On linear complexity of 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
(corresponding author; fax: 36-13812146)

Christian Mauduit
Université Aix-Marseille
Institut de Mathématiques de Luminy
CNRS, FRE 3529,
163 avenue de Luminy, 13288 Marseille cedex 9, France
and
Instituto de Matemática Pura e Aplicada
IMPA-CNRS, UMI 2924
Estrada Dona Castorina 110, 22460-320 Rio de Janeiro, RJ, Brasil
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

2010 Mathematics Subject Classification: Primary 11K45.

Keywords and phrases: linear complexity, linear recursion, two dimensions, binary lattice, pseudorandomness.

Research partially supported by Hungarian National Foundation for Scientific Research, Grants No. K72731 and K100291, French-Hungarian exchange program FR-33/2009, the Agence Nationale de la Recherche grant ANR-10-BLAN 0103 MUNUM and the János Bolyai Research Fellowship.

Abstract

The linear complexity is an important and frequently used measure of unpredictability and pseudorandomness of binary sequences. In this paper our goal is to extend this notion to two dimensions. We will define and study the linear complexity of binary lattices. The linear complexity of a truly random binary lattice will be estimated. Finally, we will analyze the connection between the linear complexity and the correlation measures, and we will utilize the inequalities obtained in this way for estimating the linear complexity of an important special binary lattice. Finally, we will study the connection between the linear complexity of binary lattices and of the associated binary sequences.

1 The linear complexity and other measures of pseudorandomness of sequences

The linear complexity is an important and frequently used measure of pseudorandomness of bit sequences which is closely related to cryptographic applications.

Definition 1 *The* linear complexity $L(S_N)$ *(over the field* $\mathbb{F}_2$*) of the finite bit sequence*

$$S_N = (s_0, s_1, \dots, s_{N-1}) \in \{0,1\}^N \tag{1.1}$$

is the length L *of a shortest linear recursion*

$$s_{n+L} = c_{L-1}s_{n+L-1} + c_{L-2}s_{n+L-2} + \cdots + c_0 s_n, \quad n = 0, 1, \dots, N-L-1 \tag{1.2}$$

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* $s_{N-1} = 1$*.*

(Note that one may also define the linear complexity of infinite binary sequences but we will not need this definition here.)

Definition 2 *The* linear complexity profile *of the bit sequence* $S_N = (s_0, s_1, \dots, s_{N-1})$ *is defined as the sequence of the numbers* $L(S_i)$, $i = 1, 2, \dots, N$ *where* S_i *is defined as* $S_i = (s_0, s_1, \dots, s_{i-1})$.

Surveys on the linear complexity are given in [16] and [18]. It is known [17] that the linear complexity of a truly random bit sequence $S_N = (s_0, s_1, \dots, s_{N-1}) \in \{0,1\}^N$ is $(1 + o(1))\frac{N}{2}$. It is easy to see that the linear complexity is nondecreasing, i.e., using the notation in Definition 2 we have

$$L(S_i) \leq L(S_{i+1}) \quad \text{for } i = 1, 2, \dots, N-1. \tag{1.3}$$

In [15] Mauduit and Sárközy introduced other quantitative measures of pseudorandomness of binary sequences. They considered binary sequences of form

$$E_N = (e_1, \dots, e_N) \in \{-1, +1\}^N. \tag{1.4}$$

(They switched from bit sequences to sequences consisting of -1 and +1 since then the formulas are slightly simpler, and this change is just a matter of notation.) Then the well-distribution measure of the sequence (1.4) is defined by

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

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

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

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

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

where the maximum is taken over all a, b, t and $\mathbf{D} = (d_1, \dots, d_k)$ such that all the subscripts $a + jb + d_\ell$ belong to $\{1, 2, \dots, N\}$. (Note that $Q_1(E_N) = W(E_N)$ and clearly $C_k(E_N) \le Q_k(E_N)$.) Then the sequence E_N is considered 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 [4] 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 [1] and [13].)

Although the linear complexity is defined for bit sequences of form (1.1) while the other measures of pseudorandomness are defined for binary sequences of form (1.4), all these measures can be used in both cases since there is a natural bijection $\varphi : \ \{0,1\}^N \to \{-1,+1\}^N$. Namely, if the sequence S_N in (1.1) is given then $\varphi(S_N)$ can be defined by

$$\begin{aligned} \varphi(S_N) = \varphi((s_0, s_1, \dots, s_{N-1})) = E_N = (e_1, e_2, \dots, e_N) \\ \text{with } e_{i+1} = (-1)^{s_i} \ (= 1 - 2s_i) \text{ for } i = 0, 1, \dots, N-1, \end{aligned} \tag{1.5}$$

while the inverse mapping is given by

$$\begin{gathered} \varphi^{-1}(E_N) = \varphi((e_1, e_2, \dots, e_N)) = S_N = (s_0, s_1, \dots, s_{N-1}) \\ \text{with } s_i = \frac{1 - e_{i+1}}{2} \text{ for } i = 0, 1, \dots, N-1. \end{gathered}$$

