On finite pseudorandom binary lattices

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

Christian Mauduit

Université Aix-Marseille, Institut de Mathématiques de Luminy
CNRS, UMR 7373, 165 avenue de Luminy, F-13288 Marseille Cedex 9, France
e-mail: mauduit@iml.univ-mrs.fr

and

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

Dedicated to the memory of Levon H. Khachatrian

Abstract

Pseudorandom binary sequences play a crucial role in cryptography. The classical approach to pseudorandomness of binary sequences is based on computational complexity. This approach has certain weak points thus in the last two decades a new, more constructive and quantitative approach has been developed. Since multidimensional analogs of binary sequences (called binary lattices) also have important applications thus it is a natural idea to extend this new approach to the multidimensional case. This extension started with a paper published in 2006, and since that about 25 papers have been written on this subject. Here our goal is to present a survey of all these papers.

2010 Mathematics Subject Classification: Primary 11K45.

Keywords and phrases: binary lattice, pseudorandomness, linear complexity, families of lattices.

Research partially supported by Hungarian National Foundation for Scientific Research, Grants No. K100291 and NK104183, the János Bolyai Research Fellowship, the Agence Nationale de la Recherche grant ANR-10-BLAN 0103 called MUNUM and Ciencia sem Fronteiras, project PVE 407308/2013-0.

1 Introduction

Finite binary sequences possessing strong *pseudorandom* properties (briefly pseudorandom or just PR sequences) play a crucial role in cryptography, e.g. sequences of this type can be applied as *key* in the classical encrypting system called *Vernam cipher*. Moreover, the theory of pseudorandomness can be also utilized in *number theory*. Thus about 20 years ago Mauduit and Sárközy [35] (partly with coauthors) started to study pseudorandomness of binary *sequences*, and we developed a *quantitative* and *constructive* theory of this subject. (Recently Gyarmati [10] has published a comprehensive survey of the papers written on pseudorandomness of finite pseudorandom binary sequences.)

Multidimensional analogs of PR binary sequences (which we will call PR binary *lattices*) also have many applications in cryptography (e.g. in encrypting images and bit maps), steganography and watermarking. Few years ago we extended our theory of pseudorandomness from one dimension to the multidimensional case. The first paper [28] written on this subject appeared in 2006, and since that about 25 related papers have been published. Here our goal is to give a short *survey* of these papers (focusing mostly on our contribution).

2 Notation, definitions, measures of pseudorandomness, a construction

Let I_N^n denote the set of n-dimensional vectors all whose coordinates are in $\{0, 1, \dots, N-1\}$:

$$I_N^n = \{\underline{x} = (x_1, x_2, \dots, x_n) : \ x_1, \dots, x_n \in \{0, 1, \dots, N-1\}\}.$$

The set I_N^n is called the *n-dimensional N-lattice* or briefly (if n is fixed, usually as $n = 2$ or 3) *N-lattice*.

We remark that the points of I_N^n form an n-dimensional cube, in particular, for $n = 2$ a square:

$$\{\underline{x} = (x_1, x_2) : \ x_1, x_2 \in \{0, 1, \dots, N-1\}\}. \tag{2.1}$$

All our definitions and results to be presented later could be extended from squares to rectangles, i.e., from the N-lattice in (2.1) to the *"(M,N)-lattice"*

$$I_{(M,N)} = \{\underline{x} = (x_1, x_2) : \ x_1 \in \{0, 1, \dots, M-1\}, x_2 \in \{0, 1, \dots, N-1\}\}.$$

However, in all but one cases we will stick to square (in general n-dimensional cube) N-lattices instead of using (M,N)-lattices since this makes the formulas slightly simpler. The only exception will be Section 7 on the linear complexity where it will be more advantageous to consider (M,N)-lattices.

Definition 1. A function of the type

$$\eta(\underline{x}) = \eta\big((x_1,\dots,x_n)\big): \ I_N^n \to \{-1,+1\}$$

is called an *n-dimensional binary N-lattice* or briefly a *binary lattice*.

In other words, from an N-lattice I_N^n we get a binary lattice η if we assign -1 or $+1$ to each point (vector) of it.

Note that in the applications the binary sequences and binary lattices usually appear as *bit* sequences

$$S_N = (S_0, S_1, \dots, S_N) \in \{0,1\}^N$$

and *bit* lattices

$$\delta: \ I_{M,N} \to \{0,1\},$$

respectively. However, there is a natural trivial bijection between $\{-1,+1\}$ and $\{0,1\}$, thus it makes no difference whether we use -1, $+1$ or bits when studying pseudorandomness of binary sequences and lattices. If we work with -1 and $+1$, then the expected value of the sum studied is usually 0 (due to cancellation) so that we need not carry a sometimes quite complicated main term. Thus we usually work with -1 and $+1$ instead of bits, and here in case of lattices we will also do this. Again, there will be just one exception: Section 7 where we will consider bit lattices instead of $\{-1,+1\}$ binary lattices.

