On linear complexity of binary lattices, II

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, CMR 6206,

163 avenue de Luminy, 13288 Marseille cedex 9, France

e-mail: mauduit@iml.univ-mrs.fr

András Sárközy

Eötvös Loránd University

Department of Algebra and Number Theory

H-1117 Budapest, Pázmány Péter sétány 1/C, Hungary

e-mail: sarkozy@cs.elte.hu

2010 Mathematics Subject Classification: Primary 11K45.

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

Research partially supported by ERC-AdG.228005, 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 MUNUM and French-Hungarian exchange program TÉT-09-01-2010-0056.

Abstract

The linear complexity is an important and frequently used measure of unpredictably and pseudorandomness of binary sequences. In Part I of this paper we extended this notion to two dimensions: we defined and studied the linear complexity of binary and bit lattices. In this paper first we will estimate the linear complexity of a truly random bit (M, N)-lattice. Next we will extend the notion of k-error linear complexity to bit lattices. Finally, we will present another alternative definition of linear complexity of bit lattices.

1 Introduction

The linear complexity is an important and frequently used measure of pseudorandomness of bit sequences which is closely related to the 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 the 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 (periodic) bit sequences, and one may also study linear complexity over other finite fields $\mathbb{F}_q$ but we will not need these definitions here.

Pseudorandomness of bit sequences also has other important quantitative measures. In particular Mauduit and Sárközy [8] introduced the well-distribution measure $W(E_N)$, correlation measure $C_k(E_N)$ of order k and the combined (well-distribution-correlation) measure $Q_k(E_N)$ of order k of binary sequences

$$E_N = (e_0, e_1, \dots, e_{N-1}) \in \{-1, +1\}^N \tag{1.3}$$

(the definition of these measures is presented in Part I [2], here we will not need these definitions). 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 (1.3), 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

$$\begin{aligned} \varphi(S_N) = \varphi((s_0, s_1, \dots, s_{N-1})) = E_N = (e_0, e_1, \dots, e_{N-1}) \text{ with} \\ e_i = (-1)^{s_i} \ (= 1 - 2s_i) \text{ for } i = 0, 1, \dots, N-1, \end{aligned} \tag{1.4}$$

while the inverse mapping is given by

$$\begin{aligned} \varphi^{-1}(E_N) = \varphi^{-1}((e_0, e_1, \dots, e_{N-1})) = S_N = (s_0, s_1, \dots, s_{N-1}) \text{ with} \\ s_i = \frac{1 - e_i}{2} \text{ for } i = 0, 1, \dots, N-1. \end{aligned}$$

Then the linear complexity of the binary sequence E_N in (1.3) can be defined by

$$L(E_N) = L(\varphi^{-1}(E_N)) = L(S_N).. \tag{1.5}$$

In [6] Hubert, Mauduit and Sárközy extended the notion of binary sequence and the measure Q_k of pseudorandomness to n dimensions. As in Part I we will restrict ourselves to the $n = 2$ special case, the case of general n could be handled similarly.

For $M, N \in \mathbb{N}$ let $I_{M,N}$ denote the lattice point rectangle

$$I_{M,N} = \{(x, y) : \ x \in \{0, 1, \dots, M-1\}, \ y \in \{0, 1, \dots, N-1\}\}. \tag{1.6}$$

Definition 2 *A function of type* $\eta(\mathbf{x}): \ I_{M,N} \to \{-1,+1\}$ *is called a* binary $(M.N)$-lattice*.*

(Note that in [6] and other earlier papers only the $M = N$ special case was studied, the case of general pairs M, N was introduced only in Part I of this paper, and all the earlier definitions and nearly all the earlier results can be extended to this general case.) Replacing all η values equal to $+1$ by 0 and all values equal to -1 by $+1$ we get a function of type $\delta(\mathbf{x}) \to \{1, 0\}$.

Definition 3 *A function of type* $\delta(\mathbf{x}) \to \{1, 0\}$ *is called* bit (M, N)-lattice*.*

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

$$\begin{aligned}\eta(i,j) = \mathbf{\Phi}\delta(i,j) = (-1)^{\delta(i,j)} \ (= 1 - 2\delta(i,j)) \text{ for} \\ i \in \{0, 1, \ldots, M-1\}, \ j \in \{0, 1, \ldots, N-1\},\end{aligned} \tag{1.7}$$

while the inverse mapping is given by

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

In [6] and [3] we extended the definitions of the measures Q_k resp. C_k of pseudorandomness from one dimension to n dimensions (while the measure W is the $k = 1$ special case of the measure Q_k) we will not need these definitions here. (See also [4] and [5], and we also recalled these definitions in Part I.) In this series our goal is to continue the work by defining and studying *the linear complexity of bit (and binary) lattices.*