Thus, e.g., the correlation of order k of the bit sequence (1.1) can be defined by

$$\begin{aligned} C_k(S_N) = C_k(\varphi(S_N)) = C_k(E_N) &= \max_{M,\mathbf{D}} \left| \sum_{n=1}^{M} e_{n+d_1} \cdots e_{n+d_k} \right| \\ &= \max_{M,\mathbf{D}} \left| \sum_{n=0}^{M-1} (-1)^{s_{n+d_1} + \cdots + s_{n+d_k}} \right|. \end{aligned} \tag{1.6}$$

Moreover, we may define the linear complexity of the binary sequence E_N in (1.4) by

$$L(E_N) = L(\varphi^{-1}(E_N)). \tag{1.7}$$

Brandstätter and Winterhof [3] showed that the linear complexity of a bit sequence S_N can be estimated in terms of the correlations of the sequence (defined by (1.4)):

Theorem A *If* $N \geq 2$ *and* E_N *is a binary sequence, then we have*

$$L(E_N) \geq N - \max_{1 \leq k \leq L(E_N)+1} C_k(E_N).$$

(They used a slightly different terminology but their result seems to be equivalent with the theorem above.) Using this inequality they have been able to give (in some cases quite strong) lower estimate for the linear complexity of binary sequences occurring in certain constructions. (Later in [5] Theorem A was generalized to m-ary sequences.) While this theorem may give quite good estimate for the linear complexity, it has the disadvantage that it also uses correlations of high order whose estimate can be very difficult. Thus Andics [2] proved another inequality which uses the correlation of order 2 only:

Theorem B If $N \in \mathbb{N}$ and E_N is a binary sequence, then we have

$$2^{L(E_N)} \geq N - C_2(E_N).$$

However, Theorem B can imply only lower bounds of logarithmic order of magnitude.

2 The measures of pseudorandomness in n dimensions

In [12] Hubert, Mauduit and Sárközy extended the notion of binary sequences to n dimensions, and they defined the measures of pseudorandomness in this situation:

Let I_N^n denote the set of n-dimensional vectors whose coordinates are integers between 0 and $N-1$:

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

This set is called an *n-dimensional N-lattice* or briefly an *N-lattice*. In [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 n-dimensional 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, thus $\mathbf{u_i}$ 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

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

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 the following type:

Definition 3 *A function of type $\eta(\mathbf{x}) :\ I_N^n \rightarrow \{-1, +1\}$ is called binary N-lattice.*

(If $\mathbf{x} = (x_1, \dots, x_n)$ and $\eta(\mathbf{x}) = \eta((x_1, \dots, x_n))$, then we will simplify the notation slightly by writing $\eta(\mathbf{x}) = \eta(x_1, \dots, x_n)$.)

In [12] the following definition of measures of pseudorandomness of binary lattices was presented: if $\eta :\ I_N^n \rightarrow \{-1, +1\}$, then the *pseudorandom measure of order k of η* is defined by

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

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.

The correlation measure of binary lattices was also introduced in [9]: The *correlation measure of order k* of the lattice $\eta : I_N^n \to \{-1,+1\}$ is defined by

$$C_k(\eta) = \max_{B', \mathbf{d_1}, \dots, \mathbf{d_k}} \left| \sum_{\mathbf{x} \in B'} \eta(\mathbf{x} + \mathbf{d_1}) \cdots \eta(\mathbf{x} + \mathbf{d_k}) \right|, \tag{2.1}$$

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

$$B' = \{\mathbf{x} = (x_1, \dots, x_n) : \ x_i \in \mathbb{N} \cup \{0\}, \ 0 \le x_1 \le t_1 (< N), \dots, \\ 0 \le x_n \le t_n (< N)\}$$

such that $B' + \mathbf{d_1}, \dots, B' + \mathbf{d_k} \subseteq I_N^n$. (As in one dimension, clearly we have $C_k(\eta) \le Q_k(\eta)$.)

In [7] and [8] we also introduced and studied measures of pseudorandomness of families of binary lattices. On the other hand, as far as we know the notion of linear complexity of binary lattices has not been defined yet. (The only n dimensional extension of linear complexity that we know about is the notion of joint linear complexity; see e.g., [6] and the references in it. However, this notion cannot be used for studying binary lattices.) Indeed, in this paper *our goal is to define and study the linear complexity of binary lattices.*

3 The definition of linear complexity of two dimensional binary lattices.

In the rest of this paper we will restrict ourselves to two dimensional binary lattices; the n dimensional binary lattices could be handled in the same way just the formulas would be more complicated. On the other hand, we will extend the notion of binary lattice slightly. Namely, in Definition 3 we defined binary lattices on squares $I_N^2 = \{0, 1, \dots, N-1\}^2$ (recall that now the dimension is $n = 2$). When we want to introduce the linear complexity in 2 dimensions then it seems to be more natural to start out from rectangles

$$I_{M,N} = \{0, 1, \ldots, M-1\} \times \{0, 1, \ldots, N-1\}.$$

(Since from now on the dimension is always 2, there is no need to include the dimension in the notation.)