Observe that in the $n=1$ special case the binary N-lattices defined in Definition 1 are the binary *sequences* of length N. We will also need the following extension of Definition 1:

Definition 2. Let $\underline{u}_1, \underline{u}_2, \dots, \underline{u}_n$ be n linearly independent n-dimensional vectors over the field of the real numbers such that the i-th coordinate of $\underline{u}_i$ is in $\{1,2,\dots,N-1\}$ and the other coordinates of $\underline{u}_i$ are 0, so that $\underline{u}_i$ is of the form $(0,\dots,0,z_i,0,\dots,0)$ with $z_i \in \{1,2,\dots,N-1\}$. Let $t_1,t_2,\dots,t_n$ be integers with $0 \leqslant t_1,t_2,\dots,t_n < N$. Then the set

$$B_N^n = \big\{\underline{x} = x_1\underline{u}_1 + \dots + x_n\underline{u}_n: \ 0 \leqslant x_i|\underline{u}_i| \leqslant t_i (< N) \text{ for } i = 1,2,\dots,n\big\}$$

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

In 2006 Hubert, Mauduit and Sárközy [28] introduced the following measures of pseudorandomness of binary lattices:

Definition 3. The *pseudorandom measure of order* k of the binary lattice $\eta: I_N^n \to \{-1,+1\}$ is defined by

$$Q_k(\eta) = \max_{B,\underline{d}_1,\dots,\underline{d}_k} \left| \sum_{x\in B} \eta(\underline{x}+\underline{d}_1)\eta(\underline{x}+\underline{d}_2)\dots\eta(\underline{x}+\underline{d}_k) \right|$$

where the maximum is taken over all distinct vectors $\underline{d}_1,\dots,\underline{d}_k$ with coordinates in $\{0,1,\dots,N-1\}$ and all box N-lattices B such that $B+\underline{d}_1,\dots,B+\underline{d}_k \in I_N^n$.

Note that in the $n=1$ special case this is the so-called *combined measure of order* k of the given binary *sequence* $\eta: I_N^1 \to \{-1,+1\}$ (see [35]).

It was shown in [28] that for a (truly) random lattice $\eta: I_N^n \to \{-1,+1\}$ the measure $Q_k(\eta)$ is around $N^{n/2}$:

Theorem 1. *If $k\in\mathbb{N}$ and $\varepsilon>0$, then there are numbers $N_0=N_0(k,\varepsilon)$ and $\delta=\delta(k,\varepsilon)>0$ such that for $N>N_0$ we have*

$$P\big(Q_k(\eta) > \delta N^{n/2}\big) > 1-\varepsilon$$

and

$$P\big(Q_k(\eta) > \big(81kN^n\log N^n\big)^{1/2}\big) < \varepsilon.$$

This was proved by the moment method as the analogous result in one dimension [5] (see also [4]), however, it makes a slight difficulty here that there is no natural ordering in I_N^n for $n>1$. Thus η can be considered as a "good" PR lattice if $Q_k(\eta)$ is not much greater than $N^{n/2}$ (at least for "small" k values).

In [28] the next problem studied was to construct a "good" PR lattice. However, this problem leads to serious difficulties. Namely, the natural idea would be to start out from a one-dimensional construction which contains a one-variable polynomial $f(x)\in\mathbb{F}_p[x]$ (almost all the one-dimensional constructions contain such a polynomial), and then to replace this polynomial by a two-variable polynomial $f(x,y)\in\mathbb{F}_p[x,y]$. Unfortunately, this idea does not work since in one dimension the proofs are based on Weil's theorem [47], while in the multidimensional situation one would need Deligne theorem [7], [8] or Katz's theorem [29], [30], [31] which are not flexible enough to use because of the strong non-singularity assumption in it. (In Section 5 we will return to this idea.)

In [28] this idea was replaced by considering finite fields $\mathbb{F}_{p^n}$ (where n is the dimension of the lattice) as a vector space over $\mathbb{F}_p$, and then using a principle due to Davenport and Lewis [6], and a few years ago generalized and expressed in a convenient form by Winterhof (by using Weil's theorem [47] in his proof). Using this detour the following theorem has been proved:

Theorem 2. *Let p be an odd prime, $n \in \mathbb{N}$, $q = p^n$, and denote the quadratic character of $\mathbb{F}_q$ by γ. Let $v_1, \dots, v_n$ be a basis of $\mathbb{F}_q$ as a vector space over $\mathbb{F}_p$. Define the lattice $\eta : I_p^n \to \{-1, +1\}$ by*

$$\eta(\underline{x}) = \eta\big((x_1, ..., x_n)\big) = \begin{cases} \gamma(x_1 v_1 + \dots + x_n v_n) & \text{for } (x_1, \dots, x_n) \neq (0, \dots, 0), \\ 1 & \text{for } (x_1, \dots, x_n) = (0, \dots, 0) \end{cases}$$

for $x_1, \dots, x_n \in \mathbb{F}_p$. Then we have

$$Q_k(\eta) < kq^{1/2}(1 + \log p)^n.$$

3 Large families of pseudorandom lattices

In the applications it is usually not enough to construct a few "good" PR lattices, one needs large families of them. Thus in 2007 Mauduit and Sárközy [36] extended Theorem 2 in this direction. We need two definitions:

Definition 4. If $q = p^n$ is a prime power, $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_q$, and $\mathcal{A} + \mathcal{B}$ represents every element of $\mathbb{F}_q$ with *even multiplicity*, i.e., for all $c \in \mathbb{F}_q$ the equation

$$a + b = c, \quad a \in \mathcal{A}, \ b \in \mathcal{B}$$

has even number of solutions (including when there is no solution), then the sum $\mathcal{A} + \mathcal{B}$ is said to have *property P*.

