Pseudorandom binary sequences and lattices

Katalin Gyarmati, Christian Mauduit, András Sárközy*

Abstract

The connection between the pseudorandomness of binary sequences and binary lattices (i.e., binary square matrices) is studied. From a binary N-lattice ($N \times N$ matrix) one can make a unique binary sequence of length N^2 by taking first the first row of the matrix, then continuing the sequence by the second row of the matrix, etc. One might like to answer the following question: is it true that if the binary sequence constructed in this way possesses strong pseudorandom properties, then the lattice also does? It is shown that the answer is negative; negative examples are presented, and the connection between the pseudorandom measures of the sequence and the lattice is analyzed.

2000 Mathematics Subject Classification: 11K45.

Key words and phrases: pseudorandom, binary lattice, concatenation.

1 Introduction

Pseudorandom binary sequences play a role of basic importance in applications, in particular, in cryptography. The notion of pseudorandomness is usually defined in terms of computational complexity (see, e.g., [8]). This approach has certain weak points, thus Mauduit and Sárközy [4] initiated another, more constructive approach (see [10] for a survey of the related work and for the comparison of the two approaches).

*Research partially supported by Hungarian National Foundation for Scientific Research, Grants K49693, K67676 and K72264, French-Hungarian exchange program F-06/48, and the János Bolyai Research Fellowship.

In the applications (e.g., in connection with image or bit map encryption) one also needs the multidimensional extension of this theory. Thus Hubert, Mauduit and Sárközy [3], [5], [6] extended the constructive theory of pseudorandom binary sequences to the multidimensional situation by studying pseudorandom binary lattices. It turns out that the multidimensional case is much more difficult than the one dimensional case; it takes a considerable effort to generalize the one dimensional methods, results and constructions, and in the most cases only much weaker partial results are achieved. Thus it is a natural question to ask: does one really need the multidimensional theory? Can one not utilize the simpler and more effective one dimensional theory in the multidimensional case? Are there no simple and cheap but, in the same time relatively satisfactory ways to convert the one dimensional results and constructions into multidimensional ones? In general, what is the connection between the one dimensional and multidimensional cases? In this paper our goal is to study these questions. More precisely, since the 2 dimensional case is simpler and more important than the 3 or higher dimensional cases, thus we will restrict ourselves to the study of the links between the one dimensional and two dimensional cases. However, with a little work our results and constructions could be extended to higher dimensions.

2 Some basic definitions and results in one, resp. n dimensions

In [4] Mauduit and Sárközy studied finite binary sequences

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

They introduced the following measures of pseudorandomness of binary sequences of this form: the *well-distribution measure* of the sequence (2.1) 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 $1 \le a \le a + (t-1)b \le N$, and the *correlation measure of order k* of E_N is defined as

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

where the maximum is taken over all $\underline{D} = (d_1, \dots, d_k)$ 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:

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

where the maximum is taken over all a, t and $\underline{D} = (d_1, d_2, \ldots, d_k)$ with $d_1 < d_2 < \cdots < d_k$ such that all the subscripts $ja+d_\ell$ belong to $\{1, \ldots, N\}$. (Note that clearly $Q_1(E_N) = W(E_N)$.) Then the sequence E_N is considered to be a "good" pseudorandom sequence if $W(E_N)$ and, for "small" k, both $C_k(E_N)$ and $Q_k(E_N)$ are "small" in terms of N (in particular, both are $o(N)$ as $N \to \infty$.) Indeed, later Cassaigne, Mauduit and Sárközy [2] showed that this terminology is justified since for fixed k for almost all $E_N \in \{-1, +1\}^N$, the measures $W(E_N), C_k(E_N)$ and $Q_k(E_N)$ are less than $N^{1/2}(\log N)^c$, where the constant c depends on k (see also [1]). It was also shown in [4] that the Legendre symbol forms a "good" pseudorandom binary sequence:

Theorem A *There is a number p_0 such that if $p > p_0$ is a prime number, $k \in \mathbb{N}$, $k < p$ and if we write*

$$E_{p-1} = \left(\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \ldots, \left(\frac{p-1}{p}\right) \right)$$

(where $\left(\frac{n}{p}\right)$ denotes the Legendre symbol), then

$$Q_k(E_{p-1}) \leq 9kp^{1/2} \log p.$$

The crucial tool in the proof of this theorem was the following consequence of Weil's theorem [12]:

Lemma 1 *Suppose that p is a prime number, χ is a non-principal character modulo p of order d (so that $d \mid p-1$), $f(x) \in \mathbb{F}_p[x]$ ($\mathbb{F}_p$ being the field of modulo p residue classes) has degree k and factorization $f(x) = b(x-x_1)^{d_1} \cdots (x-x_s)^{d_s}$ (where $x_i \neq x_j$ for $i \neq j$) in $\overline{\mathbb{F}}_p$ (the algebraic closure of $\mathbb{F}_p$) with*

$$(d, d_1, \ldots, d_s) = 1. \tag{2.2}$$

Let X, Y be real numbers with $0 < Y \leq p$. Then

$$\left| \sum_{X < n \leq X+Y} \chi(f(n)) \right| < 9kp^{1/2} \log p.$$

Note that the same conclusion also holds if assumption (2.2) on $f(x)$ is replaced by

$$f(x) \text{ is not of the form } cg(x)^d \text{ with } c \in \mathbb{F}_p,\ g(x) \in \mathbb{F}_p[x] \tag{2.3}$$

(see [7], [11]).