In Part I we gave two equivalent definitions for the linear complexity of bit lattices:

Definition 4 *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 $0 \le U < M$, $0 \le V < N$ so that the $M \times N$ matrix $(s_{i,j})$ satisfies a double (two variable) linear recursion over $\mathbb{F}_2$ of form*

$$s_{m+U,n+V} = \sum_{\substack{\max\{0,-m\}\le i\le U \\ \max\{0,-n\}\le j\le V \\ (i,j)\ne(U,V)}} c_{i,j} s_{m+i,n+j} \tag{1.8}$$

for all integers m, n with

$$\begin{aligned}(m,n) \in \{(m,n):\ 0 < m < M-U,\ -V \le n < N-V\}\cup \\ \cup\{(m,n):\ 0 < n < N-V,\ -U \le m < M-U\} \cup \{(0,0)\}\end{aligned} \tag{1.9}$$

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 (1.8) for $m \ge 0, n \ge 0$.)

Definition 4' *Define the bit lattice δ as in Definition 4, 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 so that there is a polynomial

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

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

As in the one dimensional case in (1.5), the linear complexity of the *binary* (M, N)*-lattice* η in (1.7) can be defined by

$$L(\eta) = L(\mathbf{\Phi}^{-1}\eta) = L(\delta).$$

Example 1 *Let* M, N, K *be positive integers with* $K < M$, *and define the* $M \times N$ *bit lattice* δ *by*

$$\delta(i, j) = s_{i,j} = \begin{cases} 0 & \textit{if } 0 \le i \le K - 1 \\ 1 & \textit{if } K \le i \le M - 1 \end{cases}$$

for $i \in \{0, 1, \ldots, M - 1\}$, $j \in \{0, 1, \ldots, N - 1\}$. *Then using the notations above* (1.8) *becomes*

$$s_{m+K+1,n} = s_{m+K,n}$$

for the pairs (m, n) *given in* (1.9) *with*

$$U = K + 1,\ V = 0,$$

and we have

$$L = (U + 1)(V + 1) - 1 = K + 1.$$

Moreover we have

$$f(x, y) = \sum_{m=K}^{M-1} \sum_{n=0}^{N-1} x^m y^n$$

and

$$g(x, y) = x.$$

(Here and the other examples later we will present only the facts and the values of the parameters, we leave the details and the computations to the reader.)

Example 2 *Let N, d be positive integers with $d \mid N$, and define the $N \times N$ bit lattice δ by*

$$\delta(i,j) = s_{i,j} = \begin{cases} 0 & \text{if } i \neq j, \text{ or } i = j \text{ but } d \nmid i \\ 1 & \text{if } i = j \text{ and } d \mid i \end{cases}$$

for $i \in \{0, 1, \dots, N-1\}$, $j \in \{0, 1, \dots, N-1\}$. Then (1.8) *becomes*

$$s_{m+d,n+d} = s_{m,n} \tag{1.10}$$

for the pairs (m, n) given in (1.9) *with*

$$U = V = d,$$

and we have

$$L = (U+1)(V+1) - 1 = (d+1)^2 - 1 = d^2 + 2d. \tag{1.11}$$

Moreover we have

$$f(x,y) = \sum_{k=0}^{N/d-1} (xy)^{kd}$$

and

$$g(x,y) = (xy)^d.$$

In Part I we proved that the $N = 1$ special case of Definition 4 for the linear complexity of bit (M, N)-lattices is identical with the one dimensional definition of linear complexity; we showed that the study of the linear complexity (of two dimensional binary lattices) cannot be reduced to the one dimensional case by studying the linear complexity of the binary sequence which can be assigned to the given binary lattice in the natural way; we also showed that to guarantee the pseudorandomness of a bit lattice it is not enough to estimate the linear complexity of it since it may occur that the linear complexity is large, however, the correlation is also extremely large; we studied the connection between the linear complexity of a bit lattice δ and the correlations $C_k(\delta)$ of it; we applied the inequalities obtained in this way for estimating the linear complexity of an important special binary lattice studied in an earlier paper.