Definition 5. If $q = p^n$ is a prime power, $h, \ell \in \mathbb{N}$ and $k, \ell \leqslant q$, then (k, ℓ, q) is said to be an *admissible triple* if there are no $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_q$ such that $|\mathcal{A}| = k$, $|\mathcal{B}| = \ell$, and $\mathcal{A} + \mathcal{B}$ possesses property P.

We proved the following theorems in [36]:

Theorem 3. *Assume that $q = p^n$ is the power of an odd prime, $f(x) \in \mathbb{F}_q[x]$ is of degree ℓ with $0 < \ell < p$, $f(x)$ has no multiple zero in $\mathbb{F}_q$, and the n-dimensional binary p-lattice $\eta : I_p^n \to \{-1, +1\}$ is defined by*

$$\begin{aligned} \eta(\underline{x}) &= \eta\big((x_1, \dots, x_n)\big) \\ &= \begin{cases} \gamma\big(f(x_1 v_1 + \dots + x_n v_n)\big) & \text{for } f(x_1 v_1 + \dots + x_n v_n) \neq 0, \\ 1 & \text{for } f(x_1 v_1 + \dots + x_n v_n) = 0 \end{cases} \end{aligned}$$

where γ is the quadratic character of $\mathbb{F}_q$. Assume also that $k \in \mathbb{N}$ and the triple (r, k, q) is admissible *for all $r \leqslant \ell$. Then we have*

$$Q_k(q) < k\ell\big(q^{1/2}(1 + \log p)^n + 2\big).$$

Theorem 4.

(i) *For every prime power $q = p^n$ and for $\ell \in \mathbb{N}$, $\ell < p$ the triple $(\ell, 2, q)$ is admissible.*

(ii) *If $q = p^n$ is a prime power, $k, \ell \in \mathbb{N}$, and*

$$4^{n(k+\ell)} < p,$$

then the triple (k, ℓ, q) is admissible.

Combining Theorems 3 and 4 we get a rather large family of n-dimensional binary lattices with strong PR properties (although in a certain sense the size of the family is slightly smaller than in one dimension in [9] and here more effort is needed to prove it than there). We also presented a few negative examples to illustrate the difficulties.

Mauduit and Sárközy [37] also extended another one-dimensional construction based on the use of the *multiplicative inverse* and polynomials to n dimensions, and later Liu [33] proved a similar result with other assumptions on the polynomials used.

By using multiplicative characters and polynomials, Mérai [38] presented and studied a very general construction for large families of PR lattices. In fact, his construction covers the extension of three different one-dimensional constructions [9], [11], [12], [13], [39], [43], [46] for binary sequences to binary lattices.

In [32] Liu presented another construction for a large family of pseudorandom binary lattices by using the multiplicative inverse and the quadratic character of finite fields.

In [40] Mérai presented and studied a construction for large families of binary lattices which was based on the use of elliptic curves.

Mérai extended in [41] the notion of binary lattices to *"k-ary lattices"* (i.e. to lattices composed of "k symbols"), and presented and studied a construction for PR k-ary lattices.

4 Sequences and lattices

In [17] we studied the following problem: When we try to extend the one-dimensional constructions to n dimensions, then it usually turns out that the multidimensional case is more difficult. A natural question to ask is: Does one really need the multiple-dimensional theory? Are there no simple and cheap, however, 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? The most natural step in this direction is the following construction:

Take a 2-dimensional binary N*-lattice* $\eta = \eta(x, y)$, consider the $N \times N$ matrix formed by the elements $\eta(i, j)$ with $i, j \in \{0, 1, \dots, N-1\}$, then take the first row vector of this matrix, continue with the second row vector, etc.; finally, take the last row, and *concatenate* these vectors into a single binary *sequence* $E_{N^2} = E_{N^2}(\eta) \in \{-1, +1\}^N$. *What is the connection between the PR properties of* η *and* $E_{N^2}(\eta)$*?* We showed that it may occur that η is "bad" but the corresponding sequence $E_{N^2}(\eta)$ is "good". Thus the answer to this question is negative: in general one cannot get a "good" lattice from a "good" sequence in the way described above. Conversely, we show that if the lattice η has strong pseudorandom properties, then the sequence $E_{N^2}(\eta)$ also has. Later this result was sharpened by Gyarmati in [16].