Definition 3' *A function of type* $\eta(\mathbf{x}):\ I_{M,N} \to \{-1, +1\}$ *is called a* binary (M, N)-lattice*.*

Replacing the η values equal to $+1$ by 0 and the values equal to -1 by 1 we get a function of type $\delta(\mathbf{x}):\ I_{M,N} \to \{1, 0\}$.

Definition 4 *A function of type* $\delta(\mathbf{x}):\ I_{M,N} \to \{1, 0\}$ *is called a* bit (M, N)-lattice*.*

As in one dimension, there is a bijection μ between bit lattices and binary lattices: if the bit (M, N)-lattice δ is given, then the binary (M, N)-lattice $\eta = \mu(\delta)$ is defined by

$$\begin{aligned} &\eta(i, j) = \mu(\delta)(i, j) = (-1)^{\delta(i,j)} (= 1 - 2\delta(i, j)) \\ &\qquad \text{for } i \in \{0, 1, \ldots, M-1\},\ j \in \{0, 1, \ldots, N-1\}, \end{aligned}$$

while the inverse mapping is given by

$$\begin{aligned} &\mu^{-1}(\eta)(i, j) = \delta(i, j) = \frac{1 - \eta(i, j)}{2} \\ &\qquad \text{for } i \in \{0, 1, \ldots, M-1\},\ j \in \{0, 1, \ldots, N-1\}. \end{aligned}$$

Thus the correlation of order k of the bit (M, N)-lattice δ can be defined by

$$\begin{aligned} C_k(\delta) = C_k(\mu(\delta)) = C_k(\eta) &= \max_{B', \mathbf{d_1}, \ldots, \mathbf{d_k}} \left| \sum_{\mathbf{x} \in B'} \eta(\mathbf{x} + \mathbf{d_1}) \cdots \eta(\mathbf{x} + \mathbf{d_k}) \right| \\ &= \max_{B', \mathbf{d_1}, \ldots, \mathbf{d_k}} \left| \sum_{\mathbf{x} \in B'} (-1)^{\delta(\mathbf{x}+\mathbf{d_1}) + \cdots + \delta(\mathbf{x}+\mathbf{d_k})} \right| \end{aligned}$$

(where $B', \mathbf{d_1}, \dots, \mathbf{d_k}$ are defined as in (2.1)).

The most natural definition of the linear complexity of two dimensional bit (M, N)-lattice seems to be to use double (two variable) linear recursions instead of the linear recursions used in Definition 1:

Definition 5 *Let δ be a bit (M, N)-lattice, and write $\delta(i, j) = s_{i,j}$ for $i = 0, 1, \dots, M-1$, $j = 0, 1, \dots, N-1$. Then the linear complexity $L(\delta)$ (over the field $\mathbb{F}_2$) of the lattice δ is the smallest non-negative integer L that can be written in the form $L = (U+1)(V+1) - 1$ where U, V are integers with $0 \le U < M$, $0 \le V < N$ such that the $M \times N$ matrix $(s_{i,j})$ satisfies a double (two variable) linear recursion over $\mathbb{F}_2$ of form*

$$s_{m+U,n+V} = \sum_{\substack{\max\{0,-m\} \le i \le U \\ \max\{0,-n\} \le j \le V \\ (i,j) \ne (U,V)}} c_{i,j} s_{m+i,n+j} \tag{3.1}$$

for all integers m, n with

$$(m,n) \in \{(m,n):\ 0 < m < M-U,\ -V \le n < N-V\} \\ \cup \{(m,n):\ 0 < n < N-V,\ -U \le m < M-U\} \cup \{(0,0)\}$$

with the convention that $L(\delta) = 0$ if $s_{i,j} = 0$ for all $0 \le i \le M-1$, $0 \le j \le N-1$, and $L(\delta) = MN$ if $s_{i,j} = 0$ for all $0 \le i \le M-1$, $0 \le j \le N-1$, $(i,j) \ne (M-1, N-1)$ and $s_{M-1,N-1} = 1$.

(Note that the number $(U+1)(V+1) - 1$ defining L is the number of terms on the right hand side of (3.1) for $m \ge 0, n \ge 0$.)

To understand this definition better, observe that Definition 1 can be rewritten in the following equivalent form:

Definition 1' *Consider the bit sequence S_N in (1.1), and assign the polynomial*

$$f(x) = \sum_{n=0}^{N-1} s_n x^n \in \mathbb{F}_2[x]$$

to it. Then the linear complexity of S_N is defined as the smallest positive integer L such that there is a polynomial of form

$$g(x) = \sum_{i=1}^{L} c_{L-i} x^i \in \mathbb{F}_2[x] \tag{3.2}$$

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 $0 \le n < L$.

