 Introduction

Recently a new constructive approach has been developed to study pseudorandomness of binary sequences, and later this work has been extended to two dimensions. In this series our goal is to study the measures of pseudorandomness in two dimensions. In Part I [9] we studied the measures Q_k and the normality measure, while Part II [10] was devoted to the study of the symmetry measure. Here we will return to the measures Q_k and the normality measure; in particular, we will focus on their minimal values, but we will also study some other related problems. However, first in Section 2 we will recall some basic definitions and results from the one dimensional case, and we will also add some further (one-dimensional) results. In Section 3 we will recall some main definitions and results in the two dimensional case, and we will also introduce the notion of the correlation measure in this case. The rest of the paper will be devoted to new two dimensional results and problems.

2 The basic definitions and results in one dimension

Consider a binary sequence

$$E_N = \{e_1, e_2, \dots, e_N\} \in \{-1, +1\}^N. \tag{2.1}$$

In [14] Mauduit and Sárközy introduced the following measures of pseudorandomness: The *well-distribution measure* of E_N is defined by

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

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

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

where the maximum is taken over all $\mathbf{D} = (d_1, \dots, d_k)$ and M such that $0 \le d_1 < \dots < d_k \le N - M$. 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 $N \to \infty$). Indeed, later Cassaigne, Mauduit and Sárközy [5] 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 [2].) In [14] the combination of the well-distribution measure and the correlation measure was also introduced: The *combined pseudorandom measure of order* k is defined as

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

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 $\{1, 2, \ldots, N\}$. Note that clearly we have

$$Q_1(E_N) = W(E_N) \quad \text{for all } N \in \mathbb{N} \text{ and } E_N \in \{-1, +1\}^N \tag{2.2}$$

and

$$C_k(E_N) \leq Q_k(E_N) \quad \text{for all } k, N \in \mathbb{N} \text{ with } k < N \text{ and } E_N \in \{-1, +1\}^N. \tag{2.3}$$

Now consider again the binary sequence (2.1), and for $k \in \mathbb{N}$, $M \in \mathbb{N}$ and $X = \{x_1, \ldots, x_k\} \in \{-1, +1\}^k$ let

$$T(E_N, M, X) = \left| \{n : \ 0 \leq n < M, \ \{e_{n+1}, e_{n+2}, \ldots, e_{n+k}\} = X\} \right|.$$

Then the *normality measure of order k* of E_N is defined as

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

and 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 [14] that for all N, E_N and $k < N$ we have

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

Since 1997 many papers have been written on these measures of pseudorandomness and on the pseudorandom properties of special sequences; a list of these papers is presented in Part I of this series [9]. The main subject of this paper is the estimate of the minima of the pseudorandom measures, thus here we will restrict ourselves to giving a short survey of the results proved in this direction in one dimension.

In [16] Roth proved

Theorem A *We have*

$$\min_{E_N \in \{-1,+1\}^N} W(E_N) \left(= \min_{E_N \in \{-1,+1\}^N} Q_1(E_N) \right) \gg N^{1/4}. \tag{2.4}$$

More precisely, this estimate does not appear explicitely in his paper; however, by adapting his method, one can prove the following more general result easily:

Theorem B *Let $N, Q \in \mathbb{N}$, $Q \geq 2$, and write $Q_1 = [Q/2]$. Let $s_1, s_2, \dots, s_N$ be complex numbers, and set $s_i = 0$ for $i = 0, -1, -2, \dots$ and $i = N+1, N+2, \dots$ Then we have*

$$\sum_{q=1}^{Q} \sum_{n=1-(Q_1-1)q}^{N} \left| s_n + s_{n+q} + s_{n+2q} + \dots + s_{n+(Q_1-1)q} \right|^2 \geq \left(\frac{2}{\pi} Q_1 \right)^2 \sum_{m=1}^{N} |s_m|^2 . \tag{2.5}$$

(This version of the result appears in [17].) Choosing here $s_n = e_n$ for $n = 1, 2, \dots, N$ and $Q = [\sqrt{N}]$, we get easily that the greatest term in the double sum in (2.5) satisfies

$$\left| e_n + e_{n+q} + e_{n+2q} + \dots + e_{n+([\sqrt{N}/2]-1)q} \right| \gg N^{1/4}$$

which proves (2.4).

In the opposite direction Beck [4] proved:

$$\min_{E_N \in \{-1,+1\}^N} W(E_N) \left(= \min_{E_N \in \{-1,+1\}^N} Q_1(E_N) \right) \ll N^{1/4} (\log N)^{5/2}.$$

Later Matoušek and Spencer [15] improved this to

Theorem C *We have*

$$\min_{E_N \in \{-1,+1\}^N} W(E_N) \ll N^{1/4}.$$

Thus now it is known that the exact order of magnitude of $\min W(E_N)$ is $N^{1/4}$.

Now consider $\min\limits_{E_N} C_k(E_N)$. Cassaigne, Mauduit and Sárközy [5] showed that for every fixed $k \in \mathbb{N}$ we have

$$\min_{E_N \in \{-1,+1\}^N} C_k(E_N) \ll (kN \log N)^{1/2}, \tag{2.6}$$

and if k is even, then

$$\min_{E_N \in \{-1,+1\}^N} C_k(E_N) \gg \log N \quad \text{(for } k \text{ even).} \tag{2.7}$$

On the other hand, they showed that if $E_N = \{e_1, e_2, \ldots, e_N\} \in \{-1,+1\}^N$ is defined by $e_n = (-1)^n$ for $n = 1, 2, \ldots, N$, then we have

$$C_k(E_N) = 1 \quad \text{(for } k \text{ odd)}$$

thus for all N,

$$\min_{E_N \in \{-1,+1\}^N} C_k(E_N) = 1 \quad \text{for } k \text{ odd.} \tag{2.8}$$

Later Alon, Kohayakawa, Mauduit, Moreira and Rödl [1], [13] improved (2.7) to:

Theorem D If $k, N \in \mathbb{N}$, $2 \le k \le N$ and k is even, then

$$\min_{E_N \in \{-1,+1\}^N} C_k(E_N) \gg \left(\frac{N}{k}\right)^{1/2} \quad \text{(for } k \text{ even).} \tag{2.9}$$

Thus now the order of magnitude of $\min C_k(E_N)$ is known, apart from a logarithmic factor, for fixed even k.

On the other hand, we know very little on the minimum of the normality measure. Alon, Kohayakawa, Mauduit, Moreira and Rödl [1] proved the following results:

Theorem E

(i) We have

$$\min_{E_N \in \{-1,+1\}^N} N_k(E_N) = 1 - 2^{-k} \tag{2.10}$$

for any $k \ge 1$ and any $N \ge 2^k$.