5 Replacing $f(x)$ in one-dimensional constructions by $f(x, y)$

As we have seen in Section 2, if we try to extend a one-dimensional construction involving a polynomial $f(x) \in \mathbb{F}_p[x]$ to two dimensions so that we replace $f(x)$ by some $f(x, y) \in \mathbb{F}_p[x, y]$, then we may run into trouble since we cannot use Weil's theorem *directly*. However, in some cases the situation can be saved at the expense of getting a slightly weaker estimate. This was shown first in the case of the Legendre symbol construction by Gyarmati, Sárközy and Stewart [26], [27]. In these papers the following construction was studied:

Construction 1. Let p be an odd prime, $f(x, y) \in \mathbb{F}_p[x, y]$ be a polynomial in two variables. Then define $\eta : I_p^2 \to \{-1, +1\}$ by

$$\eta(x, y) = \begin{cases} \left(\dfrac{f(x, y)}{p}\right) & \text{if } \big(f(x, y), p\big) = 1, \\ +1 & \text{if } p \mid f(x, y). \end{cases}$$

We will need the following:

Definition 6. The polynomial $f(x, y) \in \mathbb{F}_p[x, y]$ is called *degenerate* if it is of the form

$$f(x, y) = \left(\prod_{j=1}^{r} f_j(\alpha_j x + \beta_j y)\right) g(x, y)^2$$

where $\alpha_j, \beta_j \in \mathbb{F}_p$, $f_j(x) \in \mathbb{F}_p[x]$ for $j = 1, \dots, r$, and $g(x, y) \in \mathbb{F}_p[x, y]$.

It was shown in [26] by examples that if the polynomial $f(x, y)$ in Construction 1 is degenerate, then the lattice η constructed may have weak PR properties. On the other hand, it was proved:

Theorem 5. *Let $f(x, y) \in \mathbb{F}_p[x, y]$ be a* nondegenerate *polynomial of degree k. Assume that one of the following five conditions holds:*
a) *$f(x, y)$ is irreducible in $\mathbb{F}_p[x, y]$,*
b) *$\ell = 2$,*
c) *2 is a primitive root modulo p,*
d) *$4^{k+\ell} < p$,*
e) *ℓ and the degree of the polynomial $f(x, y)$ in x (or in y) are odd.*
Then for the binary p-lattice defined in Construction 1 we have

$$Q_\ell(\eta) \leqslant 11k\ell p^{3/2} \log p. \tag{5.1}$$

Comparing the sufficient conditions in this theorem with the ones in Theorem 4, we find that there are more options here, besides the new conditions here (in particular, c) and e)) are milder and more convenient. On the other hand, observe that the exponent of p in the upper bound in (5.1) is $3/2$ instead of the optimal 1. However, we also showed in Part II [27] that the optimal exponent can be achieved in certain special cases.

In the second paper [27] the *degenerate* case was analyzed. It was shown that then anything can occur: η can be "bad"; "not too bad, not too good"; "good". This is a complicated paper.

In 2009 Gyarmati, Mauduit and Sárközy [18] studied the analog of the last problem for three other basic one-dimensional constructions, i.e., in order to extend these constructions to two dimensions, we replaced $f(x)$ in them by $f(x, y)$. We proved similar results, i.e., in each of these cases we showed that under appropriate conditions the lattice constructed possesses certain PR properties but the upper bounds obtained for the PR measures are not optimal.

6 The measures of pseudorandomness of binary lattices

In three papers [19], [20], [21] Gyarmati, Mauduit and Sárközy studied the measures of pseudorandomness of finite binary lattices. In the first paper we studied the connection between the measures Q_k and Q_ℓ (with $k \neq \ell$) for two-dimensional lattices (but our results could be extended easily to $n > 2$). First we proved the following results:

Theorem 6. *For $k, \ell, N \in \mathbb{N}$, $k, \ell < N$, $k \mid \ell$ and every binary lattice $\eta :\ I_N^2 \to \{-1, +1\}$ we have*

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

So that for $k \mid \ell$, the measure $Q_k(N)$ can be estimated in terms of $Q_\ell(\eta)$. In particular, it follows from this theorem that if $k \mid \ell$, $N \to \infty$ and $Q_\ell(\eta) = o(N^2)$, then $Q_k(\eta)$ is also $o(N^2)$.

We also showed that the condition $k \mid \ell$ is necessary in Theorem 6:

Theorem 7. *If $k, N \in \mathbb{N}$ and $k \leqslant N$, then there is a binary N-lattice η such that if $\ell \in \mathbb{N}$, $\ell \leqslant N/2$, then*

$$Q_\ell(\eta) \geqslant \frac{N(N-\ell)}{k} \quad \text{if} \;\; k \mid \ell$$

and

$$Q_\ell(\eta) \ll k^2 \ell N (\log N)^2 \quad \text{if} \;\; k \mid \ell$$

Thus for this lattice η the measure $Q_\ell(\eta)$ is large if and only if $k \mid \ell$. Summarizing: if $k < \ell$, then Q_k and Q_ℓ are independent if and only if $k \nmid \ell$.