Using this approach, Definition 5 can be rewritten in the following equivalent form:

Definition 5' *Define the bit lattice δ as in Definition 5, and assign the polynomial*

$$f(x,y) = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} s_{m,n} x^m y^n \in \mathbb{F}_2[x,y]$$

to it. 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

$$g(x,y) = \sum_{\substack{0 \le i \le U \\ 0 \le j \le V \\ (i,j) \ne (0,0)}} c_{U-i,V-j} x^i y^j \in \mathbb{F}_2[x,y] \tag{3.3}$$

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 $0 \le m < N$, $0 \le n < N$ except for the terms $x^m y^n$ with $0 \le m \le U$, $0 \le n \le V$, $(m,n) \ne (U,V)$.

Note that while in (3.2) L is the number of the terms of the polynomial $g(x)$ (containing also the terms with 0 coefficient), in Definition 5' $L = (U+1)(V+1) - 1$ is the number of the terms of the polynomial $g(x,y)$ in (3.3). This shows that, indeed, Definition 5 is the natural extension of Definition 1 to two dimensions.

Now consider that special case of Definition 5 when δ is an $(N,1)$ bit lattice:

$$\delta(\mathbf{x}): \; I_{N,1} \to \{1, 0\}. \tag{3.4}$$

Then the matrix $(\delta(i,j)) = (s_{i,j})$ becomes a bit sequence of length N:

$$S_N \stackrel{\text{def}}{=} (\delta(0,0), \delta(1,0), \ldots, \delta(N-1,0)) = (s_{0,0}, s_{1,0}, \ldots, s_{N-1,0}). \qquad (3.5)$$

On the other hand, specifying Definition 5 to the case (3.4) we get that now L is defined as the smallest non-negative integer L that can be written in the form $L = (U+1)(V+1) - 1$ where U, V are integers with $0 \le U < N$, $0 \le V < 1$ so that the $N \times 1$ matrix $(s_{i,j})$, i.e., the sequence (3.5) satisfies the recursion (3.1) for all integers m, n satisfying one of the conditions

$$0 < m < N - U, \ -V \le n < 1 - V, \qquad (3.6)$$

$$0 < n < 1 - V, \ -U \le m < N - U, \qquad (3.7)$$

$$m = n = 0. \qquad (3.8)$$

It follows from the condition $0 \le V < 1$ that

$$V = 0. \qquad (3.9)$$

Then clearly, there is no integer satisfying the first inequality in (3.7), while the second inequality in (3.6) becomes $0 \le n < 1$ whence

$$n = 0. \qquad (3.10)$$

The second and third condition of the summation in (3.1) becomes

$$j = V = 0 \qquad (3.11)$$

and

$$i \ne U, \qquad (3.12)$$

respectively. By the first inequality in (3.6), (3.8), (3.9), (3.10), (3.11) and (3.12), now (3.1) is of the form

$$s_{m+U,0} = \sum_{i=0}^{U-1} c_{i,0} s_{m+i,0} \quad \text{for } m = 0, 1, \ldots, N - U - 1. \qquad (3.13)$$

Since now $V = 0$ is fixed, we are looking for the smallest non-negative integer U in $(L(\eta) =)(U+1)(V+1)-1$ such that (3.13) holds. Comparing this with equation (1.2) in Definition 1 we see immediately that this U is the linear complexity of the bit sequence S_n in (3.3): $U = L(S_N)$. It follows that the linear complexity of the bit lattice δ is

$$L(\delta) = (U+1)(V+1) - 1 = (L(S_N)+1)(0+1) - 1 = L(S_N)$$

thus $L(\delta)$ and $L(S_N)$ coincide (and this is also so when $L(\delta)$ and $L(S_N)$ are given by the convention at the end of Definition 1 and 5, respectively; we leave the details to the reader). This means that the two dimensional definition (Definition 5) includes the one dimensional definition (Definition 1) as a special case thus, indeed, the former is an extension of the latter.

As in the one dimensional case in (1.7), we may define the linear complexity of the *binary* (M,N)*-lattice* η by

$$L(\eta) = L(\mu^{-1}(\eta)).$$

Clearly, the maximal value of the linear complexity of bit (resp. binary) (M,N)-lattices is MN, and by Rueppel's theorem [17] on the linear complexity of a truly random binary sequence one may guess that there is a $c > 0$ such that the linear complexity of a truly random bit (or binary) (M,N)-lattice is greater than cMN; if this is true, then a "good" pseudorandom bit $(M,N) - lattice$ must have large linear complexity, and the lattices of small linear complexity are useless in the applications. Indeed, we conjecture the following:

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

We can prove the lower bound part of this conjecture and also a slightly weaker upper bound. However, the proofs are lengthy and complicated, thus we will present these results only in Part II of this paper.

4 The linear complexity of a bit lattice and of the associated bit sequence

In [10] we showed that the study of two dimensional binary lattices cannot be reduced to the one dimensional case in a certain sense. We will show that in the case of the linear complexity the situation is the same.