(ii) We have

$$\min_{E_N \in \{-1,+1\}^N} N_k(E_N) \ge \left(\frac{1}{2} + o(1)\right) \frac{\log N}{\log 2}. \tag{2.11}$$

Theorem F *For $N > N_0$ we have*

$$\min_{E_N \in \{-1,+1\}^N} N_k(E_N) \le 3N^{1/3} (\log N)^{2/3}. \tag{2.12}$$

There is a huge gap between the lower bound (2.11) and the upper bound (2.12). They write in [1]: "We suspect that the logarithmic lower bound" [in (2.11)] "is far from the truth". They pose the following problem:

Problem 1 *Is there an absolute constant $\alpha > 0$ for which we have*

$$\min_{E_N \in \{-1,+1\}^N} N_k(E_N) \geq N^\alpha$$

for all large enough N?

Now this is, perhaps, the most important unsolved problem in this field.

Finally, $\min_{E_N \in \{-1,+1\}^N} Q_k(E_N)$ has not been studied yet. Thus we will complete this section by proving a theorem in this direction:

Theorem 1 *(i) If $k, N \in \mathbb{N}$, $2 \leq k \leq N$ and k is even, then*

$$\min_{E_N \in \{-1,+1\}^N} Q_k(E_N) \gg \left(\frac{N}{k}\right)^{1/2} \qquad \text{(for } k \text{ even)}. \tag{2.13}$$

(ii) For every $0 < \varepsilon < 1$ there is a number $N_0(\varepsilon)$ such that if $k, N \in \mathbb{N}$, $N > N_0(\varepsilon)$ and $k \leq (1-\varepsilon)N$, then

$$\min_{E_N \in \{-1,+1\}^N} Q_k(E_N) \gg \varepsilon^{1/4} N^{1/4} \quad \text{(for all } k \leq (1-\varepsilon)N \text{)}. \tag{2.14}$$

(iii) We have

$$\min_{E_N \in \{-1,+1\}^N} Q_1(E_N) \ll N^{1/4}.$$

(iv) If $k \in \mathbb{N}$, $k \geq 2$, then there is a number $N_0 = N_0(k)$ such that for $N \in \mathbb{N}$, $N > N_0$ we have

$$\min_{E_N \in \{-1,+1\}^N} Q_k(E_N) \leq 9(kN \log N)^{1/2}. \tag{2.15}$$

(v) For all *$k, N \in \mathbb{N}$ with $2 \leq k \leq N$ we have*

$$\min_{E_N \in \{-1,+1\}^N} Q_k(E_N) \ll k N^{1/2} \log N.$$

Observe that for odd k there is a significant difference between the behavior of C_k and Q_k: while $\min_{E_N} C_k(E_N)$ is bounded for odd k by (2.8), we have $\min_{E_N} Q_k(E_N) \gg N^{1/4}$ for odd k as well by (2.14).

Proof of Theorem 1.

(i) This follows trivially from (2.3) and (2.9).

(ii) Let $E_N = \{e_1, e_2, \dots, e_N\}$, $M = [\varepsilon N]$, and define $F_M = \{f_1, f_2, \dots, f_M\} \in \{-1, +1\}^M$ by

$$f_n = e_n e_{n+1} \dots e_{n+k-1}$$

(note that $M + k - 1 \leq [\varepsilon N] + (1 - \varepsilon)N - 1 < N$). Then using (2.4) in Theorem A with F_M in place of E_N we obtain that there exist a, b, t with $1 \leq a \leq a + (t-1)b \leq M$ such that

$$\left| \sum_{j=0}^{t-1} f_{a+jb} \right| \gg M^{1/4} \gg \varepsilon^{1/4} N^{1/4}. \tag{2.16}$$

By the definition of Q_k we have

$$\left| \sum_{j=0}^{t-1} f_{a+jb} \right| = \left| \sum_{j=0}^{t-1} e_{a+jb} e_{a+jb+1} \dots e_{a+jb+k-1} \right| \leq Q_k(E_N), \tag{2.17}$$

and (2.14) follows from (2.16) and (2.17).

(iii) This follows from Theorem C by (2.2).

(iv) By the $n = 1$, $\varepsilon = \frac{1}{2}$ special case of the second half (more precisely, formula (3.3)) of Theorem 1 of Hubert, Mauduit and Sárközy in [12], choosing every $E_N \in \{-1, +1\}^N$ with equal probability 2^{-N} we have

$$P\left(Q_k(E_N) > (81kN \log N)^{1/2}\right) < \frac{1}{2}$$

for $N > N_0(k)$, so that

$$Q_k(E_N) \leq 9(kN \log N)^{1/2}$$

holds for at least half of the sequences $E_N \in \{-1, +1\}^N$ which proves (2.15).

(v) Let p denote the smallest prime greater than N, and let E_N denote the Legendre symbol sequence $E_N = \left\{ \left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \dots, \left(\frac{N}{p}\right) \right\}$. Then by (3.1) in [14] we have

$$Q_k(E_N) \leq 9kp^{1/2} \log p \ll kN^{1/2} \log N$$

as $N \to \infty$.

We remark that for odd (fixed) k there is a large gap between the lower bound (2.14) and the upper bound (2.15):

$$N^{1/4} \ll \min_{E_N \in \{-1,+1\}^N} Q_k(E_N) \ll (kN \log N)^{1/2} \qquad (k > 1 \text{ odd, fixed}). \quad (2.18)$$

Problem 2 *Tighten the gap between the lower and upper bounds in* (2.18).

We remark that a further pseudorandom measure, the symmetry measure was introduced in [7], and its minimum was also estimated there. Since both the two dimensional extension of this measure and the minimum of it was studied in Part II of this series [10] thus we do not include this measure in this paper.

3 The basic definitions and results in two dimensions

In [12] Hubert, Mauduit and Sárközy 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 [11] 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 $z_i \in \mathbb{N}$). Let $t_1,t_2,\dots,t_n$ be integers with $0 \le t_1,t_2,\dots,t_n < N$. Then we call the set

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

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

In [12] the definition of binary sequences was extended from one dimension to n 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 [12] 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 [11]): Let

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

Define the *pseudorandom measure of order k* of η by

$$Q_k(\eta) = \max_{B,\mathbf{d_1},\dots,\mathbf{d_k}} \left| \sum_{\mathbf{x}\in B} \eta(\mathbf{x}+\mathbf{d_1}) \cdots \eta(\mathbf{x}+\mathbf{d_k}) \right|, \tag{3.1}$$

where the maximum is taken over all distinct $\mathbf{d_1},\dots,\mathbf{d_k} \in I_N^n$ and all box N-lattices B such that $B+\mathbf{d_1},\dots,B+\mathbf{d_k} \subseteq I_N^n$. Note that in the one dimensional special case the measure $Q_k(\eta)$ is the same as the combined pseudorandom measure of order k described in Section 2.