Moreover, we wrote in Part I about the continuation of our program to be presented in Part II:

"Clearly, the maximal value of the linear complexity of bit (resp. binary) (M, N)-lattices is MN, and by Rueppel's theorem [9] on the linear complexity of a (truly) random binary sequence one may guess that there is a $c > 0$ so 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." (Here and in what follows we use the word "random" in the same sense as it is used in Rueppel's paper, i.e. each of the 2^N bit sequences is selected with probability $1/2^N$and later each of the 2^{MN} $(M \times N)$ bit lattices will be selected with probability $1/2^{MN}$ We will sometimes also say "(truly) random" bit sequence or lattice not to mistake it for a pseudorandom one, or a special one prepared by a physical device, etc. When we say that a random bit sequence of length N or $M \times N$ bit lattice possesses a certain property then we mean that this property holds with probability approaching 1 as N, resp. MN tends to infinity.) "Indeed, we conjecture the following:

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

Indeed, this is true for $(N, 1)$-lattices. Namely, as we have seen in Section 3 of Part I, there is a one-to-one correspondence between bit $(N, 1)$-lattices $\delta : I_{N,1} \to \{1, 0\}$ and bit sequences

$$S_N \in \{1, 0\}^N \tag{1.12}$$

of length N with $L(\delta) = L(S_N)$, and for a random bit sequence of type (1.12) we have

$$L(S_N) = \left(\frac{1}{2} + o(1)\right) N$$

by Rueppel's theorem which proves Conjecture 1 in this special case.

We continued in Part I:

"We can prove the lower bound part of this conjecture and also a slightly weaker upper bound." (The difficulty in proving the upper bound is that the proof of Rueppel's theorem on bit sequences is based on the Berlekamp-Massey algorithm for determining the linear complexity of a sequence, and we have not been able to extend this algorithm to 2 dimensions.) "However, the proofs are lengthy and complicated, thus we will present these results only in Part II of this paper."

Indeed, in this paper first we will prove the lower bound in Section 2, while the upper bound will be proved in Section 3. In Section 4 we will define and study the k-error linear complexity of binary (or bit) (M, N)-lattices. Finally, in Section 5 we will present an alternative extension of the one dimensional linear complexity notion to two dimensions.

2 Lower bound for the linear complexity of a random bit (M, N)-lattice

We will prove

Theorem 1 *For every $\varepsilon_1 > 0$, $\varepsilon_2 > 0$ there is a number $C = C(\varepsilon_1, \varepsilon_2)$ 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*

$$P\left(L(\delta) > \frac{1}{2}MN - \left(\frac{1}{2} + \varepsilon_1\right)\frac{\log MN}{\log\log MN}\right) > 1 - \varepsilon_2. \tag{2.1}$$

Proof of Theorem 1.

We will need

Lemma 1 *For every integer K with $0 < K < MN$ we have*

$$|\{\delta :\ I_{M,N} \to \{1,0\},\ L(\delta) = K\}| \leq \tau(K+1)2^{2K} \tag{2.2}$$

where $\tau(n)$ denotes the number of positive divisors of n.

Proof of Lemma 1. Let $\delta :\ I_{M,N} \to \{1,0\}$ be a bit (M,N)-lattice with

$$L(\delta) = K, \tag{2.3}$$

and write $\delta(i,j) = s_{i,j}$ for $i = 0,1,\dots,M-1$, $j = 0,1,\dots,N-1$. Then by Definition 4 and (2.3), there are non-negative integers U, V and coefficients $c_{i,j}(\in \mathbb{F}_2)$ such that

$$L(\delta) = K = (U+1)(V+1) - 1 \tag{2.4}$$

and (1.8) holds. (2.4) can be rewritten as

$$(U+1)(V+1) = K+1. \tag{2.5}$$

It follows that $U+1 \mid K+1$, thus U can be chosen in at most $\tau(K+1)$ ways, and by (2.5), U and K determine V uniquely.

Now fix U and V. The number of the coefficients

$$c_{i,j} \text{ with } 0 \leq i \leq U,\ 0 \leq j \leq V,\ (i,j) \neq (U,V) \tag{2.6}$$

in (1.8) is $(U+1)(V+1) - 1 = K$ (by (2.5)) so that these coefficients can be chosen in at most 2^K ways, and the number of initial values

$$s_{i,j} \text{ with } 0 \leq i \leq U,\ 0 \leq j \leq V,\ (i,j) \neq (U,V) \tag{2.7}$$

in (1.8) is also K, so they can be also chosen in at most 2^K ways. Thus the coefficients in (2.6) and the initial values in (2.7) can be chosen in at most $2^K \cdot 2^K = 2^{2K}$ ways independently of U and V. Since U, V, the coefficients $c_{i,j}$ and the initial values $s_{i,j}$ determine the lattice δ uniquely, thus δ can be chosen in at most $\tau(K+1)2^{2K}$ ways which proves (2.2), and this completes the proof of Lemma 1.