To any bit (M, N)-lattice

$$\delta(\mathbf{x}) : \; I_{M,N} \to \{1, 0\} \tag{4.1}$$

we may assign a unique bit sequence $S_{MN} = S_{MN}(\delta) = (s_0, s_1, \ldots, s_{MN-1}) \in \{0,1\}^{MN}$ by taking the first (from the bottom) row of the lattice (4.1) then we continue the bit sequence by taking the second row of the lattice, then the third row follows, etc; in general, we set

$$s_{iM+j} = \delta(j, i) \quad \text{ for } i = 0, 1, \ldots, N-1, j = 0, 1, \ldots, M-1.$$

It is a natural question to ask: is it true that if $L(S_{MN})$ is large, then the δ bit (M, N)-lattice also has large linear complexity? Namely, then "good" binary bit sequences would generate "good" bit lattices automatically, thus it would be sufficient to study bit sequences, there would be no need for developing a theory of linear complexity of bit lattices. The answer to this question is negative.

Theorem 1 *For every M and $N \geq 3$ there is a bit lattice $\delta(\mathbf{x}) : \; I_{M,N} \to \{0, 1\}$ such that $L(S_{MN}(\delta))$ is "large":*

$$L(S_{MN}(\delta)) = M(N-1) + 2, \tag{4.2}$$

however, $L(\delta)$ is "small":

$$L(\delta) \leq 3N - 1. \tag{4.3}$$

Proof of Theorem 1. Define $\delta(\mathbf{x}):\ I_{M,N}\to\{0,1\}$ by

$$\delta(i,j)=\begin{cases}0 & \text{if } j\le N-2,\\ 0 & \text{if } j=N-1,\ i=0,\\ 1 & \text{if } j=N-1,\ 0<i.\end{cases}$$

Then $S_{MN}(\delta)=(s_0,s_1,\dots,s_{MN-1})$ where

$$s_i=\begin{cases}0 & \text{if } i\le M(N-1),\\ 1 & \text{if } i>M(N-1).\end{cases}$$

By definition, let $S^t_{MN}(\delta)$ be the sequence formed by the first t elements of $S_{MN}(\delta)$, thus $S^t_{MN}(\delta)=(s_0,s_1,\dots,s_{t-1})$. Then $S^{M(N-1)+2}_{MN}=(0,0,\dots,0,1)$, thus by Definition 1

$$L(S^{M(N-1)+2}_{MN})=M(N-1)+2. \tag{4.4}$$

By the sharper version of Lemma 1 in Massey's paper [14] if $L(S^t_{MN})\neq L(S^{t+1}_{MN})$, then there is a linear recursion of form (1.2) which is of length $L(S^t_{MN})$ and it generates $s_0,s_1,\dots,s_{t-1}$ but not $s_0,s_1,\dots,s_t$, and then

$$L(S^{t+1}_{MN})=\max\{L(S^t_{MN}),t+1-L(S^t_{MN})\}. \tag{4.5}$$

We will prove by induction on t that for $M(N-1)+2\le t\le MN$ we have

$$L(S^t_{MN})=M(N-1)+2. \tag{4.6}$$

Indeed, for $t=M(N-1)+2$ the statement is true by (4.4). Suppose that for $t=k$ (where $M(N-1)+2\le k\le MN-1$) (4.4) holds; then we will prove that for $t=k+1$ (4.5) is also true. By the induction hypothesis

$$L(S^k_{MN})=M(N-1)+2. \tag{4.7}$$

Thus

$$\begin{aligned}\max\{L(S^k_{MN}),k+1-L(S^k_{MN})\}&=\max\{M(N-1)+2,k-M(N-1)-1\}\\ &=M(N-1)+2=L(S^k_{MN}).\end{aligned} \tag{4.8}$$

(Indeed (4.8) is equivalent with

$$\begin{aligned} M(N-1)+2 &\geq k - M(N-1) - 1, \\ 2M(N-1)+3 &\geq k \end{aligned}$$

which follows from

$$\begin{aligned} 2M(N-1)+3 &\geq MN-1 \\ MN-2M+4 &\geq 0. \end{aligned}$$

Since $N \geq 3$ this last inequality holds.) Thus (4.8) holds. We will prove

$$L(S_{MN}^{k+1}) = L(S_{MN}^{k}). \tag{4.9}$$

Indeed, if $L(S_{MN}^{k+1}) \neq L(S_{MN}^{k})$, then by (4.5) we have

$$L(S_{MN}^{k+1}) = \max\{L(S_{MN}^{k}), k+1-L(S_{MN}^{k})\}.$$

But by (4.8) we have $L(S_{MN}^{k+1}) = L(S_{MN}^{k})$ which is a contradiction. By (4.7) and (4.9) we have

$$L(S_{MN}^{k+1}) = M(N-1)+2$$

which proves (4.2).