Then η is said to have strong pseudorandom properties, or briefly, it is considered as a "good" pseudorandom binary lattice if for a fixed n and “large” N the measure $Q_k(\eta)$ is “small” (much smaller, than the trivial upper bound N^n). This terminology is justified by the fact that, as it was proved in [12], for a truly random binary lattice defined on I_N^n and for fixed k the measure $Q_k(\eta)$ is “small”, more precisely, it is less than $N^{n/2}$ multiplied by a logarithmic factor. A list of papers written on pseudorandomness of binary lattices is presented in Part I of this series [9].

Note that while in one dimension we separated Q_k into the measures W and C_k, here in n dimension the analog of C_k has not been introduced yet (the analog of $W(E_N) = Q_1(E_N)$ is $Q_1(\eta)$). The reason of this is that in one dimension the distribution in arithmetic progression and the correlation are standard notions which are intensively studied independently of the notion of pseudorandomness, and this fact has no analog in n dimensions; besides, if we are interested only in pseudorandomness, then the use of the measure Q_k is sufficient. In spite of this now we introduce the n-dimensional extension of the notion of correlation since later in this paper we will need it:

The *correlation measure of order* k of the lattice $\eta : I_N^2 \to \{-1, +1\}$ is defined by

$$C_k(\eta) = \max_{B', \mathbf{d_1}, \ldots, \mathbf{d_k}} \left| \sum_{\mathbf{x} \in B'} \eta(\mathbf{x} + \mathbf{d_1}) \cdots \eta(\mathbf{x} + \mathbf{d_k}) \right|,$$

where the maximum is taken over all distinct $\mathbf{d_1}, \ldots, \mathbf{d_k} \in I_N^n$ and all box lattices B' of the special form

$$B' = \{\mathbf{x} = (x_1, \ldots, x_n) : \ 0 \leq x_1 \leq t_1(< N), \ldots, \ 0 \leq x_n \leq t_n(< N)\}$$

such that $B' + \mathbf{d_1}, \ldots, B' + \mathbf{d_k} \subseteq I_N^n$. Note that it follows trivially from the definition that for all η, k we have

$$C_k(\eta) \leq Q_k(\eta) \tag{3.2}$$

(but Q_k is usually much greater than C_k). Later some of our methods used for giving lower bounds for Q_k will also give the same lower bound for C_k. It will be worth to formulate these results in terms of C_k instead of Q_k since in this way we get sharper results by (3.2).

In this section so far we have been considering n-dimensional binary lattices. From now on (as in the earlier parts of this series) we restrict ourselves to the special case $n = 2$. Namely, the general case could be handled similarly, just the formulas are much more complicated and lengthy.

Another measure of pseudorandomness, the *normality measure* in two dimensions was introduced in Part I of this series [9]. 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 (two-dimensional) binary lattice, and for $X = (x_{ij}) \in \mathcal{M}(k, \ell)$ let

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

Then the *the normality measure of order (k, ℓ) of η* is defined as

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

while the *normality measure of η* is defined as

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

In this paper, first in Section 4 we will prove a result of independent interest to be used in the estimate of $\min Q_k(\eta)$. Then in Section 5, 6 and 7 we will estimate $\min C_k(\eta)$ and $\min Q_k(\eta)$. In Section 8 we will prove an inequality on C_2 and C_3. Finally, in Section 9 we will estimate $\min N(\eta)$.

4 Generalization of Roth's theorem to two dimensions

In this section we will prove the following two dimensional generalization of Roth's Theorem A, more precisely, of the more general Theorem B:

Theorem 2 *Let $N \in \mathbb{N}$, $Q \in \mathbb{N}$ and*

$$Q \geq 2, \tag{4.1}$$

and write $Q_1 = [Q/2]$. For $u = 1, 2, \ldots, N$ and $v = 1, 2, \ldots, N$, let $s_{u,v}$ be complex numbers, and set

$$s_{u,v} = 0 \text{ if } u, v \in \mathbb{Z} \text{ and one of } u < 1,\ u > N,\ v < 1,\ v > N \text{ holds.} \tag{4.2}$$

For $m, n \in \mathbb{Z}$ and $q, r, \ell \in \mathbb{N}$, write

$$D(m, n, q, r, \ell) = \sum_{j=0}^{\ell-1} \sum_{k=0}^{\ell-1} s_{m+jq, n+kr}.$$

Then we have

$$\sum_{q=1}^{Q} \sum_{r=1}^{Q} \sum_{m=1-(Q_1-1)q}^{N} \sum_{n=1-(Q_1-1)r}^{N} |D(m, n, q, r, Q_1)|^2 \geq \left(\frac{2}{\pi} Q_1\right)^4 \sum_{m=1}^{N} \sum_{n=1}^{N} |s_{m,n}|^2 . \tag{4.3}$$

Corollary 1 *Having the assumptions and notations of Theorem 2, there exist $m, n \in \mathbb{Z}$ and $q, r \in \mathbb{N}$ such that*

$$1 \leq q, r \leq Q \tag{4.4}$$

and

$$|D(m, n, q, r, Q_1)| \geq \left(\frac{2}{\pi}\right)^2 \left[\frac{Q}{2}\right]^2 Q^{-1} \left(N + \frac{Q^2}{4}\right)^{-1} \left(\sum_{m=1}^{N} \sum_{n=1}^{N} |s_{m,n}|^2\right)^{1/2} . \tag{4.5}$$

Corollary 2 *If $\varepsilon > 0$, $N > N_0(\varepsilon)$ is a positive integer, $s_{u,v} \in \mathbb{C}$ for $u, v \in \{1, 2, \ldots, N\}$, and we also use the notation (4.2), then there exist $m, n \in \mathbb{Z}$ and $q, r \in \mathbb{N}$ such that $q, r \leq N^{1/2}$ and*

$$\left|D(m, n, q, r, [N^{1/2}/2])\right| \geq \left(\frac{4}{5\pi^2} - \varepsilon\right) \left(\frac{1}{N^2} \sum_{m=1}^{N} \sum_{n=1}^{N} |s_{m,n}|^2\right)^{1/2} N^{1/2}.$$

We remark that we will use these results, more precisely, Corollary 2 later in section 5 in the lower estimate of $\min Q_k$ in Theorem 3 where it would suffice to use a more special result of Doerr, Srivastav and Wehr [6]. However, the more general form presented above can be useful in many applications (e.g., character sum estimates in the manner of [17]), study of k-ary lattices, i.e., lattices composed of k symbols instead of binary lattices, etc.); besides, in [6] the authors write "... we were not able to generalize Roth's proof to higher dimensions. Instead we use a different approach..." Thus we think it is of some interest to present here the much more general result Theorem 2 which can be proved by an adaption of Roth's original method using elementary harmonic analysis only.