Now we return to the proof of Theorem 1. Write

$$H = \left[\frac{1}{2}MN - \left(\frac{1}{2} + \varepsilon_1\right)\frac{\log MN}{\log\log MN}\right].$$

If the event considered in (2.1) does not hold for some $\delta:\ I_{M,N} \to \{1,0\}$, then there is a $K \le H$ such that $L(\delta) = K$. Thus by Lemma 1 we have

$$\begin{aligned}
P(L(\delta) \le H) &= \sum_{K=0}^{H} |\{\delta:\ I_{M,N} \to \{1,0\}, L(\delta) = K\}| \frac{1}{2^{MN}} \\
&\le \left(|\{\delta:\ I_{M,N} \to \{1,0\}, L(\delta) = K\}| + \sum_{K=0}^{H} \tau(K+1)2^{2K} \right) \frac{1}{2^{MN}} \\
&\le \frac{1}{2^{MN}} + \frac{1}{2^{MN}} \left(\max_{n \le 2H} \tau(n) \right) \sum_{K=0}^{H} 2^{2K} \\
&\le \frac{1}{2^{MN}} + \left(\max_{n \le MN} \tau(n) \right) 2^{2H+1-MN}. \qquad (2.8)
\end{aligned}$$

By Wigert's theorem [11] (see also [7]) we have

$$\tau(n) \le 2^{(1+o(1))\frac{\log n}{\log\log n}}. \qquad (2.9)$$

It follows from (2.8) and (2.9) for MN large enough that

$$P(L(\delta) \le H) \le \frac{1}{2^{MN}} + 2^{(o(1)-2\varepsilon_1)(\log MN)/(\log\log MN)} < \varepsilon_2$$

which proves (2.1).

3 Upper bounds for the linear complexity of a random bit (M,N)-lattice.

We will prove

Theorem 2 *Let* $0 < \varepsilon \leq 1$ *and* $M, N \in \mathbb{N}$ *with*

$$\max\{M, N\} \geq \frac{15}{\varepsilon}. \tag{3.1}$$

Then choosing each bit (M, N)*-lattice* $\delta : I_{M,N} \to \{1, 0\}$ *with equal probability* $\frac{1}{2^{MN}}$*, we have*

$$P\left(L(\delta) < \frac{3}{4}MN + \frac{1}{\sqrt{\varepsilon}}(MN)^{3/4}\right) \geq 1 - \varepsilon. \tag{3.2}$$

Proof of Theorem 2 We will derive the theorem from the following

Lemma 2 *Let* $0 < \varepsilon \leq 1$ *and* $M, N \in \mathbb{N}$ *with*

$$M \geq \frac{15}{\varepsilon} \text{ and } N \leq M. \tag{3.3}$$

Define $\tilde{L}$ *and* U *by*

$$\tilde{L} = \frac{M}{2} + \frac{5}{18} + \sqrt{\frac{86}{81\varepsilon}}N^{1/2}, \ U = \left\lceil \frac{\tilde{L} + M - 1}{2} \right\rceil.$$

Then there are at least $(1-\varepsilon)2^{MN}$ *different bit* (M, N)*-lattices such that there exist coefficients* $c_{i,j} \in \{0, 1\}$ $(0 \leq i \leq U, \ 0 \leq j \leq N - 1)$ *depending only on* δ *for which for*

$$m \in \{U, U + 1, \ldots, M - 1\}, \ n \in \{0, 1, \ldots, N - 1\}$$

we have

$$\delta(m, n) = \sum_{i=1}^{U} \sum_{j=0}^{n} c_{i,j}\delta(m - i, n - j)$$

over $\mathbb{F}_2$*.*

Indeed, it follows from Lemma 2 that if (3.3) holds then

$$P\left(L(\delta) \leq (U + 1)N - 1\right) \geq 1 - \varepsilon. \tag{3.4}$$

Here by (3.3) and $0 < \varepsilon \leq 1$ we have

$$
\begin{aligned}
(U+1)N - 1 &< (U+1)N \\
&\leq \frac{\tilde{L}+M+2}{2}N \\
&= \frac{3}{4}MN + \frac{41}{36}N + \sqrt{\frac{43}{162\varepsilon}}N^{3/2} \\
&< \frac{3}{4}MN + \frac{1}{3\sqrt{\varepsilon}}(MN)^{3/4} + \frac{2}{3\sqrt{\varepsilon}}(MN)^{3/4} \\
&= \frac{3}{4}MN + \frac{1}{\sqrt{\varepsilon}}(MN)^{3/4}. \qquad (3.5)
\end{aligned}
$$

By symmetry reasons we may suppose that $N \leq M$ holds in Theorem 2. Thus by (3.5) we get from (3.4) that

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

In order to complete the proof of Theorem 2, we need to prove Lemma 2.