Next we prove (4.3). Let $U = 2, V = N-1$ and for $0 \leq i \leq U$, $0 \leq j \leq V$, $(i,j) \neq (U,V)$ define the constants $c_{i,j}$ by

$$c_{i,j} = \begin{cases} 1 & \text{if } (i,j) = (1, N-1) \\ 0 & \text{otherwise.} \end{cases}$$

Then it is easy to see that

$$s_{m+U,n+V} = \sum_{\substack{\max\{0,-m\} \leq i \leq U \\ \max\{0,-n\} \leq j \leq V \\ (i,j) \neq (u,v)}} c_{i,j} s_{m+i,n+j} = s_{m+U-1,N+V}$$

for all integers m, n with

$$\begin{aligned} (m,n) \in &\{(m,n): \ 0 < m < M-U, \ -V \leq n < N-V\} \cup \\ &\{(m,n): \ 0 < n < N-V, \ -U \leq m < M-U\} \cup \{(0,0)\}. \end{aligned}$$

Thus by Definition 5

$$L(\delta) \le 3N - 1$$

which proves (4.3).

5 Large linear complexity is not enough

By Theorem 1 a "pseudorandom type" bit lattice must have large linear complexity. On the other hand, large linear complexity is only one of the pseudorandom properties, it is not enough to guarantee the pseudorandom nature of the lattice. We will illustrate this by an example:

Example 1 *Let $M, K \in \mathbb{N}$, $N = 2K$. Define the $\delta(\mathbf{x}) : \ I_{M.N} \to \{0,1\}$ bit (M,N)-lattice by*

$$\delta(i,j) = \begin{cases} 0 & \textit{for } (i,j) \neq (M-1, K-1),\ (i,j) \neq (M-1, 2K-1) \\ 1 & \textit{for } (i,j) = (M-1, K-1) \textit{ and } (i,j) = (M-1, 2K-1). \end{cases}$$

Then by restricting δ to $I_{M,K}$, by the last convention in Definition 5 the linear complexity of this restricted bit lattice is MK. It is easy to see that extending a bit lattice, the linear complexity of the extended one is at least as large as of the original one, thus considering δ on $I_{M,N}$, the linear complexity of this extended lattice is also at least $MK = \frac{MN}{2}$, thus it is optimally large.

On the other hand, writing $B' = I_{M,K}$, $\mathbf{d} = (0, K)$, the correlation of order 2 of δ is large:

$$C_2(\delta) \ge \left| \sum_{\mathbf{x} \in B'} (-1)^{\delta(\mathbf{x}) + \delta(\mathbf{x}+\mathbf{d})} \right| = \left| \sum_{\mathbf{x} \in B'} (-1)^{2\delta(\mathbf{x})} \right| = \sum_{\mathbf{x} \in B'} 1 = MK = \frac{MN}{2}$$

thus δ cannot be considered a "good" pseudorandom lattice, it certainly possesses a very special, not random type structure.

6 Estimate of the linear complexity in terms of the correlation

As Theorems A and B show, in one dimension, i.e., in case of binary sequences the linear complexity can be estimated in terms of the correlation. Now we will show that in two dimensions the situation is the same, and we will be able to adapt the methods of the proofs of both Theorems A and B for proving theorems of this type, although here we have to formulate the results in a slightly different way. (Note that as Example 1 in the previous section shows nothing can be proved in the opposite direction, i.e., one cannot give upper bound for the correlation in terms of the linear complexity.) To simplify the discussion we will restrict ourselves to the case $M = N$, i.e., to bit (N, N)-lattices.

Theorem 2 *Let $N \in \mathbb{N}$, and let δ be a bit (N, N)-lattice. Then either the linear complexity $L = L(\delta)$ of δ satisfies $L > N/2$ or we have*

$$\frac{N^2}{4} \leq \max_{k \leq L+1} C_k(\delta). \tag{6.1}$$

Proof of Theorem 2. We have to show that assuming

$$L \leq N/2 \tag{6.2}$$

(6.1) must hold. Define U, V as in Definition 5 thus

$$L = (U + 1)(V + 1) - 1 \tag{6.3}$$

and (3.1) holds with some $c_{i,j} \in \mathbb{F}_2$, $0 \leq i \leq U$, $0 \leq j \leq V$, $(i, j) \neq (U, V)$ and with $s_{i,j} = \delta(i, j)$ for all $0 \leq i, j < N$. Since $V \geq 0$ it follows from (6.3) that

$$L + 1 \geq U + 1$$

whence, by (6.2)

$$U \leq L \leq N/2 \tag{6.4}$$

and in the same way

$$V \leq N/2. \tag{6.5}$$

Now set $c_{U,V} = 1$. Then (3.1) can be rewritten (in $\mathbb{F}_2$) as

$$0 = \sum_{i,j} c_{i,j} s_{m+i,n+j} \tag{6.6}$$

where i, j run over the same integers as in (3.1) but also including $(i, j) = (U, V)$, and this holds for every (m, n) belonging to the union of the 3 sets presented after (3.1). It follows form (6.6) that

$$(-1)^{\sum_{i,j} c_{i,j} s_{m+i,n+j}} = 1 \tag{6.7}$$

for every (m, n) belonging to the union of the 3 sets described above. Observe that every pair (m, n) with

$$0 \leq m < M - U (= N - U), \ 0 \leq n < N - V \tag{6.8}$$

belongs to this union, and for these pairs the summation $\sum_{i,j}$ simplifies to $\sum_{\substack{0 \leq i \leq U \\ 0 \leq j \leq V}}$ (independently of m, n). Adding (6.7) for every (m, n) satisfying (6.8), by (6.4) and (6.5) we get

$$\sum_{\substack{0 \leq m < N-U \\ 0 \leq n < N-V}} (-1)^{\sum_{i,j} c_{i,j} s_{m+i,n+j}} = (N - U)(N - V) \geq \frac{N^2}{4}. \tag{6.9}$$