Proof of Theorem 2. Let

$$F(\alpha) = \sum_{j=0}^{Q_1-1} e(j\alpha)$$

(we use the notion $e(\beta) = e^{2\pi i\beta}$) and

$$S(\alpha, \beta) = \sum_{m=1}^{N} \sum_{n=1}^{N} s_{m,n} e(m\alpha)e(n\beta).$$

Adapting Roth method, we start out from the integral

$$\mathcal{J} = \int_0^1 \int_0^1 \sum_{q=1}^{Q} \sum_{r=1}^{Q} |F(q\alpha)F(r\beta)S(\alpha, \beta)|^2 \, d\alpha d\beta.$$

As Roth proved (see (11) in [16]) we have

$$\sum_{q=1}^{Q} |F(q\alpha)|^2 \geq \left(\frac{2}{\pi} Q_1\right)^2 \qquad \text{for all } 0 \leq \alpha \leq 1.$$

Thus by Parseval's formula we have

$$\begin{aligned}
\mathcal{J} &= \int_0^1 \int_0^1 |S(\alpha,\beta)|^2 \sum_{q=1}^{Q} |F(q\alpha)|^2 \sum_{r=1}^{Q} |F(r\beta)|^2 \, d\alpha d\beta \\
&\geq \left(\frac{2}{\pi} Q_1\right)^4 \int_0^1 \int_0^1 |S(\alpha,\beta)|^2 \, d\alpha d\beta \\
&= \left(\frac{2}{\pi} Q_1\right)^4 \sum_{m=1}^{N} \sum_{n=1}^{N} |s_{m,n}|^2 . \qquad (4.6)
\end{aligned}$$

On the other hand, again by Parseval's formula (and using also (4.2)) we have

$$\begin{aligned}
\mathcal{J} &= \sum_{q=1}^{Q} \sum_{r=1}^{Q} \int_0^1 \int_0^1 |F(q\alpha)F(r\beta)S(\alpha,\beta)|^2 \, d\alpha d\beta \\
&= \sum_{q=1}^{Q} \sum_{r=1}^{Q} \int_0^1 \int_0^1 \left| \sum_{j=0}^{Q_1-1} e(jq\alpha) \sum_{k=0}^{Q_1-1} e(kr\beta) \sum_{m=1}^{N} \sum_{n=1}^{N} s_{m.n} e(m\alpha) e(n\beta) \right|^2 d\alpha d\beta \\
&= \sum_{q=1}^{Q} \sum_{r=1}^{Q} \int_0^1 \int_0^1 \left| \sum_{j=0}^{Q_1-1} \sum_{k=0}^{Q_1-1} \sum_{m=1}^{N} \sum_{n=1}^{N} s_{m.n} e((m+jq)\alpha) e((n+kr)\beta) \right|^2 d\alpha d\beta \\
&= \sum_{q=1}^{Q} \sum_{r=1}^{Q} \int_0^1 \int_0^1 \left| \sum_{u=1}^{N+(Q_1-1)q} \sum_{v=1}^{N+(Q_1-1)r} \sum_{j=0}^{Q_1-1} \sum_{k=0}^{Q_1-1} s_{u-jq.v-kr} e(u\alpha) e(v\beta) \right|^2 d\alpha d\beta \\
&= \sum_{q=1}^{Q} \sum_{r=1}^{Q} \int_0^1 \int_0^1 \Bigg| \sum_{u=1}^{N+(Q_1-1)q} \sum_{v=1}^{N+(Q_1-1)r} \\
&\qquad D(u-(Q_1-1)q, v-(Q_1-1)r, q, r, Q_1) e(u\alpha) e(v\beta) \Bigg|^2 d\alpha d\beta \\
&= \sum_{q=1}^{Q} \sum_{r=1}^{Q} \sum_{u=1}^{N+(Q_1-1)q} \sum_{v=1}^{N+(Q_1-1)r} |D(u-(Q_1-1)q, v-(Q_1-1)r, q, r, Q_1)|^2 \\
&= \sum_{q=1}^{Q} \sum_{r=1}^{Q} \sum_{m=1-(Q_1-1)q}^{N} \sum_{n=1-(Q_1-1)r}^{N} |D(m,n,q,r,Q_1)|^2 \qquad (4.7)
\end{aligned}$$

(4.3) follows from (4.6) and (4.7) and this completes the proof of the theorem.

Proof of Corollary 1. Let us write

$$D = \max_{\substack{1 \le q, r \le Q \\ 1-(Q_1-1)q \le m, n \le N}} |D(m,n,q,r,Q_1)|\,.$$

Then the left hand side of (4.3) is

$$\begin{aligned}
&\sum_{q=1}^{Q}\sum_{r=1}^{Q}\sum_{m=1-(Q_1-1)q}^{N}\sum_{n=1-(Q_1-1)r}^{N} |D(m,n,q,r,Q_1)|^2 \\
&\le D^2 \left(\sum_{q=1}^{Q} N + (Q_1-1)q\right)^2 \qquad (4.8)\\
&\le D^2 Q^2 \left(N + \left(\frac{Q}{2} - 1\right)\frac{(Q+1)}{2}\right)^2 \\
&\le D^2 Q^2 \left(N + \frac{Q^2}{4}\right)^2. \qquad (4.9)
\end{aligned}$$

Combining (4.3) with (4.9) we obtain

$$D^2 Q^2 \left(N + \frac{Q^2}{4}\right)^2 \ge \left(\frac{2}{\pi} Q_1\right)^4 \sum_{m=1}^{N}\sum_{n=1}^{N} |s_{m,n}|^2\,.$$

It follows from this that

$$D \ge \left(\frac{2}{\pi}\right)^2 \left[\frac{Q}{2}\right]^2 Q^{-1} \left(N + \frac{Q^2}{4}\right)^{-1} \left(\sum_{m=1}^{N}\sum_{n=1}^{N} |s_{m,n}|^2\right)^{1/2}$$

which proves that there exist $m, n \in \mathbb{Z}$ and $q, r \in \mathbb{Q}$ satisfying (4.4) and (4.5).

Corollary 2 can be obtained from Corollary 1 by choosing $Q = [\sqrt{N}]$, we leave the details to the reader.

5 The minimum of Q_k in two dimensions: lower bound for every k

First we will prove the two dimensional analog of (ii) in Theorem 1.

Theorem 3 *For every number $0 < \varepsilon < 1$ there is a number $N_0(\varepsilon)$ such that if $k, N \in \mathbb{N}$, $N > N_0(\varepsilon)$ and $k \leq (1-\varepsilon)N$, then*

$$\min_{\eta:\ I_N^2\{-1,+1\}} Q_k(\eta) \gg \varepsilon^{1/2} N^{1/2} \qquad \textit{(for all } k \leq (1-\varepsilon)N\textit{).} \tag{5.1}$$

Proof of Theorem 3. Consider first the special case $k = 1$. Then by Theorem 1.2 of Doerr, Srivastov and Wehr [6] we have

$$Q_1(\eta) \gg N^{1/2} \tag{5.2}$$

for all $\eta:\ I_N^2 \to \{-1,+1\}$ (note that this also follows from Corollary 2 immediately by taking there $s_{m,n} = \eta(m,n)$) which proves (5.1) for $k = 1$.