Proof of Lemma 2 First we prove that

$$\tilde{L} \leq U. \qquad (3.6)$$

Indeed, by (3.3) we get

$$M^{1/2} > \sqrt{\frac{86}{81\varepsilon}} + \sqrt{\frac{86}{81\varepsilon} + \frac{23}{9\varepsilon}} \geq \sqrt{\frac{86}{81\varepsilon}} + \sqrt{\frac{86}{81\varepsilon} + \frac{23}{9}}$$

By (3.3) and (3.6) we get

$$
\begin{aligned}
0 &\leq \frac{M}{2} - \sqrt{\frac{86}{81\varepsilon}}M^{1/2} - \frac{23}{18} \leq \frac{M}{2} - \sqrt{\frac{86}{81\varepsilon}}N^{1/2} - \frac{23}{18} \\
&= M - \tilde{L} - 1,
\end{aligned}
$$

from which (3.6) follows.

Definition 5 *Let $\mathcal{P}(-1)$ denote the set of all different bit (M,N)-lattices. Moreover for $0 \leq k \leq N-1$ let $\mathcal{P}(k)$ denote the set of all different bit*

(M,N)-lattices δ for which there exist coefficients $c_{i,j} \in \{0,1\}$ $(U-\tilde{L}+1 \leq i \leq U,\ 0 \leq j \leq k)$, depending only on the following elements of δ:

$$\delta(i,j):\ 0 \leq i \leq M-1,\ 0 \leq j \leq k$$

such that for

$$U \leq m \leq M-1,\ 0 \leq n \leq k$$

we have

$$\delta(m,n) = \sum_{i=U-\tilde{L}+1}^{U} \sum_{j=0}^{n} c_{i,j}\delta(m-i,n-j). \tag{3.7}$$

First we note that

$$|\mathcal{P}(-1)| = 2^{MN}. \tag{3.8}$$

Clearly, for $\delta \in \mathcal{P}(N-1)$ we have

$$L(\delta) \leq (U+1)N-1.$$

Thus it is sufficient to prove

$$|\mathcal{P}(N-1)| \geq (1-\varepsilon)2^{MN}, \tag{3.9}$$

since then (3.4) holds, which completes the proof of Lemma 2. We will prove by induction the following

Lemma 3

$$|\mathcal{P}(r)| \geq \left(1-\frac{\varepsilon(r+1)}{N}\right)2^{MN} \tag{3.10}$$

for $-1 \leq r \leq N-1$.

Indeed, using (3.10) with $r = N-1$ we get (3.9). Thus in order to prove Theorem 2 we have to prove Lemma 3.

For every $-1 \leq k \leq N-2$ and $\delta \in \mathcal{P}(k)$ we define a sequence $s(\delta,k) \in \{0,1\}^M$.

Definition 6 *For $k = -1$ and $\delta \in \mathcal{P}(-1)$ we define the sequence $s(\delta, k) = s(\delta, -1) = (s_0, s_1, \dots, s_{M-1}) \in \{0,1\}^M$ by*

$$s_m = \delta(m, 0). \tag{3.11}$$

For $0 \le k \le N-2$ and $\delta \in \mathcal{P}(k)$ we define the sequence $s(\delta, k) = (s_0, s_1, \dots, s_{M-1}) \in \{0,1\}^M$ by

$$s_m = \begin{cases} \delta(m,0) & \text{for } m \le U-1, \\ \delta(m, k+1) + \sum_{i=U-\tilde{L}+1}^{U} \sum_{j=0}^{k} c_{i,j}\delta(m-i, k+1-j) & \text{for } m \ge U \end{cases} \tag{3.12}$$

over $\mathbb{F}_2$, where the coefficients $c_{i,j}$ ($U-\tilde{L}+1 \le i \le U,\ 0 \le j \le k$) are chosen so that (3.7) *holds for the coefficients $c_{i,j}$ ($U-\tilde{L}+1 \le i \le U,\ 0 \le j \le k$) for $U \le m \le M-1$, $0 \le n \le k$ (if there are more possibilities for choosing the coefficients $c_{i,j}$ in such a way, then we pick one of these possibilities and fix it).*

The proof of Lemma 3 is based on the following two lemmas.

Lemma 4 *Let $0 \le r \le N-1$. If $\delta \in \mathcal{P}(r-1)$ and $L(s(\delta, r-1)) \le \tilde{L}$, then $\delta \in \mathcal{P}(r)$.*

Lemma 5 *Let $-1 \le r \le N-2$ and let $A(r)$ denote the number of bit (M,N)-lattices δ for which $\delta \in \mathcal{P}(r)$ and $L(s(\delta, r)) > \tilde{L}$. Then*

$$A(r) \le \frac{\varepsilon}{N} 2^{MN}.$$

We will prove these two lemmas later, now we will deduce Lemma 3 from the two lemmas above.