In [3] Hubert, Mauduit and Sárközy extended this constructive theory of pseudorandomness from one dimension to n dimensions (see also [5], [6]). Let I_N^n denote the set of the n-dimensional vectors all whose coordinates are selected from the set $\{0, 1, \ldots, N-1\}$:

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

We call this set *n-dimensional N-lattice* or briefly (if n is fixed) *N-lattice*. A function of the type

$$\eta(\underline{x}) : \ I_N^n \to \{-1, +1\} \tag{2.4}$$

is called *n-dimensional binary N-lattice* or briefly *binary lattice*. (Note that in the $n = 1$ special case these functions are the binary sequences $E_N \in \{-1, +1\}^N$.) In [3] the use of the following measures of pseudorandomness of binary lattices was proposed: if $\eta = \eta(\underline{x})$ is an n-dimensional binary N-lattice of form (2.4), $k \in \mathbb{N}$, and $\underline{u}_i$ $(i = 1, 2, \ldots, n)$ denotes the n-dimensional unit vector whose i-th coordinate is 1 and the other coordinates are 0, then write

$$Q_k(\eta) = \max_{\underline{B}, \underline{d}_1, \ldots, \underline{d}_k, \underline{T}} \Bigg| \sum_{j_1=0}^{t_1} \cdots \sum_{j_n=0}^{t_n} \eta(j_1 b_1 \underline{u}_1 + \cdots + j_n b_n \underline{u}_n + \underline{d}_1) \cdots \\ \eta(j_1 b_1 \underline{u}_1 + \cdots + j_n b_n \underline{u}_n + \underline{d}_k) \Bigg|$$

where the maximum is taken over all n-dimensional vectors $\underline{B} = (b_1, \ldots, b_n)$, $\underline{d}_1, \ldots, \underline{d}_k$, $\underline{T} = (t_1, \ldots, t_n)$ such that their coordinates are non-negative integers, $b_1, \ldots, b_n$ are non-zero, $\underline{d}_1, \ldots, \underline{d}_k$ are distinct, and all the points $j_1 b_1 \underline{u}_1 + \cdots + j_n b_n \underline{u}_n + \underline{d}_i$ occurring in the multiple sum belong to the n-dimensional N-lattice I_N^n. Then $Q_k(\eta)$ is called the *pseudorandom* (briefly PR) measure of order k of η. (Note that in the one-dimensional special case $Q_k(\eta)$ is the combined PR-measure Q_k of order k.)

It was proved in [3] that for a fixed $k \in \mathbb{N}$ and for a truly random n-dimensional binary N-lattice $\eta(\underline{x})$ we have

$$N^{n/2} \ll Q_k(\eta) \ll N^{n/2} (\log N^n)^{1/2}$$

with probability $> 1 - \varepsilon$, while the trivial upper bound for $Q_k(\eta)$ is N^n. Thus an n-dimensional binary N-lattice η can be considered as a "good" pseudorandom lattice if the PR measure of order k of η is "small" in terms of N (in particular, $Q_k(\eta) = o(N^n)$ for fixed n and $N \to \infty$) for small k.

Moreover in [3] an example was given (by using the quadratic character of a finite field) for a "good" n-dimensional binary lattice (for any n).

In the rest of the paper we will restrict ourselves to the $n = 2$ special case, i.e., to two dimensional binary lattices.

3 Binary lattices whose rows are "good" PR binary sequences

Suppose we want to construct a "good" PR two dimensional lattice. As we have mentioned earlier, it is easier to construct binary sequences than binary lattices. Thus one might like to construct a binary lattice by combining binary sequences. More precisely, assume that a sequence of "good" PR binary sequences $E_N^{(1)}, E_N^{(2)}, \dots, E_N^{(j)} = (e_1^{(j)}, e_2^{(j)}, \dots, e_N^{(j)}), \dots$ is given; then it is a natural idea is to consider the two dimensional binary lattice η whose j-th row is the vector $E_N^{(j)}$ as a candidate for being a "good" PR two dimensional binary lattice, i.e.,

$$\eta((i, j-1)) = e_{i+1}^{(j)} \text{ for } j = 1, 2, \dots, N, \; i = 0, 1, \dots, N-1. \tag{3.1}$$

If, say, $E_N^{(1)} = E_N^{(2)} = \dots = E_N^{(N)}$, then the binary lattice η is certainly not of PR type. Thus in order to ensure the pseudorandomness of η one needs an assumption on the connection between the sequences $E_N^{(j)}$. A natural assumption of this type is that the vectors $E_N^{(j)}$ are near orthogonal, i.e., the scalar products $(E_N^{(i)}, E_N^{(j)})$ are "small":

$$\left|(E_N^{(i)}, E_N^{(j)})\right| = \left|e_1^{(i)} e_1^{(j)} + e_2^{(i)} e_2^{(j)} + \dots + e_N^{(i)} e_N^{(j)}\right| \text{ is "small" for } 1 \le i < j \le N. \tag{3.2}$$

So the question is: if $E_N^{(1)}, E_N^{(2)}, \dots, E_N^{(N)}$ are "good" PR binary sequences, and (3.2) also holds, then does this imply that the lattice η in (3.1) is a "good" PR binary lattice? We will show by an example that the answer to this question is negative. This example shows clearly that from "good" PR binary sequences we cannot construct a "good" lattice in this manner.

Theorem 1 *Let p be a prime number, and for $j = 1, 2, \dots, p$ define the binary sequence $E_p^{(j)} = (e_1^{(j)}, e_2^{(j)}, \dots, e_p^{(j)})$ by*

$$e_i^{(j)} = \begin{cases} \left(\frac{i+j}{p}\right) & \text{for } p \nmid i+j, \\ +1 & \text{for } p \mid i+j. \end{cases}$$

Define the binary lattice η *by* (3.1) *(with* p *in place of* N*) so that, for* $(x,y) \in \{0,1,\dots,p-1\}^2$,

$$\eta((x,y)) = e_{x+1}^{(y+1)} = \begin{cases} \left(\frac{x+y+2}{p}\right) & \text{for } p \nmid x+y+2, \\ +1 & \text{for } p \mid x+y+2. \end{cases}$$

Then for $k \in \mathbb{N},\ k < p,\ j = 1,2,\dots,p$ *we have*

$$Q_k(E_p^{(j)}) < 10kp^{1/2}\log p \tag{3.3}$$

(so that $E_p^{(1)}, E_p^{(2)}, \dots, E_p^{(p)}$ *are "good" PR binary sequences) and*

$$\left|(E_p^{(i)}, E_p^{(j)})\right| < 4p^{1/2} \text{ for } 1 \le i < j \le p \tag{3.4}$$