Assume now that $\eta:\ I_N^2 \to \{-1,+1\}$ and $2 \leq k \leq (1-\varepsilon)N$. Write $M = [\varepsilon N]$, and define the binary M-lattice $\varphi:\ I_M^2 \to \{-1,+1\}$ by

$$\varphi(u,v) = \eta(u,v)\eta(u+1,v+1)\dots\eta(u+k-1,v+k-1) \quad \text{for } 0 \leq u,v \leq M-1$$

(note that then $\max\{u+k-1, v+k-1\} \leq M-1+k-1 \leq \varepsilon N - 1 + (1-\varepsilon)N - 1 < N-1$). Then using the $k = 1$ special case in (5.2) of (5.1) (that we have proved already) with M and φ in place of N and η we obtain that

$$Q_1(\varphi) \gg M^{1/2} \gg \varepsilon^{1/2} N^{1/2},$$

i.e., there is a box M-lattice B and a $\mathbf{d} \in I_M^2$ with $B + \mathbf{d} \subseteq I_M^2$ and

$$\begin{aligned} &\left|\sum_{\mathbf{x}\in B} \varphi(\mathbf{x}+\mathbf{d})\right| \\ = &\left|\sum_{\mathbf{x}\in B} \eta(\mathbf{x}+\mathbf{d})\eta(\mathbf{x}+(\mathbf{d}+(1,1)))\dots\eta(\mathbf{x}+(\mathbf{d}+(k-1,k-1)))\right| \\ \gg &\ \varepsilon^{1/2} N^{1/2} \end{aligned}$$

which proves (5.1).

6 The minimum of C_k in two dimensions, lower bound for Q_k for even k

First we will show that as in one dimension, C_k is bounded if k is odd:

Proposition 1 *If $k, N \in \mathbb{N}$, $1 \le k \le N$ and $k = 2\ell + 1$ is odd, then we have*

$$\min_{\eta:\ I_N^2 \to \{-1,+1\}} C_k(\eta) = 1. \tag{6.1}$$

Note that as in one dimension, there is a significant difference between the behavior of $\min C_k$ and $\min Q_k$ for odd k: by (6.1) we have $\min_\eta C_k(\eta) = O(1)$, while $\min_\eta Q_k(\eta) \gg N^{1/2}$ holds for odd k as well by (5.1).

Proof of Proposition 1. For any $\eta :\ I_N^2 \to \{-1,+1\}$ consider the box B' consisting of the single point $(0,0)$. Then for any distinct $\mathbf{d_1}, \mathbf{d_2}, \dots . \mathbf{d_k} \in I_N^2$ we have

$$\left| \sum_{\mathbf{x} \in B'} \eta(\mathbf{x} + \mathbf{d_1}) \dots \eta(\mathbf{x} + \mathbf{d_k}) \right| = |\eta(\mathbf{d_1}) \dots \eta(\mathbf{d_k})| = 1$$

whence

$$C_k(\eta) \ge 1$$

for all η, so that

$$\min_\eta C_k(\eta) \ge 1. \tag{6.2}$$

To show that this minimum is ≤ 1, consider the special lattice η defined by

$$\eta(i,j) = (-1)^{i+j} \quad \text{for } i, j \in \{0, 1, \dots, N-1\},$$

and consider any B', $\mathbf{d_1} = (d'_1, d_1")$, $\ldots$, $\mathbf{d_k} = (d'_k, d_k")$ satisfying the requirements in the definition of C_k. Then we have

$$\begin{aligned}
&\left|\sum_{\mathbf{x}\in B'} \eta(\mathbf{x}+\mathbf{d_1})\ldots\eta(\mathbf{x}+\mathbf{d_k})\right| \\
&= \left|\sum_{(i,j)\in B'} \eta((i,j)+(d'_1, d_1"))\ldots\eta((i,j)+(d'_k, d_k"))\right| \\
&= \left|\sum_{(i,j)\in B'} \eta(i+d'_1, j+d_1")\ldots\eta(i+d'_k, j+d_k")\right| \\
&= \left|\sum_{(i,j)\in B'} (-1)^{(i+d'_1+j+d_1")+\cdots+(i+d'_k+j+d_k")}\right| \\
&= \left|(-1)^{d'_1+d_1"+\cdots+d'_k+d_k"} \sum_{(i,j)\in B'} (-1)^{k(i+j)}\right| \\
&= \left|\sum_{(i,j)\in B'} (-1)^{i+j}\right|
\end{aligned}$$

since k is odd. It is easy to see that for a box B' of the type studied by us this last sum is always $-1, 0$ or $+1$, thus we always have

$$\left|\sum_{\mathbf{x}\in B'} \eta(\mathbf{x}+\mathbf{d_1})\ldots\eta(\mathbf{x}+\mathbf{d_k})\right| \leq 1$$

so that

$$C_k(\eta) \leq 1.$$

Thus we have

$$\min_{\eta} C_k(\eta) \leq 1. \tag{6.3}$$

(6.1) follows from (6.2) and (6.3), and this completes the proof of Proposition 1.

Now we will prove the two dimensional analog of (2.9) in Theorem D.

Theorem 4 *If $k, N \in \mathbb{N}$, $2 \le k \le N$ and $k = 2\ell$ is even, then*

$$\min_{\eta:\ I_N^2 \to \{-1,+1\}} C_k(\eta) \ge \frac{\sqrt{2}}{3k} N. \tag{6.4}$$

It follows from (3.2) and Theorem 4 that

$$\min_{\eta} Q_k(\eta) \ge \frac{\sqrt{2}}{3k} N \qquad (\text{for } k \text{ even})$$

also holds which is much better than the lower bound $\gg N^{1/2}$ in Theorem 3 valid for all k.

Proof of Theorem 4. We adapt the method of Anantharam [3] to prove the theorem. We remark that the method of the proof of Alon, Kohayakawa, Mauduit, Moreira and Rödl [1], [13] also could be adapted and, indeed, it would give this lower bound with a slightly better absolute constant factor. (One can prove $Q_{2k}(\eta) \ge \frac{\sqrt{3}}{2} \left[\frac{N}{k+1}\right]$ by their method.) However, we preferred to use Anantharam's method since it is simpler and easier to adapt.