Indeed, by (3.8) for $r = -1$ we have

$$|\mathcal{P}(r)| = |\mathcal{P}(-1)| = 2^{MN} = \left(1 - \frac{\varepsilon(r+1)}{N}\right) 2^{MN}.$$

By Lemma 4 and Lemma 5 for $0 \le r \le N-1$ we have

$$\begin{aligned}|\mathcal{P}(r)| &\ge |\mathcal{P}(r-1)| - A(r-1)\\ &\ge |\mathcal{P}(r-1)| - \frac{\varepsilon}{N}2^{MN}.\end{aligned}$$

By iterating this argument we get

$$\begin{aligned}|\mathcal{P}(r)| &\ge |\mathcal{P}(-1)| - \frac{\varepsilon(r+1)}{N}2^{MN}\\ &= \left(1 - \frac{\varepsilon(r+1)}{N}\right)2^{MN}\end{aligned}$$

which was to be proved.

Thus in order to prove Theorem 2 we need to prove Lemma 4 and Lemma 5.

Proof of Lemma 4 We will use the following lemma:

Lemma 6 *Let $s = (s_0, s_1, \dots, s_{M-1}) \in \{0,1\}^{M-1}$ be a sequence for which $L(s) \le \tilde{L}$. Then for every $\tilde{L} \le U \le M-1$ there exist constants $c_i^{(U)}$ (where $U - \tilde{L} + 1 \le i \le U$) such that for $m \ge U$ we have*

$$s_m = \sum_{i=U-\tilde{L}+1}^{U} c_i^{(U)} s_{m-i}.$$

Proof of Lemma 6 We will prove the lemma by induction on U. Indeed, for $U = \tilde{L}$, Lemma 6 follows from the definition of linear complexity. Thus there exist coefficients $c_i^{(\tilde{L})}$ $(1 \le i \le \tilde{L})$ such that for $m \ge \tilde{L}$ we have

$$s_m = \sum_{i=1}^{\tilde{L}} c_i^{(\tilde{L})} s_{m-i} \tag{3.13}$$

Now suppose that Lemma 6 is true for $U = \tilde{L}, \tilde{L}+1, \dots, k-1$ (where $k \ge \tilde{L}+1$), and now we will prove it for $U = k$.

By the induction hypothesis there exist coefficients $c_i^{(k-1)}$ $(k-1-\tilde{L}+1 \le i \le k-1)$ such that for $m \ge k-1$ we have

$$s_m = \sum_{i=k-\tilde{L}}^{k-1} c_i^{(k-1)} s_{m-i}. \tag{3.14}$$

Let now $m \geq k$. Then $m-(k-\tilde{L}) \geq \tilde{L}$, thus by (3.13)

$$s_{m-(k-\tilde{L})} = \sum_{i=1}^{\tilde{L}} c_i^{(\tilde{L})} s_{m-(k-\tilde{L})-i}.$$

Replacing $k+i-\tilde{L}$ by i we get

$$s_{m-(k-\tilde{L})} = \sum_{i=k-\tilde{L}+1}^{k} c_{i+\tilde{L}-k}^{(\tilde{L})} s_{m-i}.$$

Replacing $s_{m-(k-\tilde{L})}$ on the right hand side of (3.14) by the sum above we get from $m \geq k$ that

$$\begin{aligned} s_m &= \sum_{i=k-\tilde{L}}^{k-1} c_i^{(k-1)} s_{m-i} \\ &= c_{k-\tilde{L}}^{(k-1)} s_{m-(k-\tilde{L})} + \sum_{i=k-\tilde{L}+1}^{k-1} c_i^{(k-1)} s_{m-i} \\ &= c_{k-\tilde{L}}^{(k-1)} \sum_{i=k-\tilde{L}+1}^{k} c_{i+\tilde{L}-k}^{(\tilde{L})} s_{m-i} + \sum_{i=k-\tilde{L}+1}^{k-1} c_i^{(k-1)} s_{m-i}. \end{aligned}$$

Thus writing

$$c_i^{(k)} = \begin{cases} c_{k-\tilde{L}}^{(k-1)} c_{i+\tilde{L}-k}^{(\tilde{L})} + c_i^{(k-1)} & \text{for } k-\tilde{L}+1 \leq i \leq k-1, \\ c_{k-\tilde{L}}^{(k-1)} c_{\tilde{L}}^{(\tilde{L})} & \text{for } i = k \end{cases}$$

we get

$$s_m = \sum_{i=k-\tilde{L}+1}^{k} c_i^{(k)} s_{m-i}$$

which proves Lemma 6 for $U = k$. This completes the proof of Lemma 6.