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

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

Definition 7. The *normality measure of order (k, ℓ) of η* is defined as

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

We proved the following results:

Theorem 8. *For $N, k, \ell \in \mathbb{N}$, $k < N$, $\ell < N$ and every binary lattice $\eta :\ I_N^2 \to \{-1, +1\}$ we have*

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

We also proved that if $k \leqslant r$, $\ell \leqslant s$, and r, s are "small", then $N_{(k,\ell)}(\eta)$ cannot be much greater than $N_{(r,s)}(\eta)$:

Theorem 9. *For every $N, k, \ell, r, s \in \mathbb{N}$, $k \leqslant r \leqslant N$, $\ell \leqslant s \leqslant N$ and every binary lattice $\eta: \ I_N^2 \to \{-1, +1\}$ we have*

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

In [14] Gyarmati introduced the *symmetry measure* for studying binary *sequences*. In our second triple paper on the PR measures of binary lattices [20] we extended the symmetry measure to two dimensions, i.e., to binary *lattices*. It turned out that there are three equally natural ways to do this, thus we introduced three different *symmetry measures* for binary lattices. We showed that these three measures are independent, and we estimated these measures for (truly) *random* binary lattices. Finally, we presented a construction for which each of the three pseudorandom measures is small.

In the third part [21] of this series first we defined the correlation of binary lattices:

Definition 8. The *correlation measure of order k* of the lattice $\eta: \ I_N^n \to \{-1, +1\}$ is defined by

$$C_k(\eta) = \max_{B', \underline{d}_1, \ldots, \underline{d}_k} \left| \sum_{\underline{x} \in B'} \eta(\underline{x} + \underline{d}_1) \ldots \eta(\underline{x} + \underline{d}_k) \right|$$

where the maximum is taken over all distinct $\underline{d}_1, \ldots, \underline{d}_k \in I_N^n$ and all box lattices B' of the special form

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

such that $B' + \underline{d}_1, \ldots, B' + \underline{d}_k \in I_N^n$. Then clearly we have

$$C_k(\eta) \leqslant Q_k(\eta).$$

Next we generalized a theorem of Roth [44] to two dimensions:

Theorem 10. *Let $N \in \mathbb{N}$, $Q \in \mathbb{N}$ and $Q \geqslant 2$, 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*

(6.1) $\quad S_{u,v} = 0$ *if $u, v \in \mathbb{Z}$ and one of $u < 1, \ u > N, \ v < 1, \ v > N$ holds.*

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

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

Corollary. *If* $\varepsilon > 0$*,* $N > N_0(\varepsilon)$*,* $N \in \mathbb{N}$*,* $S_{u,v} \in \mathbb{C}$ *for* $u, v \in \{1, 2, \dots, N\}$*, and we also use the notation* (6.1)*, then there exist* $m, n \in \mathbb{Z}$ *and* $q, r \in \mathbb{N}$ *such that* $q, r \leqslant N^{1/2}$ *and*

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

Finally, we studied the minimal values of the Q_k, correlation and normality measures.

In [15] Gyarmati started out from the observation that "…the form of the box lattices B in the definition of $Q_\ell(\eta)$…" [Definition 3] "… is very restricted". Thus she introduced two new measures for pseudorandomness of binary lattices: "the convex measure of order ℓ" (where the maximum in the definition is taken over certain convex polytopes) and "the line measure of order ℓ" (where the maximum is taken over certain lines). She studied the connection between these new measures and the measure $Q_\ell(\eta)$, and estimated the values of these measures for a (truly) random η, and she presented a construction where these measures are small.

7 The linear complexity of binary lattices

For binary *sequences* the most classical measure of pseudorandomness is the *linear complexity*. For finite binary sequences the definition is the following:

Definition 9. The *linear complexity* $L(S_N)$ (over the field $\mathbb{F}_2$) of the finite *bit sequence* $S_N = (s_0, s_1, \dots, s_{N-1}) \in \{0,1\}^N$ is the *length of a shortest linear recursion*

$$s_{n+L} = c_{L-1}s_{n+L-1} + c_{L-2}s_{n+L-2} + \cdots + c_0 s_n, \quad n = 0, 1, \dots, N-L+1$$

over $\mathbb{F}_2$ which is satisfied by the sequence S_N, with the convention that $L(S_N) = 0$ if $s_0 = s_1 = \cdots = s_{N-1} = 0$ and $L(S_N) = N$ if $s_0 = s_1 = \cdots = s_{N-2} = 0$ and $s_{N-1} = 1$.

Berlekamp and Massey [34] presented an algorithm for computing the linear complexity of a given bit sequence, and Rueppel [45] proved that the linear complexity of a (truly) random bit sequence of length N is $(1+o(1))\frac{N}{2}$.

It is a natural idea to define and study the linear complexity of binary *lattices*; we did this in two papers [22], [23]. First we extended Definition 9 (the definition the linear complexity of bit sequences) to two dimensions; this extended definition is very complicated. A slightly more transparent definition can be given by rewriting the one-dimensional definition in a more algebraic form:

Definition 9'. Consider the bit sequence $S_N = (s_0, s_1, \dots, s_{N-1}) \in \{0,1\}^N$, and assign the polynomial $f(x) = \sum\limits_{n=0}^{N-1} s_n x^n \in \mathbb{F}_2[x]$ (which can be considered the *generating polynomial* of S_N) to it. Then the *linear complexity* of S_N is defined as the smallest positive integer L such that there is a polynomial $g(x) = \sum\limits_{i=1}^{L} c_{L-i} x^i \in \mathbb{F}_2[x]$ with the property that the coefficient of x^n in the polynomial $f(x)g(x)$ is s_n for $n < N$ except for the terms x^n with $0 \leqslant n < L$.