Let $M, L \in \mathbb{N}$, $M + L \le N + 1$, $\eta:\ I_N^2 \to \{-1,+1\}$, and write

$$c_{\mathbf{d_1},\mathbf{d_2},\dots,\mathbf{d_k}} = \sum_{\mathbf{u} \in I_M^2} \eta(\mathbf{u}+\mathbf{d_1})\eta(\mathbf{u}+\mathbf{d_2})\dots\eta(\mathbf{u}+\mathbf{d_k}).$$

Then we have

$$\begin{aligned}
\sum_{\mathbf{d_1},\dots,\mathbf{d_k} \in I_L^2} c^2_{\mathbf{d_1},\dots,\mathbf{d_k}} &= \sum_{\mathbf{d_1},\mathbf{d_2},\dots,\mathbf{d_k} \in I_L^2} \left(\sum_{\mathbf{u} \in I_M^2} \eta(\mathbf{u}+\mathbf{d_1})\dots\eta(\mathbf{u}+\mathbf{d_k}) \right)^2 \\
&= \sum_{\mathbf{d_1},\mathbf{d_2},\dots,\mathbf{d_k} \in I_L^2} \sum_{\mathbf{u} \in I_M^2} \sum_{\mathbf{v} \in I_M^2} \\
&\qquad \eta(\mathbf{u}+\mathbf{d_1})\dots\eta(\mathbf{u}+\mathbf{d_k})\eta(\mathbf{v}+\mathbf{d_1})\dots\eta(\mathbf{v}+\mathbf{d_k}) \\
&= \sum_{\mathbf{u} \in I_M^2} \sum_{\mathbf{v} \in I_M^2} \left(\sum_{\mathbf{d} \in I_L^2} \eta(\mathbf{u}+\mathbf{d})\eta(\mathbf{v}+\mathbf{d}) \right)^k \\
&\overset{(a)}{\ge} \sum_{\mathbf{u} \in I_M^2} \left(\sum_{\mathbf{d} \in I_L^2} \eta(\mathbf{u}+\mathbf{d})^2 \right)^k \\
&= M^2 L^{2k}.
\end{aligned}$$

where step (a) comes from dropping all the off-diagonal terms, which are nonnegative since k is even. Now we may write

$$\sum_{\mathbf{d_1},\mathbf{d_2},\ldots,\mathbf{d_k}\in I_L^2} c_{\mathbf{d_1},\ldots,\mathbf{d_k}}^2 = k! \sum\nolimits^* c_{\mathbf{d_1},\ldots,\mathbf{d_k}}^2 + \text{other terms},$$

where in $\sum^*$ we sum over all k-element subsets $\{\mathbf{d_1},\ldots,\mathbf{d_k}\}$ of I_L^2, the total number of other terms is $(L^2)^k - L^2(L^2-1)\ldots(L^2-(k-1))$, and each of these other terms is bounded above by M^4. It is straightforward to prove by induction that

$$(L^2)^k - L^2(L^2-1)\ldots(L^2-(k-1)) \le \frac{k}{2}(k-1)(L^2)^{k-1},$$

so

$$(L^2)^k - L^2(L^2-1)\ldots(L^2-(k-1)) \le \frac{1}{2}k^2(L^2)^{k-1}.$$

It follows that

$$\sum_{\mathbf{d_1},\mathbf{d_2},\ldots,\mathbf{d_k}\in I_L^2} c_{\mathbf{d_1},\ldots,\mathbf{d_k}}^2 \le (L^2)^k C_k^2(\eta) + \frac{1}{2}k^2(L^2)^{k-1}M^4.$$

Combining this with the lower bound that was proved previously we get

$$C_k(\eta) \ge \sqrt{\frac{M^2\left(L^2 - \frac{1}{2}k^2M^2\right)}{L^2}}.$$

Set $M = \varepsilon N$ and $L = N - M$, and assume that $L > \frac{1}{\sqrt{2}}M$. Then

$$C_k(\eta) \ge \sqrt{\frac{\varepsilon^2\left((1-\varepsilon)^2 - \frac{1}{2}k^2\varepsilon^2\right)}{(1-\varepsilon)^2}}N,$$

where $\varepsilon < \frac{1}{\frac{1}{\sqrt{2}}k+1}$. Choose $\varepsilon = \frac{2}{3k}$, then by $k \ge 2$

$$\begin{aligned}\varepsilon^2\left(1 - \frac{\frac{1}{2}k^2\varepsilon^2}{(1-\varepsilon)^2}\right) &= \frac{4}{9k^2}\left(1 - \frac{k^2\frac{4}{9k^2}}{2\left(1-\frac{2}{3k}\right)^2}\right)\\ &\ge \frac{4}{9k^2}\left(1 - \frac{2}{9\left(1-\frac{1}{3}\right)^2}\right)\\ &= \frac{4}{18k^2}.\end{aligned}$$

Thus

$$C_k(\eta) \geq \frac{\sqrt{2}}{3k} N$$

which completes the proof of (6.4).

7 The minimum of Q_k in two dimensions: upper bounds

We will prove

Theorem 5 *(i) We have*

$$\min_{\eta:\ I_N^2 \to \{-1,+1\}} Q_1(\eta) \ll N^{1/2}.$$

(ii) If $k \in \mathbb{N}$, $k \geq 2$, then there is a number $N_0 = N_0(k)$ such that for $N \in \mathbb{N}$, $N > N_0$ we have

$$\min_{\eta:\ I_N^2 \to \{-1,+1\}} Q_k(\eta) \leq 9\sqrt{2} k^{1/2} N \log N. \tag{7.1}$$

(iii) For all $k, N \in \mathbb{N}$ *with* $2 \leq k \leq N$ *we have*

$$\min_{\eta:\ I_N^2 \to \{-1,+1\}} Q_k(\eta) \ll kN(\log N)^2. \tag{7.2}$$

Proof of Theorem 5. (i) This holds by the upper bound in Theorem 1.2 of Doerr, Srivastav and Wehr in [6], so that together with their lower bound (5.1), their results give the exact order of magnitude of $\min_\eta Q_1(\eta)$: it is $\asymp N^{1/2}$.

(ii) By the $n = 2$, $\varepsilon = \frac{1}{2}$ special case of the second half of Theorem 1 of Hubert, Mauduit and Sárközy in [12], choosing every $\eta :\ I_N^2 \to \{-1,+1\}$ with equal probability 2^{-N^2} we have

$$P\left(Q_k(\eta) > (81kN^2 \log N^2)^{1/2}\right) < \frac{1}{2}$$

so that at least half of these lattices satisfies

$$Q_k(\eta) \leq 9\sqrt{2}k^{1/2}N \log N$$

which proves (7.1).