(so that (3.2) *also holds), however, we have*

$$Q_2(\eta) \ge (p-1)^2. \tag{3.5}$$

Proof. Denote the quadratic character of $\mathbb{F}_p$ by χ^*:

$$\chi^*(n) = \begin{cases} \left(\frac{n}{p}\right) & \text{for } p \nmid n, \\ 0 & \text{for } p \mid n. \end{cases}$$

Then we have

$$\begin{aligned} Q_k(E_p^{(j)}) &= \max_{a,t,\underline{D}} \left| \sum_{i=0}^{t} e_{ia+d_1}^{(j)} \cdots e_{ia+d_k}^{(j)} \right| \\ &\le \max_{a,t,\underline{D}} \left(\left| \sum_{\substack{0 \le i \le t \\ p \nmid (j+ia+d_1)\cdots(j+ia+d_k)}} \left(\frac{(j+ia+d_1)\cdots(j+ia+d_k)}{p} \right) \right| \right. \\ &\quad \left. + \sum_{\substack{0 \le i \le t \\ p \mid (j+ia+d_1)\cdots(j+ia+d_k)}} 1 \right) \\ &\le \max_{a,t,\underline{D}} \left(\left| \sum_{i=0}^{t} \chi^*((j+ia+d_1)\cdots(j+ia+d_k)) \right| + k \right) \end{aligned}$$

whence by Lemma 1, (3.3) follows.

Moreover, for $1 \le i < j \le p$ we have

$$\begin{aligned} \left|(E_p^{(i)}, E_p^{(j)})\right| &= \left| \sum_{\ell=1}^{p} e_\ell^{(i)} e_\ell^{(j)} \right| \le \left| \sum_{\substack{1 \le \ell \le p \\ p \nmid (\ell+i)(\ell+j)}} \left(\frac{(\ell+i)(\ell+j)}{p} \right) \right| + \sum_{\substack{1 \le \ell \le p \\ p \mid (\ell+i)(\ell+j)}} 1 \\ &\le \left| \sum_{\ell=1}^{p} \chi^*((\ell+i)(\ell+j)) \right| + 2. \end{aligned} \tag{3.6}$$

It follows from Weil's theorem [12] (see also Lemma 2C in [11]) that the first sum is $\leq 2p^{1/2}$. Thus (3.4) follows from (3.6).

Finally it follows from the definition of $Q_k(\eta)$ that

$$Q_2(\eta) \geq \left| \sum_{j_1=0}^{p-2} \sum_{j_2=1}^{p-1} \eta((j_1, j_2) + (0,0)) \eta\left((j_1, j_2) + (+1, -1)\right) \right|$$
$$= \left| \sum_{j_1=0}^{p-2} \sum_{j_2=1}^{p-1} \eta((j_1, j_2)) \eta\left((j_1 + 1, j_2 - 1)\right) \right|. \tag{3.7}$$

We have

$$\eta((j_1, j_2)) \eta\left((j_1 + 1, j_2 - 1)\right) = \left(\frac{j_1 + j_2 + 2}{p}\right)\left(\frac{j_1 + j_2 + 2}{p}\right)$$
$$= +1 \text{ for } p \nmid j_1 + j_2 + 2$$

and

$$\eta((j_1, j_2)) \eta\left((j_1 + 1, j_2 - 1)\right) = (+1)(+1) = +1 \text{ for } p \mid j_1 + j_2 + 2$$

so that, from (3.7)

$$Q_2(\eta) \geq \sum_{j_1=0}^{p-2} \sum_{j_2=1}^{p-1} 1 = (p-1)(p-1) = (p-1)^2$$

which proves (3.5) and this completes the proof of Theorem 1.

Remark 1 We note that the construction presented in Theorem 1 is a special case of a more general construction: Let $E_N^{(1)} = \{e_1^{(1)}, e_2^{(1)}, \dots, e_N^{(1)}\} \in \{-1, +1\}^N$ be a truly random binary sequence, and for $2 \leq j \leq n$ let $E_N^{(j)}$ be a translated version of $E_N^{(1)}$, so $E_N^{(j)} = \{e_1^{(j)}, e_2^{(j)}, \dots, e_N^{(j)}\} = \{e_j^{(1)}, e_{j+1}^{(1)}, \dots, e_N^{(1)}, e_1^{(1)}, e_2^{(1)}, \dots, e_{j-1}^{(1)}\}$. Then the $E_N^{(j)}$'s satisfy inequalities of type (3.3) and (3.4) (with N in place of p and with upper bounds $O\left(N^{1/2}(\log N)^c\right)$) with probability 1. Define the lattice η by

$$\eta(x, y) = e_{x+1}^{(y+1)} = e_{r_N(x+y+1)}^{(1)}, \text{ (for } (x, y) \in \{0, 1, \dots, p-1\}^2)$$

where $r_N(x + y + 1)$ denotes the least positive residue of $x + y + 1$ modulo N. Similarly to (3.7) we easily get

$$Q_2(\eta) \geq (N-1)^2.$$

In Theorem 1 we presented a special case of the above construction, where $E_N^{(1)}$ was defined by the Legendre symbol, and then indeed (3.3) and (3.4) hold.

4 Trying to reduce the two dimensional case to the one dimensional one: the PR measures of order 1

The simplest and more natural way to reduce the two dimensional case to the one dimensional one is the following:

To any 2-dimensional binary N-lattice

$$\eta(\underline{x}) : \ I_N^2 \to \{-1, +1\} \tag{4.1}$$

we may assign a unique binary sequence $E_{N^2} = E_{N^2}(\eta) = (e_1, e_2, \dots, e_{N^2}) \in \{-1, +1\}^N$ by taking the first (from the bottom) row of the lattice (4.1) then we continue the binary sequence by taking the second row of the lattice, then the third row follows, etc.; in general, we set

$$e_{iN+j} = \eta((j-1, i)) \text{ for } i = 0, 1, \dots, N-1, \ j = 1, 2, \dots, N. \tag{4.2}$$

It is a natural question to ask: is it true that if $E_{N^2}(\eta)$ is a "good" PR binary *sequence* then η is a "good" PR 2-dimensional lattice? Namely, then "good" PR binary *sequences* would generate "good" PR-binary lattices automatically, thus it would be sufficient to study binary sequences, there would be no need for developing a theory of pseudorandomness of binary lattices. Unfortunately, the answer to this question is negative; we will show in sections 4 and 5 that it may occur that the PR measures of sequence $E_{N^2}(\eta)$ are small, however, the corresponding PR-measures of the lattice η are large.