Now we continue the proof of Lemma 4. First consider the case $r = 0$. Let $\delta \in \mathcal{P}(-1)$ and $L(s(\delta,-1)) \leq \tilde{L}$. Then by (3.11)

$$s(\delta,-1) = (\delta(0,0), \delta(1,0), \ldots, \delta(M-1,0)).$$

By (3.6) we have $\tilde{L} \leq U$, thus we may use Lemma 6 which says that there exist coefficients c_i $(U-\tilde{L}+1 \leq i \leq U)$ such that for $m \geq U$ we have

$$\delta(m,0) = \sum_{i=U-\tilde{L}+1}^{U} c_i \delta(m-i,0).$$

Thus it follows from the definition of $\mathcal{P}(0)$ that we have $\delta \in \mathcal{P}(0)$.

Next consider the case $1 \le r \le N-2$. Let $\delta \in \mathcal{P}(r-1)$ with $L(s(\delta, r-1)) \le \tilde{L}$. We will determine coefficients $c_{i,j}$ $(U-\tilde{L}+1 \le i \le U,\ 0 \le j \le r)$ such that for

$$U \le m \le M-1,\ 0 \le n \le r$$

we have

$$\delta(m,n) = \sum_{i=U-\tilde{L}+1}^{U} \sum_{j=0}^{n} c_{i,j}\delta(m-i, n-j). \tag{3.15}$$

First we will fix the coefficients $c_{i,j}$ for $U-\tilde{L}+1 \le i \le U$, $1 \le j \le r-1$.

Since $\delta \in \mathcal{P}(r-1)$ by Definition 6 we can fix the constant $c_{i,j}$ $(U-\tilde{L}+1 \le i \le U,\ 1 \le j \le r-1)$ so that for

$$U \le m \le M-1,\ 0 \le n \le r-1$$

we have (3.15) and the sequence $s(\delta, r-1) = (s_0, s_1, \ldots, s_{M-1})$ is defined by

$$s_m = \begin{cases} \delta(m,0) & \text{for } m \le U-1, \\ \delta(m,r) + \sum\limits_{i=U-\tilde{L}+1}^{U} \sum\limits_{j=0}^{r-1} c_{i,j}\delta(m-i, r+1-j) & \text{for } m \ge U \end{cases} \tag{3.16}$$

Next we will determine the remaining coefficients $c_{i,r}$ $(U-\tilde{L}+1 \le i \le U)$ so that (3.15) also holds for $U \le m \le M-1,\ n = r$. In other words

$$\delta(m,r) = \sum_{i=U-\tilde{L}+1}^{U} \sum_{j=0}^{r} c_{i,j}\delta(m-i, r-j). \tag{3.17}$$

(3.17) is equivalent with

$$\delta(m,r) + \sum_{i=U-\tilde{L}+1}^{U} \sum_{j=0}^{r-1} c_{i,j}\delta(m-i, r-j) = \sum_{i=U-\tilde{L}+1}^{U} c_{i,r}\delta(m-i, 0). \tag{3.18}$$

For $m \ge U$ the left hand side of (3.18) is s_m, where s_m was defined by (3.16) and $s(\delta, r-1) = (s_0, s_1, \ldots, s_{N-1})$. The right hand side of (3.18) involves

$\delta(m-i,0)$'s with $U-\tilde{L}+1 \leq i \leq U$. Then by the definition of $\tilde{L}$ we have $m-i \leq M-1-i \leq M-1-(U-\tilde{L}+1) \leq U-1$, hence by (3.16) then

$$\delta(m-i,0) = s_{m-i}.$$

Thus we have to prove that there exist coefficients $c_{i,r} = c_i$ $(U-\tilde{L}+1 \leq i \leq U)$ such that for $m \geq U$ we have

$$s_m = \sum_{i=U-\tilde{L}+1}^{U} c_i s_{m-i}. \tag{3.19}$$

The existence of these coefficients follows from Lemma 6 since for $s(\delta, r-1) = (s_0, s_1, \ldots, s_{M-1})$ we have $L(s(\delta, r-1)) \leq \tilde{L}$. This completes the proof of Lemma 4.

Proof of Lemma 5 We will use the following theorem of Rueppel [9, pp. 177-179].

Lemma 7 *Let $s \in \{0,1\}^M$. Then*

$$E(L(s)) = \frac{M}{2} + \frac{4+R_2(M)}{18} - 2^{-M}\left(\frac{M}{3} + \frac{2}{9}\right),$$

where $R_2(M)$ denotes the remainder when M is divided by 2. Moreover, for any $k > 0$, we have

$$P\left(|L(s) - E(L(s))| \geq k\right) \leq \frac{86}{81k^2}.$$

Using Lemma 7 with $k = \sqrt{\frac{86}{81\varepsilon}N}$ we get the following

Lemma 8 *Let H denote the number of sequences $s \in \{0,1\}^M$ for which*

$$L(s) > \frac{M}{2} + \frac{5}{18} + \sqrt{\frac{86}{81\varepsilon}}N^{1/2} = \tilde{L}.$$