Writing $B' = \{(m, n) : \ 0 \leq m < M - U, \ 0 \leq n < N - V\}$ and $\mathcal{D} = \{\mathbf{d_1}, \ldots, \mathbf{d_k}\} = \{(i, j) : \ 0 \leq i \leq U, \ 0 \leq j \leq V, \ c_{i,j} = 1\}$ the left hand side of (6.9) can be rewritten as

$$\sum_{\mathbf{x} \in B'} (-1)^{\delta(\mathbf{x}+\mathbf{d_1}) + \cdots + \delta(\mathbf{x}+\mathbf{d_k})}.$$

By the definition of $C_k(\delta)$ this is not greater than $C_k(\delta)$ with

$$k = |\mathcal{D}| \leq |\{(i, j) : \ 0 \leq i \leq U, \ 0 \leq j \leq V\}| = (U + 1)(V + 1) = L + 1$$

and this completes the proof of the theorem.

In [3] Brandstätter and Winterhof presented several applications of their Theorem A. Among others, they estimated the linear complexity profile of the Legendre symbol sequence $E_{p-1} = \left(\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \dots, \left(\frac{p-1}{p}\right)\right)$ by using also the estimates for the correlation of order k of this sequence given by Mauduit and Sárközy in [15]. Here in two dimensions the situation is similar: one can use our Theorem 2 for estimating the linear complexity of a two dimensional extension of this Legendre symbol construction presented by Hubert, Mauduit and Sárközy in [12] by applying their estimates for the correlation of the lattice.

Theorem 3 *Let p be a prime, let γ denote the quadratic character of $\mathbb{F}_{p^2}$, and let v_1, v_2 be a basis of $\mathbb{F}_{p^2}$ as a vector space over $\mathbb{F}_p$. Then define the (2-dimensional) binary (p,p)-lattice $\eta: I_p^2 \to \{-1,+1\}$ by*

$$\eta(\mathbf{x}) = \eta(x_1, x_2) = \begin{cases} \gamma(x_1 v_1 + x_2 v_2) & \textit{for } (x_1,x_2) \neq (0,0), \\ 1 & \textit{for } (x_1,x_2) = (0,0) \end{cases}$$

for any $x_1, x_2 \in \mathbb{F}_p$, and let $\delta = \mu^{-1}(\eta)$ denote the bit lattice associated with the binary lattice η in the sense described in Section 3. Then for p large enough we have

$$L(\delta) > \frac{p}{5(\log p)^2}. \tag{6.10}$$

Proof of Theorem 3. We have

$$C_k(\delta) = C_k(\eta) \leq Q_k(\eta) \quad \text{for every } k \in \mathbb{N}, \tag{6.11}$$

and by Theorem 2 in [12] we have

$$Q_k(\eta) < kp(1 + \log p)^2 \quad \text{for every } k \in \mathbb{N}. \tag{6.12}$$

If $L > p/2$, then (6.10) holds for p large enough. Thus it suffices to show that (6.10) also follows from (6.1) (with p in place of N), i.e., from

$$\frac{p^2}{4} \leq \max_{k \leq L+1} C_k(\delta). \tag{6.13}$$

By (6.11) and (6.12) we have

$$\max_{k\le L+1} C_k(\delta) < \max_{k\le L+1} kp(1+\log p)^2 \le (L+1)p(1+\log p)^2. \tag{6.14}$$

It follows from (6.13) and (6.14) that

$$L+1 > \frac{p}{4(1+\log p)^2}$$

whence

$$L > \frac{p}{4(1+\log p)^2} - 1 > \frac{p}{5(\log p)^2}$$

for p large enough thus, indeed, (6.10) holds.

Theorem 4 *Let $N \in \mathbb{N}$, and let δ be a bit (N,N)-lattice. If N is large enough, then we have*

$$2^{L(\delta)} > \frac{N^2}{16} - C_2(\delta). \tag{6.15}$$

We remark that by using this theorem one cannot get better lower bound for $L(\delta)$ than $c\log N$. However, using only the correlation of order 2 one cannot expect a better bound; the computational evidence presented by Andics [2] seems to indicate that there are (N,N)-lattices δ with $L(\delta) = O(\log N)$ and small $C_2(\delta)$.