(*iii*) Let p denote the smallest prime with $p \geq N$, and consider the p-lattice $\eta : I_p^2 \to \{-1, +1\}$ defined in formula (4.1) of Hubert, Mauduit and Sárközy in [12]. Then by Theorem 2 in [12] for all $k, N \in \mathbb{N}$ we have

$$Q_k(\eta) < kp(1 + \log p)^2. \tag{7.3}$$

Now truncate this p-lattice so that we keep only its first N-rows and N columns. Then we get an N-lattice $\eta : I_N^2 \to \{-1, +1\}$ which by (7.3) and Chebysev's theorem satisfies

$$Q_k(\eta) < kp(1 + \log p)^2 \ll kN(\log N)^2, \tag{7.4}$$

and this proves (7.2).

As in one dimension, while the order of magnitude of $\min Q_1$ is known, for fixed odd $k > 1$ there is a large gap between the lower bound (5.1) and the upper bound (7.1) for Q_k:

$$N^{1/2} \ll \min_{\eta:\ I_N^2 \to \{-1,+1\}} Q_k(\eta) \ll k^{1/2}N \log N \quad \text{(for fixed odd } k > 1). \tag{7.5}$$

Problem 3 *Tighten the gap between the lower and upper bounds in* (7.5)

In one dimension Gyarmati [8] and later Anantharam [3] proved theorems which seem to indicate that, perhaps, the upper bound in (2.15) is closer to the truth than the lower bound (2.14). In the next section we will prove the two dimensional analog of one of their theorem so that again the upper bound seems to be closer to the truth.

8 An inequality involving C_2 and C_3

Gyarmati [8] proved that if in one dimension $C_2(E_N) \ll N^{2/3}$, then $C_3(E_N) \gg N^{1/2}$. Later Anantharam [3] sharpened this result, and it follows from the proof of Theorem 4 in [3] that $C_3^2(E_N)C_2^3(E_N) \gg N^3$ if $C_3(E_N) \ll \sqrt{N}$. By adapting his method, we will prove the following two dimensional analog of this result:

Theorem 6 *If $\eta : I_N^2 \to \{-1,+1\}$ and $C_3(\eta) \le \frac{N}{13}$, then for $N > N_0$ we have*

$$C_3(\eta)^2 C_2(\eta)^3 \ge \frac{1}{576} N^6.$$

Proof of Theorem 6. Let $M \ge 1$ and $L \ge 1$ such that $3 \le L \le N - M + 1$, let $\eta : I_N^2 \to \{-1,+1\}$ and write

$$c_{\mathbf{d_1},\mathbf{d_2},\mathbf{d_3}} = \sum_{\mathbf{u} \in I_M^2} \eta(\mathbf{u}+\mathbf{d_1})\eta(\mathbf{u}+\mathbf{d_2})\eta(\mathbf{u}+\mathbf{d_3}).$$

Observe that

$$\begin{aligned}
\sum_{\mathbf{d_1}\in I_L^2}\sum_{\mathbf{d_2}\in I_L^2}\sum_{\mathbf{d_3}\in I_L^2} c^2_{\mathbf{d_1},\mathbf{d_2},\mathbf{d_3}} &= \sum_{\mathbf{d_1}\in I_L^2}\sum_{\mathbf{d_2}\in I_L^2}\sum_{\mathbf{d_3}\in I_L^2} \\
&\quad \left(\sum_{\mathbf{u}\in I_M^2} \eta(\mathbf{u}+\mathbf{d_1})\eta(\mathbf{u}+\mathbf{d_2})\eta(\mathbf{u}+\mathbf{d_3})\right)^2 \\
&= \sum_{\mathbf{d_1}\in I_L^2}\sum_{\mathbf{d_2}\in I_L^2}\sum_{\mathbf{d_3}\in I_L^2}\sum_{\mathbf{u}\in I_M^2}\sum_{\mathbf{v}\in I_M^2} \\
&\quad \eta(\mathbf{u}+\mathbf{d_1})\eta(\mathbf{u}+\mathbf{d_2})\eta(\mathbf{u}+\mathbf{d_3})\eta(\mathbf{v}+\mathbf{d_1})\eta(\mathbf{v}+\mathbf{d_2})\eta(\mathbf{v}+\mathbf{d_3}) \\
&= \sum_{\mathbf{u}\in I_M^2}\sum_{\mathbf{v}\in I_M^2}\left(\sum_{\mathbf{d}\in I_L^2}\eta(\mathbf{u}+\mathbf{d})\eta(\mathbf{v}+\mathbf{d})\right)^3 \\
&= \sum_{\mathbf{u}\in I_M^2}\left(\sum_{\mathbf{d}\in I_L^2}\eta(\mathbf{u}+\mathbf{d})\eta(\mathbf{u}+\mathbf{d})\right)^3 + \text{off diagonal terms} \\
&= M^2L^6 + \text{off diagonal terms}.
\end{aligned}$$

The total number of off-diagonal terms is $M^2(M^2-1) < M^4$. Suppose that $\mathbf{u}, \mathbf{v} \in I_M^2$, $\mathbf{u} \neq \mathbf{v}$. Then we have

$$\left| \sum_{\mathbf{d} \in I_L^2} \eta(\mathbf{u}+\mathbf{d})\eta(\mathbf{v}+\mathbf{d}) \right| \leq C_2(\eta).$$

It follows that the sum of the off-diagonal terms in the preceeding equation is at most $M^4 C_2^3(\eta)$, thus we have

$$\sum_{\mathbf{d_1} \in I_L^2} \sum_{\mathbf{d_2} \in I_L^2} \sum_{\mathbf{d_3} \in I_L^2} c^2_{\mathbf{d_1},\mathbf{d_2},\mathbf{d_3}} \geq M^2 L^6 - M^4 C_2^3(\eta).$$

On the other hand, we also have

$$\begin{aligned}\sum_{\mathbf{d_1} \in I_L^2} \sum_{\mathbf{d_2} \in I_L^2} \sum_{\mathbf{d_3} \in I_L^2} c^2_{\mathbf{d_1},\mathbf{d_2},\mathbf{d_3}} &= 6 \sum\nolimits^{*} c^2_{\mathbf{d_1},\mathbf{d_2},\mathbf{d_3}} + \sum\nolimits^{**} c^2_{\mathbf{d_1},\mathbf{d_2},\mathbf{d_3}} \\ &\leq L^2(L^2-1)(L^2-2)C_3(\eta)^2 + \sum\nolimits^{**} c^2_{\mathbf{d_1},\mathbf{d_2},\mathbf{d_3}} \\ &\leq L^6 C_3(\eta)^2 + \sum\nolimits^{**} c^2_{\mathbf{d_1},\mathbf{d_2},\mathbf{d_3}},\end{aligned}$$

where in $\sum^*$ we sum over all 3-element subsets $\{\mathbf{d_1}, \mathbf{d_2}, \mathbf{d_3}\}$ of I_L^2, while in $\sum^{**}$ we sum over the triples $\{\mathbf{d_1}, \mathbf{d_2}, \mathbf{d_3}\}$ such that at least two of them are equal. The number of terms in $\sum^{**}$ is $L^6 - L^2(L^2-1)(L^2-2) \leq 3L^4$, and each of them is bounded above by M^4. Thus we have

$$\sum_{\mathbf{d_1} \in I_L^2} \sum_{\mathbf{d_2} \in I_L^2} \sum_{\mathbf{d_3} \in I_L^2} c^2_{\mathbf{d_1},\mathbf{d_2},\mathbf{d_3}} \leq L^6 C_3(\eta)^2 + 3L^4 M^4.$$