We will denote the PR measures of $E_{N^2}(\eta)$ by W, C_k, Q_k, while we write $\overline{Q}_k$ for the pseudorandom measure of order k of η. First we will compare the PR measures of order 1, i.e., $Q_1 = W$ and $\overline{Q}_1$.

Theorem 2 *For every even number $N = 2R \in \mathbb{N}$ there is a binary lattice η such that $Q_1(E_{N^2}(\eta))$ is "small":*

$$Q_1(E_{N^2}(\eta)) = W(E_{N^2}(\eta)) < 4N, \tag{4.3}$$

however, $\overline{Q}_1(\eta)$ is large:

$$\overline{Q}_1(\eta) > \frac{1}{2}N^2. \tag{4.4}$$

Proof. Define the N-lattice of of type (4.1) by

$$\eta((i,j)) = \begin{cases} +1 & \text{for } i = 0, 1, \dots, R-1 \text{ and } j = 0, 1, \dots, N-1, \\ -1 & \text{for } i = R, R+1, \dots, N-1 \text{ and } j = 0, 1, \dots, N-1. \end{cases}$$

We will show that this lattice η satisfies (4.3) and (4.4).

By the definition of W and Q_1 we have

$$Q_1(E_{N^2}(\eta)) = W(E_{N^2}(\eta)) = \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right|$$

where the maximum is taken over all $a, b, t \in \mathbb{N}$ with $1 \le a \le a+(t-1)b \le N^2$. Take one of the sums $\sum_{j=0}^{t-1} e_{a+jb}$ considered here. There are unique integers u, v with

$$0 \le u \le v \le N-1,$$

$$a \in (uN, uN+N],$$

$$a+(t-1)b \in (vN, vN+N].$$

Then we have

$$\sum_{j=0}^{t-1} e_{a+jb} = \sum_{\substack{0\le j\le t-1 \\ a+jb\in(uN,(u+1)N]}} e_{a+jb} + \sum_{u<w<v} \sum_{\substack{0\le j\le t \\ a+jb\in(wN,(w+1)N]}} e_{a+jb}$$
$$+ \sum_{\substack{0\le j\le t-1 \\ a+jb\in(vN,(v+1)N]}} e_{a+jb} \tag{4.5}$$

Clearly

$$\left| \sum_{\substack{0\le j\le t-1 \\ a+jb\in(uN,(u+1)N]}} e_{a+jb} \right| \le \sum_{a+jb\in(uN,(u+1)N]} 1 \le N, \tag{4.6}$$

$$\left| \sum_{\substack{0\le j\le t-1 \\ a+jb\in(vN,(v+1)N]}} e_{a+jb} \right| \le \sum_{a+jb\in(vN,(v+1)N]} 1 \le N \tag{4.7}$$

and, for $u < w < v$, by the definition of η and E_{N^2},

$$\left|\sum_{j:\ a+jb\in(wN,(w+1)N]} e_{a+jb}\right| = \left|\sum_{j:\ a+jb\in(wN,wN+R]} \eta((a+jb-wN-1,w))\right.$$

$$\left. + \sum_{j:\ a+jb\in(wN+R,(w+1)N]} \eta((a+jb-wN-1,w))\right|$$

$$= \left|\sum_{j:\ a+jb\in(wN,wN+R]} 1 - \sum_{j:\ a+jb\in(wN+R,(w+1)N]} 1\right|$$

$$= \big|\, |\{m:\ m\equiv a \pmod b,\ wN < m \le wN+R\}|$$

$$- |\{m:\ m\equiv a \pmod b,\ wN+R < m \le (w+1)N\}|\,\big|$$

$$= |(|\{m:\ m\equiv a \pmod b,\ wN < m \le wN+R\}| - R/b)$$

$$- (|\{m:\ m\equiv a \pmod b,\ wN+R < m \le (w+1)N\}| - R/b)|$$

$$\le 1+1 = 2. \tag{4.8}$$

It follows from (4.5), (4.6), (4.7) and (4.8) that

$$\left|\sum_{j=0}^{t-1} e_{a+jb}\right| \le N + 2(v-u-1) + N < 4N$$

which proves (4.3).

On the other hand, we have

$$\overline{Q}_1(\eta) \ge \left|\sum_{j_1=0}^{R-1}\sum_{j_2=0}^{N-1} \eta((j_1,j_2))\right| = \sum_{j_1=0}^{R-1}\sum_{j_2=0}^{N-1} 1 = RN = \frac{1}{2}N^2$$

which proves (4.4).

Remark 2 It is easy to see that in the example above we have

$$Q_2(E_{N^2}(\eta)) \ge C_2(E_{N^2}(\eta)) \gg N^2.$$

One might like to give a construction where we also have $Q_2(E_{N^2})(\eta) = o(N^2)$ or at least $C_2(E_{N^2})(\eta) = o(N^2)$. We have not be able to give such a construction. So we arrive to the following natural question:

Problem 1 *Is it true that*

$$C_2(E_{N^2})(\eta) = o(N^2) \ \Rightarrow\ \overline{Q}_1(\eta) = o(N^2)?$$

5 Trying to reduce the two dimensional case to the one dimensional case: the PR measures of order 2

One might like to save the above idea on reducing the two dimensional case to the one dimensional one by also considering the PR measures of order 2. So one may ask the question: is it true that if $W(E_{N^2}(\eta))$ and $C_2(E_{N^2}(\eta))$ are small, then η must be a "good" PR binary lattice? Again, the answer is negative:

Theorem 3 *For every even number $N = 2R \in \mathbb{N}$ there is a binary lattice η such that $Q_1(E_{N^2}(\eta))$ and $C_2(E_{N^2}(\eta))$ are small:*

$$Q_1(E_{N^2}(\eta)) = W(E_{N^2}(\eta)) < 6N(\log N)^{1/2} \tag{5.1}$$

and

$$C_2(E_{N^2}(\eta)) < 12N(\log N)^{1/2}, \tag{5.2}$$

however, $\overline{Q}_2(\eta)$ is large:

$$\overline{Q}_2(\eta) \geq \frac{1}{4}N^2. \tag{5.3}$$

Proof. We will present a probabilistic construction, more precisely we will consider all the binary N-lattices η satisfying certain conditions and chosen with equal probability, and then we will show that for $\varepsilon > 0$ and $N > N_0(\varepsilon)$, such a lattice η satisfies (5.1), resp. (5.2) with probability greater than $1 - \varepsilon$, and all these lattices η also satisfy (5.3).