Proof of Theorem 4. If $L = L(\delta) \ge \frac{2}{\log 2}\log N - 4$, then we have

$$2^L \ge \frac{N^2}{16}$$

thus (6.15) holds trivially. Thus we may assume that

$$L \le \frac{2}{\log 2}\log N - 4. \tag{6.16}$$

Define U, V as in Definition 5 thus again (6.3) holds and

$$\max(U,V) \le L \le \frac{2}{\log 2}\log N - 4, \tag{6.17}$$

and assume that (3.1) holds with some $c_{i,j} \in \mathbb{F}_2$, $0 \le i \le U$, $0 \le j \le V$, $(i,j) \neq (U,V)$ and with $s_{i,j} = \delta(i,j)$ for all $0 \le i, j < N$. For every

$$(x,y) \in \left\{0, 1, \dots, \left[\frac{N}{4}\right]\right\}^2, \tag{6.18}$$

consider the values of the bits

$$s_{x+i,y+j} \text{ with } 0 \le i \le U,\ 0 \le j \le V,\ (i,j) \neq (U,V). \tag{6.19}$$

The number of these bits is $(U+1)(V+1) - 1 = L$, thus by (6.17) their values can be chosen in at most

$$2^L \le 2^{\frac{2}{\log 2}\log N - 4} = \frac{N^2}{16}$$

ways. On the other hand, the number of points (x,y) in (6.18) is

$$\left(\left[\frac{N}{4}\right] + 1\right)^2 > \left(\frac{N}{4}\right)^2 = \frac{N^2}{16},$$

thus by the pigeon hole principle there are two pints $(x_1, y_1) \neq (x_2, y_2)$ with

$$0 \le x_1, y_1, x_2, y_2 \le \left[\frac{N}{4}\right] \tag{6.20}$$

thus replacing (x,y) in (6.19) first by (x_1, y_1) and then by (x_2, y_2) we get the same bits:

$$s_{x_1+i,y_1+j} = s_{x_2+i,y_2+j} \quad \text{for } 0 \le i \le U,\ 0 \le j \le V,\ (i,j) \neq (U,V).$$

By the recursion (3.1) it follows that we have

$$\delta(x_1+i, y_1+j) = s_{x_1+i,y_1+j} = s_{x_2+i,y_2+j} = \delta(x_2+i, y_2+j)$$

for every $0 \le i \le N-1-\max(x_1,x_2)$, $0 \le j \le N-1-\max(y_1,y_2)$.

Write

$$\begin{aligned} B' = \{(i,j) : \ & i \in 0, 1, \dots, N-1-\max(x_1,x_2), \\ & j \in 0, 1, \dots, N-1-\max(y_1,y_2)\} \end{aligned}$$

and

$$\mathbf{d_1} = (x_1, y_1),\ \mathbf{d_2} = (x_2, y_2).$$

Thus by the definition of C_k and (6.20) we have

$$\begin{aligned}
C_2(\delta) &\geq \left| \sum_{\mathbf{x} \in B'} (-1)^{\delta(\mathbf{x}+\mathbf{d_1})+\delta(\mathbf{x}+\mathbf{d_2})} \right| = \sum_{\mathbf{x} \in B'} 1 = |B'| \\
&= (N - \max(x_1, x_2))(N - \max(y_1, y_2)) \geq \left(N - \left[\frac{N}{4} \right] \right)^2 \\
&> \left(\frac{N}{2} \right)^2 = \frac{N^2}{4} > \frac{N^2}{16} - 2^L
\end{aligned}$$

which proves (6.15).

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. 95 (2007), 778-812.

[2] Á. Andics, *On the linear complexity of binary sequences*, Annales Univ. Sci. Budapest. 48 (2005), 173-180.

[3] N. Brandstätter and A. Winterhof, *Linear complexity profile of binary sequences with small correlation measure*, Periodica Math. Hungar. 52 (2006), 1-8.

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

[5] Z. Chen and A. Winterhof, *Linear complexity profile of m-ary pseudorandom sequences with small correlation measure*, Indag. Math. (N.S.) 20 (2009), 631-640.

[6] X. Feng and Z. Dai, *Expected value of the linear complexity of two-dimensional binary sequences*, in: SETA 2004, eds. T. Helleseth et al., LNCS 3486, Springer-Verlag, Berlin, 2005; pp. 113-128.

[7] 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.

[8] 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.

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

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

[11] K. Gyarmati, A. Sárközy and C. L. Stewart, *On Legendre symbol lattices*, Unif. Distrib. Theory 4 (2009), 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, 159-169, TUCS Gen. Publ. 27, Turku Cent. Comput. Sci., Turku, 2003.

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

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

[16] A. Menezes, P. C. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRS Press, Boca Raton, 1997.

[17] R. A. Rueppel, *Linear complexity and Random Sequences*, Proc. Advances in Cryptology - EUROCRYPT '85, Linz, Austria, April 9-12, 1985, LNCS 219, pp. 167-188.

[18] A. Winterhof, *Linear complexity and related complexity measures*, in: Selected Topics in Information and Coding Theory, eds. I, Woungang et al., World Scientific Publishing Co., 2010.