This definition can be extended to two dimensions in the following way:

Definition 10. Write $I_{M,N} = \{0,1,\dots,M-1\} \times \{0,1,\dots,N-1\}$. Consider the *bit* (M,N)-lattice $\delta = \delta(\underline{x}) : \ I_{M,N} \to \{1,0\}$, and write $\delta(i,j) = s_{i,j}$ for $i = 0,1,\dots,M-1$, $j = 0,1,\dots,N-1$. Assign the polynomial $f(x,y) = \sum\limits_{m=0}^{M-1} \sum\limits_{n=0}^{N-1} s_{m,n} x^m y^n \in \mathbb{F}_2[x,y]$ (this is the generating polynomial of η) to the bit lattice δ. Then the *linear complexity of* δ is defined as the smallest *positive* integer L that can be written in the form $L = (U+1)(V+1) - 1$ with non-negative integers U, V such that there is a polynomial

$$g(x,y) = \sum_{\substack{0 \leqslant i \leqslant U \\ 0 \leqslant j \leqslant V \\ (i,j) \neq (0,0)}} c_{U-i,V-j} x^i y^j \in \mathbb{F}_2[x,y]$$

with the property that the coefficient of $x^m y^n$ in the polynomial $f(x,y)g(x,y)$ is $s_{m,n}$ for $0 \leqslant m < N$, $0 \leqslant n < N$ except for the terms $x^m y^n$ with $0 \leqslant m \leqslant U$, $0 \leqslant n \leqslant V$, $(m,n) \neq (U,V)$.

Note that while in the one-dimensional Definition 9' the linear complexity L is the number of the terms of the polynomial $g(x)$ (counting also the terms with 0 coefficients), in the two-dimensional Definition 10 the linear complexity $L = (U+1)(V+1)-1$ is the number of the terms of the polynomial $g(x,y)$ (playing a similar role in Definition 8 as $g(x)$ in Definition 9'); this is why now L is defined by the complicated formula $(U+1)(V+1)-1$.

We showed that in the special case when δ is a bit $(N,1)$-lattice ($\delta : I_{N,1} \to \{1,0\}$, i.e., δ is a binary *sequence*), then the two-dimensional linear complexity of δ is the same as the one-dimensional one, so that the *two-dimensional definition is an extension of the one-dimensional one.*

We conjectured:

Conjecture 1. *The linear complexity of a (truly) random bit (M, N)-lattice $\delta: I_{M,N} \to \{1, 0\}$ is $\left(\frac{1}{2} + o(1)\right) MN$.*

We could prove only a slightly weaker result. The difficulty is that we have not been able to find the two-dimensional analog of the Berlekamp–Massey algorithm; there are several papers dealing with generalizations of the Berlekamp-Massey algorithm to vector sequences (see, e.g., [42]), but these results cannot be used for estimating the linear complexity of a random bit lattice.

Theorem 11. *For every $\varepsilon_1, \varepsilon_2 > 0$ there is a $C = C(\varepsilon_1, \varepsilon_2)$ such that if $M, N \in \mathbb{N}$, $MN > C$, then choosing each bit (M, N)-lattice $\delta: I_{M,N} \to \{1, 0\}$ with equal probability $\frac{1}{2^{MN}}$, we have*

$$P\left(L(\delta) > \frac{1}{2}MN - \left(\frac{1}{2} + \varepsilon_1\right) \frac{\log MN}{\log\log MN}\right) > 1 - \varepsilon_2.$$

(This proves the *lower* estimate part of Conjecture 1.)

Theorem 12. *If $0 < \varepsilon \leqslant 1$ and $M, N \in \mathbb{N}$ with $\max(M, N) > \frac{15}{\varepsilon}$, then choosing every bit (M, N)-lattice $\delta: I_{M,N} \to \{1, 0\}$ with equal probability $\frac{1}{2^{MN}}$, we have*

$$P\left(L(\delta) < \frac{3}{4}MN + \frac{1}{\varepsilon^{1/2}}(MN)^{3/4}\right) \geqslant 1 - \varepsilon.$$

(So that we proved an *upper* estimate with constant factor $\frac{3}{4}$ instead of the conjectured $\frac{1}{2}$.)

In our two papers we also studied the following problems: the connection between the linear complexity of a bit (M, N)-*lattice* δ and the linear complexity of the bit *sequence* obtained by concatenation of the row vectors of the $M \times N$ bit matrix assigned to δ; we showed that large linear complexity is not enough to guarantee that the bit lattice δ is a "good" PR lattice; the estimate of linear complexity of a bit lattice in terms of its correlations; the extension of the notion of k-error linear complexity from bit sequences to two-dimensional bit lattices.

8 Measures of pseudorandomness of families of binary lattices

In the applications it is usually not enough to have a "few" binary lattices with strong PR properties; one needs large families of them, and we also need information on the structure of these families. Thus in order to study pseudorandomness of families of binary lattices, in two papers [24], [25] we extended the notions of *family complexity*, *collision* and *avalanche effect* from the one-dimensional case to the multidimensional case.