Define the N-lattice η so that
(i) for $0 \leq x \leq N-1$, $0 \leq y \leq R-1$ the numbers $\eta(x, y)$ are independent random variables with distribution

$$P(\eta(x, y) = +1) = P(\eta(x, y) = -1) = 1/2, \tag{5.4}$$

moreover, we have
(ii) $\eta(x, y) = -\eta(x, y-R)$ for $R \leq x \leq N-1,\ R \leq y \leq N-1$ and
(iii) $\eta(x, y) = \eta(x, y-R)$ for $0 \leq x \leq R-1,\ R \leq y \leq N-1$.
The structure of this binary lattice η is the following:

Y	-Z
Y	Z

Then defining the binary sequence $E_{N^2} = E_{N^2}(\eta) = (e_1, e_2, \ldots, e_{N^2})$ by (4.2), it is easy to check that $e_1, e_2, \ldots, e_{N^2}$ posses the following properties:

(P1) For $n = 1, 2, \ldots, N^2$ the number e_n is a random variable with distribution

$$P(e_n = +1) = P(e_n = -1) = 1/2.$$

(P2) If $1 \le n < n + d \le N^2$ and $d \ne RN$, then the random variables e_n and e_{n+d} are independent.

(P3) If $1 \le n < n+d \le N^2$, $d = RN$, and we write n in the form $iN + j$ with $i \in \{0, 1, \ldots, R-1\}$, $j \in \{1, 2, \ldots, N\}$, then we have

$$e_{n+d} = e_n \text{ for } 1 \le j \le R$$

and

$$e_{n+d} = -e_n \text{ for } R < j \le N (= 2R).$$

We will denote the mean value and standard deviation of the random variable ξ by $M(\xi)$ and $D(\xi)$, respectively. We will need Bernstein's inequality [9, Ch.7]:

Lemma 2 *If $\xi_1, \ldots, \xi_m$ are independent random variables with $M(\xi_k) = M_k$, $D(\xi_k) = D_k$ and $|\xi_k - M_k| \le K$ for $(k = 1, 2, \ldots, m)$, then, writing $\xi = \xi_1 + \cdots + \xi_m$, $M = M_1 + \cdots + M_m$ and $D = (D_1^2 + \cdots + D_m^2)^{1/2}$, for any positive number μ with $\mu \le \frac{D}{K}$ we have*

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

To estimate $W(E_{N^2}(\eta))$, fix positive integers a, b, t with $1 \le a \le a + (t-1)b \le N^2$, and consider the sum

$$S(a, b, t) = \sum_{j=0}^{t-1} e_{a+jb}.$$

Denote by t^* the largest integer for which

$$a + (t^* - 1)b < \frac{N^2}{2}.$$

Let

$$S_1(a, b, t) = \sum_{j=0}^{t^*-1} e_{a+jb}, \quad S_2(a, b, t) = \sum_{j=t^*}^{t-1} e_{a+jb}.$$

Then

$$S(a, b, t) = S_1(a, b, t) + S_2(a, b, t).$$

By properties (P1) and (P2) we may use Lemma 2 with $e_{a+(k-1)b}$ in place of ξ_k for $k = 1, \ldots, t^*$ and for $k = t^* + 1, \ldots, t$ so that now $M_k = 0$, $D_k = \frac{1}{2}$,

$K = \frac{1}{2}$, $M = 0$ and in the first case $D = \frac{1}{2}t^{*1/2}$ and in the latter case $D = \frac{1}{2}\left(t - t^*\right)^{1/2}$. Then using Lemma 2 with $\mu = 12(\log N)^{1/2}$ we easily get

$$P\left(|S_1(a,b,t)| > 6N(\log N)^{1/2}\right) < \frac{1}{2N^8},$$
$$P\left(|S_2(a,b,t)| > 6N(\log N)^{1/2}\right) < \frac{1}{2N^8}$$

uniformly in a, b, t for $N > N_0$. By this and the triangle-inequality we get

$$P\left(|S(a,b,t)| > 12N(\log N)^{1/2}\right) \le P\left(|S_1(a,b,t)| > 6N(\log N)^{1/2}\right) + P\left(|S_2(a,b,t)| > 6N(\log N)^{1/2}\right) \le \frac{1}{N^8}.$$

Thus we have

$$\begin{aligned} P(W(E_{N^2}) > 12N\left(\log N\right)^{1/2}) &= P\left(\max_{a,b,t} |S(a,b,t)| > 12N(\log N)^{1/2}\right) \\ &\le \sum_{a,b,t} P\left(|S(a,b,t)| > 12N(\log N)^{1/2}\right) \\ &\le \sum_{1 \le a,b,t \le N^2} \frac{1}{N^8} = \frac{1}{N^2}. \end{aligned} \tag{5.5}$$

Now we will estimate $C_2(E_{N^2}(\eta))$

$$C_2(E_{N^2}(\eta)) = \max_{L,d_1,d_2} \left| \sum_{n=1}^{L} e_{n+d_1} e_{n+d_2} \right| = \max_{U,V,d} \left| \sum_{n=U}^{V} e_n e_{n+d} \right| \tag{5.6}$$

where the maximum is taken over all U, V, d with $1 \le U \le V < V + d \le N^2$. Consider one of these sums $\sum_{n=U}^{V} e_n e_{n+d}$. We have to distinguish two cases.