Combining the upper bound with the previously proved lower bound we have

$$\begin{aligned} M^2 L^6 - M^4 C_2^3(\eta) &\leq L^6 C_3^2(\eta) + 3L^4 M^4, \\ M^2 L^6 &\leq L^6 C_3^2(\eta) + M^4 C_2^3(\eta) + 3L^4 M^4. \end{aligned}$$

Note that this inequality holds for all $M \geq 1$, $L \geq 1$ satisfying $3 \leq L \leq N - M + 1$ and for all η. Suppose that

$$C_3(\eta) \leq \frac{N}{13}. \tag{8.1}$$

We now set $M = 2C_3(\eta)$. Then

$$3C_3(\eta)^2 L^6 \leq 16 C_3^4(\eta) C_2^3(\eta) + 48 C_3^4(\eta) L^4.$$

We take $L = \left[\frac{N}{2}\right]$. Then for large enough N we have

$$\frac{3}{65} C_3(\eta)^2 N^6 \leq 16 C_3^4(\eta) C_2^3(\eta) + 3 C_3^4(\eta) N^4 \tag{8.2}$$

By (8.1)

$$3C_3^4(\eta) N^4 \leq 3 C_2^3(\eta) \frac{N^6}{169}.$$

Thus from (8.2)

$$\frac{1}{36} C_3(\eta)^2 N^6 < \left(\frac{3}{65} - \frac{3}{169}\right) C_3(\eta)^2 N^6 \leq 16 C_3^4(\eta) C_2^3(\eta),$$

$$\frac{1}{576} N^6 \leq C_3^2(\eta) C_2^3(\eta)$$

which was to be proved.

9 The normality measure

First we will prove the two dimensional analog of (2.11):

Theorem 7 *For $N \to \infty$ we have*

$$\min_{\eta:\ I_N^2 \to \{-1,+1\}} N(\eta) \geq \left(\frac{1}{2} + o(1)\right) \frac{\log N}{\log 2}. \tag{9.1}$$

Proof of Theorem 7. By the definition of the normality measure we have

$$N(\eta) \geq \max_{k \leq (\log N)/\log 2} \max_{X \in \mathcal{M}(k,1)} \max_{0 < U \leq N+1-k} \left| Z(\eta, U, 1, X) - \frac{U}{2^k} \right| \stackrel{\text{def}}{=} A. \tag{9.2}$$

Define a binary sequence $E_N = \{e_1, e_2, \ldots, e_N\}$ by

$$e_n = \eta(n-1, 0)$$

for $1 \leq n \leq N$. For $X = (x_{ij}) \in \mathcal{M}(k,1)$ let $Y = \{y_1, \ldots, y_k\}$ be defined by

$$y_i = x_{i1}$$

for $1 \le i \le k$. Then

$$A = \max_{k \le (\log N)/\log 2} \max_{Y \in \{-1,+1\}^k} \max_{0<U\le N+1-k} \left| T(E_N, U, Y) - \frac{U}{2^k} \right|$$
$$= \max_{k \le (\log N)/\log 2} N_k(E_N) = N(E_N). \tag{9.3}$$

It follows from (2.11), (9.2) and (9.3) that

$$N(\eta) \ge \left(\frac{1}{2} + o(1)\right) \frac{\log N}{\log 2},$$

which proves (9.1).

We have not been able to prove the two dimensional analogues of (2.10) and (2.12). We will prove a weaker estimate than (2.12):

Theorem 8 *For $N \in \mathbb{N}$ we have*

$$\min_{\eta:\ I_N^2 \to \{-1,+1\}} N(\eta) \ll N(\log N)^3. \tag{9.4}$$

Proof of Theorem 8. Consider again the binary N-lattice described in the proof of (iii) in Theorem 4. Then as we showed, (7.4) holds for all k. By Theorem 3 in [9] we have

$$N_{k,\ell}(\eta) \le \max_{1\le t\le k\ell} Q_t(\eta) \tag{9.5}$$

for $N, k, \ell \in \mathbb{N}$, $k < N$, $\ell < N$ and every binary lattice $\eta:\ I_N^2 \to \{-1,+1\}$. It follows from (7.4), (9.5) and the definition of the normality measure that for the lattice η described above we have

$$N(\eta) = \max_{k\ell \le (2\log N)/\log 2} N_{(k,\ell)}(\eta) \le \max_{k\ell \le (2\log N)/\log 2} \max_{1\le t\le k\ell} Q_t(\eta)$$
$$\ll \max_{1\le t\le k\ell} tN(\log N)^2 \ll N(\log N)^3$$

which proves (9.4).

There is a large gap between the lower bound (9.1) and the upper bound (9.4):

$$\left(\frac{1}{2} + o(1)\right) \frac{\log N}{\log 2} \ll \min_{\eta:\ I_N^2 \to \{-1,+1\}} N(\eta) \ll N(\log N)^3. \tag{9.6}$$

Problem 4 *Tighten the gap between the lower and upper bounds in* (9.6).

Since here the upper bounds is weaker, than in one dimension, one might like to answer the following question at least:

Problem 5 *Thus there exist a constant* $c < 1$ *such that*

$$\min_{\eta\colon\ I_N^2 \to \{-1,+1\}} N(\eta) \ll N^c?$$

References

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

[2] 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.

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

[4] J. Beck, *Roth's estimate on the discrepancy of integer sequences is nearly sharp*, Combinatorica 1 (1981), 319-325.

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

[6] B. Doerr, A. Srivastav, P. Wehr, *Discrepancy of Cartesian products of arithmetic progressions*, Electron. J. Comb. 11 (2004), no. 1, Research Paper 5, 16 pp. (electronic).

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

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

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

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

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

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

[13] Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, *Measures of pseudorandomness for finite sequences: minimum and typical values*, Proceedings of WORDS'03, 156-169, TUCS Gen. Publ., 27, Turku Cent. Comput. Sci., Turku 2003.

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

[15] J. Matoušek and J. Spencer, *Discrepancy in arithmetic progressions*, J. American Math. Soc. 9 (1996), 195-204.

[16] K. F. Roth, *Remark concerning integer sequences*, Acta Arith. 9 (1964), 257-260.

[17] A. Sárközy, *Some remarks concerning irregularities of distribution of sequences of integers in arithmetic progressions, IV*, Acta Math. Acad. Sci. Hungar. 30 (1977), 155-162.