In the one-dimensional case, the notion of family complexity was introduced by Ahlswede, Khachatrian, Mauduit and Sárközy in [1] and it was studied and extended in [2] and [3] (we were planning to work jointly with Khachatrian on this project; unfortunately he could not join us because of his untimely passing away).

In the multidimensional case we introduced the following definitions:

Definition 11. Assume that $n, N \in \mathbb{N}$, and a family $\mathcal{F}$ of n-dimensional binary N-lattices $\eta : I_N^n \to \{-1,+1\}$ is given. Then the *family complexity* $\Gamma(\mathcal{F})$ of the family $\mathcal{F}$ is defined as the greatest integer j so that for any distinct vectors $\underline{x}_1, \underline{x}_2, \dots, \underline{x}_j \in I_N^n$ and every $(\varepsilon_1, \dots, \varepsilon_j) \in \{-1,+1\}^j$ there is a lattice $\eta \in \mathcal{F}$ which satisfies the specification $\eta(\underline{x}_1) = \varepsilon_1$, $\eta(\underline{x}_2) = \varepsilon_2, \dots$, $\eta(\underline{x}_j) = \varepsilon_j$.

Now assume that $N \in \mathbb{N}$, $\mathcal{S}$ is a given finite set ("parameter set"), to each $s \in \mathcal{S}$ we assign a unique binary N-lattice $\eta = \eta_s : I_N^n \to \{-1,+1\}$, and let $\mathcal{F} = \mathcal{F}(\mathcal{S})$ denote the family of the binary lattices obtained in this way:

$$\mathcal{F} = \mathcal{F}(\mathcal{S}) = \big\{\eta_s;\ s \in \mathcal{S}\big\}. \tag{8.1}$$

Definition 12. If $s, s' \in \mathcal{S}$, $s \neq s'$ and $\eta_s = \eta_{s'}$ then this is said to be a *collision* in $\mathcal{F} = \mathcal{F}(\mathcal{S})$. If there is no collision in $\mathcal{F} = \mathcal{F}(\mathcal{S})$, then $\mathcal{F}$ is said to be *collision-free.* (A "good" family is expected to be collision-free.)

Definition 13. If $\mathcal{F}$ is of form (8.1), and for any $s \in \mathcal{S}$, changing s for any $s' \in \mathcal{S}$, $s \neq s'$ changes "many" elements of $\eta_s : I_N^n \to \{-1,+1\}$, then we speak about *avalanche effect*, and we say that $\mathcal{F} = \mathcal{F}(\mathcal{S})$ possesses the *avalanche property.* If for any $s, s' \in \mathcal{S}$, $s \neq s'$ we have $\eta_s(\underline{x}) \neq \eta_{s'}(\underline{x})$ for at least $\left(\frac{1}{2} - o(1)\right) N^n$ points $\underline{x} \in I_N^n$, then $\mathcal{F}$ is said to possess the *strict avalanche property.*

Definition 14. If $n, N \in \mathbb{N}$, $\eta, \eta' : I_N^n \to \{-1, +1\}$, then the *distance* $d(\eta, \eta')$ between η and η' is defined by

$$d(\eta, \eta') = \left|\left\{\underline{x} \in I_N^n : \ \eta(\underline{x}) \neq \eta'(\underline{x})\right\}\right|.$$

If $\mathcal{F}$ is of parametric form (8.1), then the *distance minimum* $m(\mathcal{F})$ in $\mathcal{F}$ is defined by $m(\mathcal{F}) = \min\limits_{\substack{s,s' \in \mathcal{S} \\ s \neq s'}} d(\eta_s, \eta_{s'})$. (So that $\mathcal{F}$ is collision-free if $m(\mathcal{F}) > 0$, and it possesses the strict avalanche property if we have $m(\mathcal{F}) \geqslant \left(\frac{1}{2} - o(1)\right) N^n$.)

In [24] first we studied the family of binary lattices constructed in Theorem 3. We showed that certain large subfamilies (defined by restrictions on the degree of the polynomials used) of this family have large family complexity, are collision-free, and possess the strict avalanche property. We also proved similar results on two other basic constructions for large families of binary lattices with strong PR properties.

References

[1] R. Ahlswede, L. H. Khachatrian, C. Mauduit and A. Sárközy, A complexity measure for families of binary sequences, *Period. Math. Hungar.* **46** (2003), 107–118.

[2] R. Ahlswede, C. Mauduit and A. Sárközy, Large families of pseudorandom sequences of k symbols and their complexity, I, in: *General Theory of Information Transfer and Combinatorics*, eds. R. Ahlswede et al., LNCS 4123, Springer, Berlin, 2006, 293–307.

[3] R. Ahlswede, C. Mauduit and A. Sárközy, Large families of pseudorandom sequences of k symbols and their complexity, II, in: *General Theory of Information Transfer and Combinatorics*, eds. R. Ahlswede et al., LNCS 4123, Springer, Berlin, 2006, 308–325.

[4] 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.

[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] H. Davenport and D. J. Lewis, Character sums and primitive roots in finite fields, *Rend Circ Mat Palermo* **12** (1963), 129–136.