CASE 1. Assume first that

$$d \ne RN. \tag{5.7}$$

Define the sets $\mathcal{A}_1$ and $\mathcal{A}_2$ by

$$\mathcal{A}_1 = \{U, U+1, \ldots, V\} \cap_{k=0}^{+\infty} \{2kd+1, 2kd+2, \ldots, (2k+1)d\}$$

and

$$\mathcal{A}_2 = \{U, U+1, \ldots, V\} \cap_{k=0}^{+\infty} \{(2k+1)d+1, (2k+1)d+2, \ldots, (2k+2)d\}$$

so that we have

$$\begin{aligned} \left| \sum_{n=U}^{V} e_n e_{n+d} \right| &= \left| \sum_{n \in \mathcal{A}_1} e_n e_{n+d} + \sum_{n \in \mathcal{A}_2} e_n e_{n+d} \right| \le \left| \sum_{n \in \mathcal{A}_1} e_n e_{n+d} \right| + \left| \sum_{n \in \mathcal{A}_2} e_n e_{n+d} \right| \\ &= \left| \sum\nolimits_1 \right| + \left| \sum\nolimits_2 \right|, \end{aligned} \tag{5.8}$$

say. It follows from the properties (P1), (P2) and (5.7) that the terms of the $\sum_1$ are independent random variables of distribution

$$P(e_n e_{n+d} = +1) = P(e_n e_{n+d} = -1) = \frac{1}{2} \text{ (for } n \in \mathcal{A}_1).$$

Thus the terms of the sum $\sum_1$ can be estimated by using Lemma 2 (in the same way as we did in the estimate of $W(E_{N^2})$). We obtain for large N that

$$P\left(\left|\sum\nolimits_1\right| > 6N(\log N)^{1/2}\right) < \frac{1}{2N^8}. \tag{5.9}$$

for $N > N_0$. In the same way we get

$$P\left(\left|\sum\nolimits_2\right| > 6N(\log N)^{1/2}\right) < \frac{1}{2N^8}. \tag{5.10}$$

It follows from (5.8), (5.9) and (5.10) that for every U, V and d (satisfying (5.7)) we have

$$\begin{aligned} P\left(\left|\sum_{n=U}^{V} e_n e_{n+d}\right| > 12N(\log N)^{1/2}\right) &\le P\left(\left|\sum\nolimits_1\right| > 6N(\log N)^{1/2}\right) \\ &\quad + P\left(\left|\sum\nolimits_2\right| > 6N(\log N)^{1/2}\right) \\ &< \frac{1}{2N^8} + \frac{1}{2N^8} = \frac{1}{N^8} \end{aligned}$$

whence

$$\begin{aligned} &P\left(\max_{U,V,d\neq RN}\left|\sum_{n=U}^{V} e_n e_{n+d}\right| > 12N(\log N)^{1/2}\right) \\ &\le \sum_{U,V,d\neq RN} P\left(\left|\sum_{n=U}^{V} e_n e_{n+d}\right| > 12N(\log N)^{1/2}\right) < \sum_{U,V,d\neq RN} \frac{1}{N^8} \\ &\le \left(N^2\right)^3 \frac{1}{N^8} = \frac{1}{N^2} \text{ (for } N > N_0). \end{aligned} \tag{5.11}$$

CASE 2. Assume that

$$d = RN. \tag{5.12}$$

Let K_1 and K_2 denote the smallest and greatest integer K with

$$(KN, (K+1)N] \cap [U, V] \neq 0$$

respectively. Then by property (P3) and (5.12) we have

$$\begin{aligned}
\left|\sum_{n=U}^{V} e_n e_{n+d}\right| &= \left|\sum_{n=U}^{(K_1+1)N} e_n e_{n+d} + \sum_{K=K_1+1}^{K_2-1} \sum_{n=KN+1}^{(K+1)N} e_n e_{n+d} + \sum_{n=K_2N+1}^{V} e_n e_{n+d}\right| \\
&\le \left|\sum_{n=U}^{(K_1+1)N} 1\right| + \sum_{K=K_1+1}^{K_2-1} \left|\sum_{n=KN+1}^{KN+R} e_n e_{n+d} + \sum_{n=KN+R+1}^{(K+1)N} e_n e_{n+d}\right| \\
&+ \left|\sum_{n=K_2N+1}^{V} 1\right| \le N + \sum_{K=K_1+1}^{K_2-1} \left|\sum_{n=KN+1}^{KN+R} 1 + \sum_{n=KN+R+1}^{(K+1)N} (-1)\right| + N \\
&= 2N \text{ (for } d = RN). \qquad (5.13)
\end{aligned}$$

Finally, by (ii) we have

$$\begin{aligned}
\overline{Q}_2(\eta) &\ge \left|\sum_{j_1=0}^{R-1}\sum_{j_2=0}^{R-1} \eta((j_1,j_2)+(0,0))\eta((j_1,j_2)+(0,R))\right| \\
&= \left|\sum_{j_1=0}^{R-1}\sum_{j_2=0}^{R-1} \eta((j_1,j_2))^2\right| = \sum_{j_1=0}^{R-1}\sum_{j_2=0}^{R-1} 1 = R^2 = \frac{1}{4}N^2. \qquad (5.14)
\end{aligned}$$

By (5.5), (5.11) and (5.13), for $N \ge N_0(\varepsilon)$ both (5.1) and (5.2) hold with probability greater than $1-\varepsilon$, and by (5.14) for all lattices η considered (5.3) also holds, and this completes the proof of Theorem 3.

Remark 3 In Theorem 3 we could have replaced $C_2(E_{N^2})$ by $Q_2(E_{N^2})$ but this would have been lengthier, thus we preferred to present this simpler version. It is easy to see that in the construction of Theorem 3 we have

$$Q_4(E_{N^2}(\eta)) \ge C_4(E_{N^2}(\eta)) \gg N^2.$$

Thus one might like to answer the following question:

Problem 2 *Is it true that $Q_4(E_{N^2}(\eta)) = o(N^2)$ implies $\overline{Q}_2(\eta) = o(N^2)$?*

Remark 4 Theorem 3 could be extended from $C_2(E_{N^2})$ to $C_k(E_{N^2})$ (and beyond that to $Q_k(E_{N^2})$) by using the following generalization of our construction: Let $N = 2kR$ where $k, R \in \mathbb{N}$. Define the N-lattice η so that
(i) for $0 \le x \le N-1$, $0 \le y \le (2k-2)R-1$ the numbers $\eta(x,y)$ are independent random variables with distribution

$$P(\eta(x,y) = +1) = P(\eta(x,y) = -1) = 1/2,$$

moreover we define
(ii) $\eta(x,y) = \prod_{i=1}^{k-1} \eta((x, y-2iR))$

for $0 \le x \le kR-1,\ (2k-2)R \le y \le N-1$ and

(iii) $\eta(x,y) = -\prod_{i=1}^{k-1} \eta((x, y-2iR))$

for $kR \le x \le N-1,\ (2k-2)R \le y \le N-1$.