[7] P. Deligne, La conjecture de Weil. I. (French), *Inst. Hautes tudes Sci. Publ. Math.* **43** (1974), 273-307.

[8] P. Deligne, La conjecture de Weil. II. (French), *Inst. Hautes tudes Sci. Publ. Math.* **52** (1980), 137252.

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

[10] K. Gyarmati, Measures of pseudorandomness, in: *Finite Fields and Their Applications*, eds. P. Charpin et al., Radon Series on Computational and Applied Mathematics **11**, de Gruyter, 2013; pp. 43–64.

[11] K. Gyarmati, On a family of pseudorandom binary sequences, *Period. Math. Hungar.* **49** (2004), 45–63.

[12] K. Gyarmati, On a fast version of a pseudorandom generator, in: *General Theory of Information Transfer and Combinatorics*, eds. R. Ahlswede et al., LNCS 4123, Springer, Berlin, 2006; pp. 326–342.

[13] K. Gyarmati, A note to the earlier paper "On a fast version of a pseudorandom generator", *Annals Univ. Sci. Budapest. Eötvös Sect. Math.* **49** (2006), 87–93.

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

[15] K. Gyarmati, On new measures of pseudorandomness of binary lattices, *Acta Math. Hungar.* **131** (2011), 346–359.

[16] K. Gyarmati, On the correlation of subsequences, *Unif. Distrib. Theory* **7** (2012), 169–195.

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

[18] K. Gyarmati, C. Mauduit and A. Sárközy, Constructions of pseudorandom binary lattices, *Unif. Distrib. Theory* **4** (2009), 59–80.

[19] K. Gyarmati, C. Mauduit and A. Sárközy, Measures of pseudorandomness of finite binary lattices, I. (The measures Q_k, normality), *Acta Arith.* **144** (2010), 295–313.

[20] K. Gyarmati, C. Mauduit and A. Sárközy, Measures of pseudorandomness of finite binary lattices, II. (The symmetry measures), *Ramanujan J.* **25** (2011), 155–178.

[21] K. Gyarmati, C. Mauduit and A. Sárközy, Measures of pseudorandomness of binary lattices, III. (Q_k, correlation, normality, minimal values), *Unif. Distrib. Theory* **5** (2010), 183–207.

[22] K. Gyarmati, C. Mauduit and A. Sárközy, On the linear complexity of binary lattices, *Ramanujan J.* **32** (2013), 185–201.

[23] K. Gyarmati, C. Mauduit and A. Sárközy, On the linear complexity of binary lattices, II, *Ramanujan J.* **34** (2014), 237–263.

[24] K. Gyarmati, C. Mauduit and A. Sárközy, Measures of pseudorandomness of families of binary lattices, I. (Definitions, a construction using quadratic characters), *Publ. Math. Debrecen* **79** (2011), 445–460.

[25] K. Gyarmati, C. Mauduit and A. Sárközy, Measures of pseudorandomness of families of binary lattices, II. (A further construction), *Publ. Math. Debrecen* **80** (2012), 481–504.

[26] K. Gyarmati, A. Sárközy and C. L. Stewart, On Legendre symbol lattices, *Unif. Distrib. Theory* **4** (2009), 81–95.

[27] K. Gyarmati, A. Sárközy and C. L. Stewart, On Legendre symbol lattices, II. *Unif. Distrib. Theory* **8** (2013), 47–65.

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

[29] N. Katz, Estimates for "singular" exponential sums, *Int. Math. Res. Not.* **16** (1999), 875–899.

[30] N. Katz, Estimates for nonsingular multiplicative character sums, *Int. Math. Res. Not.* **7** (2002), 333–349.

[31] N. Katz, Estimates for nonsingular mixed character sums *Int. Math. Res. Not.* **19** (2007), 19pp.

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

[33] H. Liu, Large families of pseudorandom binary sequences and lattices by using the multiplicative inverse, *Acta Arith.* **159** (2013), 123–131.

[34] J. L. Massey, Shift-register synthesis and BCH decoding, *IEEE Transactions Information Theory* **15** (1969), 122–127.

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

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

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

[38] L. Mérai, Construction of pseudorandom binary lattices based on multiplicative characters, *Period. Math. Hungar.* **59** (2009), 43–51.

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

[40] L. Mérai, Construction of pseudorandom binary lattices using elliptic curves, *Proc. Amer. Math. Soc.* **139** (2011), 407–420.

[41] L. Mérai, On finite pseudorandom lattices of k symbols, *Monatshefte Math.* **161** (2010), 173–191.

[42] G. L. Mullen and D. Panario, Handbook of Finite Fields, CRC Press, Taylor & Francis Group, Boca Raton, Florida, 2013.

[43] S. M. Oon, On pseudo-random properties of certain Dirichlet series, *Ramanujan J.* **15** (2008), 19–30.

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

[45] R. A. Rueppel, Linear complexity and random sequences, in: *Proc. Advances in Cryptology – EUROCRYPT '85*, Linz, Austria, April 9–12, 1985, LNCS 219; pp. 167–188.

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

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

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