The structure of this lattice η is the following:

$$
\begin{array}{r|c|c|}
 & \overbrace{\hphantom{\textstyle\prod Y_i\quad\quad}}^{kR} & \overbrace{\hphantom{-\textstyle\prod Z_i\quad\quad}}^{kR} \\
\cline{2-3}
2R\{ & \prod Y_i & -\prod Z_i \\
\cline{2-3}
2R\{ & Y_{k-1} & Z_{k-1} \\
\cline{2-3}
\vdots & \vdots & \vdots \\
\cline{2-3}
2R\{ & Y_3 & Z_3 \\
\cline{2-3}
2R\{ & Y_2 & Z_2 \\
\cline{2-3}
2R\{ & Y_1 & Z_1 \\
\cline{2-3}
\end{array}
$$

(Here $\prod Y_i$ means that the j-th element in the ℓ-th row of this $2R \times kR$ matrix is the product of the corresponding elements of the matrices $Y_1, Y_2, \dots, Y_{k-1}$; the meaning of $\prod Z_i$ is similar.)

It is easy to see that in this construction we have

$$Q_{2k}(E_{N^2}(\eta)) \ge C_{2k}(E_{N^2}(\eta)) \gg N^2.$$

This motivates the following question:

Problem 3 *Is it true that if $Q_{2k}(E_{N^2}(\eta)) = o(N^2)$ for some fixed $k > 1$, then we have $\overline{Q}_k(\eta) = o(N^2)$?*

By Theorem 3 it may occur that $C_2(E_{N^2})$ is small but $\overline{Q}_2(\eta)$ is large. The opposite of this cannot be occur:

Theorem 4 *For every binary N-lattice η and $k \in \mathbb{N}$ we have*

$$Q_k(E_{N^2}(\eta)) \le 3N\left(\overline{Q}_k(\eta)\right)^{1/2}.$$

Note that as it was shown in [3], for a truly random 2-dimensional N-lattice η the order of magnitude of $\overline{Q}_k(\eta)$ is N, so that the right hand side is $O(N^{3/2})$. Thus in general this theorem gives the nontrivial bound $O(N^{3/2})$ for $Q_k(E_{N^2}(\eta))$.

Proof. By the definition of $Q_k(E_{N^2}(\eta))$ there exist a, t and $D = (d_1, d_2, \dots, d_k)$ with $0 < d_1 < d_2 < \dots < d_k$ such that

$$Q_k(E_{N^2}(\eta)) = \left| \sum_{j=0}^{t} e_{ja+d_1} e_{ja+d_2} \cdots e_{ja+d_k} \right|, \tag{5.15}$$

where all subscripts $ja+d_\ell$ belong to $\{1,2,\ldots,N^2\}$. We split $\{1,2,\ldots,N^2\}$ into subsets. For $0 \le i \le N-1$ the $i+1$-st subset is

$$I_i = \{iN+1, iN+2, \ldots, (i+1)N\}.$$

For $0 \le j \le t$ the minimum value of $ja+d_1$ is d_1. Write d_1 in form

$$d_1 = y_{\min}N + x_1 \text{ where } 0 \le x_1 \le N-1.$$

For $0 \le j \le t$ the maximum value of $ja+d_1$ is $ta+d_1$. Write $ta+d_1$ in form

$$ta+d_1 = y_{\max}N + x_2 \text{ where } 0 \le x_2 \le N-1.$$

Then

$$\begin{aligned}
Q_k(E_{N^2}(\eta)) &= \left| \sum_{i=y_{\min}}^{y_{\max}} \sum_{\substack{0\le j\le t\\ ja+d_1\in I_i}} e_{ja+d_1}\cdots e_{ja+d_k} \right| \\
&\le \left| \sum_{\substack{0\le j\le t\\ ja+d_1\in I_{y_{\min}}\cup I_{y_{\max}}}} e_{ja+d_1}\cdots e_{ja+d_k} \right| \\
&+ \left| \sum_{i=y_{\min}+1}^{y_{\max}-1} \sum_{\substack{0\le j\le t\\ ja+d_1\in I_i}} e_{ja+d_1}\cdots e_{ja+d_k} \right| \\
&\le 2N + \left| \sum_{i=y_{\min}+1}^{y_{\max}-1} \sum_{\substack{0\le j\le t\\ ja+d_1\in I_i}} e_{ja+d_1}\cdots e_{ja+d_k} \right| \\
&= 2N + \left| \sum_{\ell=0}^{a-1} \sum_{\substack{i=y_{\min}+1\\ i\equiv \ell \pmod a}}^{y_{\max}-1} \sum_{\substack{0\le j\le t\\ ja+d_1\in I_i}} e_{ja+d_1}\cdots e_{ja+d_k} \right| \\
&\le 2N + \sum_{\ell=0}^{a-1} \left| \sum_{\substack{i=y_{\min}+1\\ i\equiv \ell \pmod a}}^{y_{\max}-1} \sum_{\substack{0\le j\le t\\ ja+d_1\in I_i}} e_{ja+d_1}\cdots e_{ja+d_k} \right| . \qquad (5.16)
\end{aligned}$$

It is easy to check that if $0 \le \ell < a$ and

$$\{e_{ja+d_1} : \ ja+d_1 \in I_\ell, \ j \in \mathbb{N}\} = \{\eta(x_\ell,\ell), \ \eta(x_\ell+a,\ell), \ldots, \eta(x_\ell+t_\ell a,\ell)\}, \qquad (5.17)$$

then for $i \equiv \ell \pmod a$ we have

$$\{e_{ja+d_1} : \ ja+d_1 \in I_i, \ j \in \mathbb{N}\} = \{\eta(x_\ell,i), \ \eta(x_\ell+a,i), \ldots, \eta(x_\ell+t_\ell a,i)\}.$$

In (5.16) j assumes values from the interval $[0,t]$. By the definition of $y_{\min}$ and $y_{\max}$, (5.17), $i \equiv \ell \pmod a$ and $y_{\min}+1 \le i \le y_{\max}-1$, then

$$\begin{aligned}&\{e_{ja+d_1} :\ ja+d_1 \in I_i,\ 0 \le j \le t\}\\ &= \{\eta(x_\ell, i),\ \eta(x_\ell + a, i), \dots, \eta(x_\ell + t_\ell a, i)\}.\end{aligned}$$

Write $d_i - d_1$ in form

$$d_i - d_1 = d_{i,1}N + d_{i,2} \text{ with } 0 \le d_{i,2} \le N-1$$

and define

$$\underline{d}'_{i-1} = (d_{i,1}, d_{i,2}).$$

Then $i \equiv \ell \pmod a$ and $y_{\min}+1 \le i \le y_{\max}-1$ we have

$$\begin{aligned}&\sum_{\substack{0\le j\le t\\ ja+d_1\in I_i}} e_{ja+d_1}\cdots e_{ja+d_k}\\ &= \sum_{j=0}^{t_\ell} \eta((x_\ell + ja, i))\eta((x_\ell + ja, i) + \underline{d}'_1)\cdots \eta((x_\ell + ja, i) + \underline{d}'_{k-1}).\end{aligned}$$

Let

$$\{i :\ i \equiv \ell \pmod a,\ y_{\min}+1 \le i \le y_{\max}-1\} = \{y_\ell, y_\ell + a, \dots, y_\ell + s_\ell a\}.$$

Then

$$\begin{aligned}&\sum_{\substack{i=y_{\min}+1\\ i\equiv \ell \pmod a}}^{y_{\max}-1} \sum_{\substack{0\le j\le t\\ ja+d_1\in I_i}} e_{ja+d_1}\cdots e_{ja+d_k}\\ &= \sum_{i=0}^{s_\ell}\sum_{j=0}^{t_\ell} \eta((x_\ell + ja, y_\ell + ia))\eta((x_\ell + ja, y_\ell + ia) + \underline{d}'_1)\cdots\\ &\quad \eta((x_\ell + ja, y_\ell + ia) + \underline{d}'_{k-1}).\end{aligned}$$

By the definition of $\overline{Q}_k(\eta)$ we have

$$\begin{aligned}&\left|\sum_{\substack{i=y_{\min}+1\\ i\equiv \ell \pmod a}}^{y_{\max}-1} \sum_{\substack{0\le j\le t\\ ja+d_1\in I_i}} e_{ja+d_1}\cdots e_{ja+d_k}\right|\\ &= \left|\sum_{i=0}^{s_\ell}\sum_{j=0}^{t_\ell} \eta((x_\ell + ja, y_\ell + ia))\eta((x_\ell + ja, y_\ell + ia) + \underline{d}'_1)\right.\\ &\quad \left.\cdots \eta((x_\ell + ja, y_\ell + ia) + \underline{d}'_{k-1})\right| \le \overline{Q}_k(\eta). \qquad (5.18)\end{aligned}$$

Using (5.16) and (5.18) we get

$$Q_k(E_{N^2}(\eta)) \leq 2N + a\overline{Q}_k(\eta). \tag{5.19}$$

On the other hand, the number of terms in (5.15) is

$$t + 1 \leq 2t \leq \frac{2N^2}{a},$$

thus

$$Q_k(E_{N^2}(\eta)) \leq \frac{2N^2}{a}.$$

Then

$$a \leq \frac{2N^2}{Q_k(E_{N^2}(\eta))}.$$

Using this and (5.19)

$$\begin{aligned}
Q_k(E_{N^2}(\eta)) &\leq 2N + \frac{2N^2\overline{Q}_k(\eta)}{Q_k(E_{N^2}(\eta))}, \\
Q_k(E_{N^2}(\eta))^2 &\leq 2NQ_k(E_{N^2}(\eta)) + 2N^2\overline{Q}_k(\eta), \\
(Q_k(E_{N^2}(\eta)) - N)^2 &\leq N^2 + 2N^2\overline{Q}_k(\eta), \\
Q_k(E_{N^2}(\eta)) &\leq N + N\left(1 + 2\overline{Q}_k(\eta)\right)^{1/2}, \\
Q_k(E_{N^2}(\eta)) &\leq 3N\left(\overline{Q}_k(\eta)\right)^{1/2}
\end{aligned}$$

which was to be proved.

References

[1] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, *Measures of pseudorandomness for finite sequences: typical values*, Proc. London Math. Soc. (3) 95 (2007), 778-812.

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

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

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

[5] C. Mauduit and A. Sárközy, *On large families of pseudorandom binary lattices*, J. Uniform Distribution Theory 2 (2007), 23-37 (electronic).

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

[7] C. Mauduit and A. Sárközy, *On finite pseudorandom sequences of k symbols*, Indag. Mathem. 13 (2002), 89-101.

[8] A. Menezes, P. van Oorschot, S.Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[9] A. Rényi, *Probability Theory*, in: North-Holland Series in Applied Mathematics and Mechanics, Vol. 10, North-Holland Publishing Co., New York 1970.

[10] A. Sárközy, *On finite pseudorandom binary sequences and their applications in cryptography*, Tatra Mountains J., to appear.

[11] W. M. Schmidt, *Equations over Finite Fields, An Elementary Approach*, Lecture Notes in Math. 536, Springer, New York, 1976.

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

Alfréd Rényi Institute of Mathematics
H-1053 Reáltanoda utca 13-15
Hungary
e-mail: gykati@cs.elte.hu

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

Department of Algebra and Number Theory
Eötvös Loránd University
H-1117 Budapest, Pázmány Péter sétány 1/c
Hungary
e-mail: sarkozy@cs.elte.hu