Then

$$H \leq \frac{\varepsilon}{N} 2^M.$$

Now we are ready to prove Lemma 5. First we prove the statement for $r = -1$. For $\delta \in \mathcal{P}(-1)$ we have

$$s(\delta, -1) = (\delta(0,0), \delta(1,0), \dots, \delta(M-1,0)).$$

By Lemma 8 we can choose the elements $\delta(i,0)$ $(0 \le i \le M-1)$ in at most $\frac{\varepsilon}{N} 2^M$ different ways so that

$$L(s(\delta, -1)) > \tilde{L}. \tag{3.20}$$

All the other elements of δ can be chosen arbitrarily, thus the number of δ's for which (3.20) holds is at most $\frac{\varepsilon}{N} 2^M 2^{(N-1)M} = \frac{\varepsilon}{N} 2^{MN}$ which was to be proved.

Next we prove Lemma 5 for $0 \le r \le N-2$. First we define two types of addition of sequences. For $A = (a_0, a_1, \dots, a_n) \in \{0,1\}^n$ and $B = (b_0, b_1, \dots, b_m) \in \{0,1\}^m$ we define $A \oplus B$ by

$$A \oplus B = (a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_m) \in \{0,1\}^{n+m}.$$

If A and B are sequences of the same length so that $A = (a_0, a_1, \dots, a_n) \in \{0,1\}^n$ and $B = (b_0, b_1, \dots, b_n) \in \{0,1\}^n$, then we define $A \boxplus B$ by

$$A \boxplus B = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n) \in \{0,1\}^n,$$

where the elements of the sequences are added by modulo 2.

For $\delta \in \mathcal{P}(r)$ we define the following quantities:

$$
\begin{aligned}
H_1(\delta) &= (\delta(0,0), \delta(1,0), \ldots, \delta(U-1,0)) \\
H_2(\delta) &= (\delta(U,0), \delta(U+1,0), \ldots, \delta(M-1,0)) \\
H_3(\delta) &= (\delta(0,1), \delta(1,1), \ldots, \delta(M-1,1), \\
&\quad\ \delta(0,2), \delta(1,2), \ldots, \delta(M-1,2), \\
&\quad\quad \vdots \\
&\quad\ \delta(0,r), \delta(1,r), \ldots, \delta(M-1,r)) \\
H_4(\delta) &= (\delta(0,r+1), \delta(1,r+1), \ldots, \delta(U-1,r+1)) \\
H_5(\delta) &= (\delta(U,r+1), \delta(U+1,r+1), \ldots, \delta(M-1,r+1)) \\
H_6(\delta) &= (\delta(0,r+2), \delta(1,r+2), \ldots, \delta(M-1,r+2), \\
&\quad\ \delta(0,r+3), \delta(1,r+3), \ldots, \delta(M-1,r+3), \\
&\quad\quad \vdots \\
&\quad\ \delta(0,N-1), \delta(1,N-1), \ldots, \delta(M-1,N-1))
\end{aligned}
$$

(if $r = 0$ then $H_3(\delta)$ is the empty sequence and if $r = N-2$ then $H_6(\delta)$ is the empty sequence.) Define $\mathcal{V} = \{(H_1(\delta), H_2(\delta), H_3(\delta)) :\ \delta \in \mathcal{P}(r)\}$.

Suppose that $\delta \in \mathcal{P}(r)$. Then by Definition 6 there exist coefficients $c_{i,j}$ such that (3.7) holds for $U \leq m \leq M-1$, $n \leq r$ and $s(\delta, r+1) = (s_0, s_1, \ldots, s_{M-1})$ can be defined by

$$
s_m = \begin{cases} \delta(m,0) & \text{for } m \leq U-1, \\ \delta(m,r+1) + \sum\limits_{i=U-\tilde{L}+1}^{U} \sum\limits_{j=0}^{r} c_{i,j}\delta(m-i,k+1-j) & \text{for } m \geq U \end{cases} \tag{3.21}
$$

Here the summation $\sum\limits_{i=U-\tilde{L}+1}^{U} \sum\limits_{j=0}^{r} c_{i,j}\delta(m-i,r+1-j)$ depends on values $\delta(a,b)$'s with $a \leq M-1-(U-\tilde{L}+1) \leq U-1$, $1 \leq b \leq M-1$. Thus the summation $\sum\limits_{i=U-\tilde{L}+1}^{U} \sum\limits_{j=0}^{r} c_{i,j}\delta(m-i,r+1-j)$ depends only on (some elements of) $H_1(\delta), H_2(\delta), H_3(\delta)$, and $H_4(\delta)$. Thus we may define a function $T : \{0,1\}^U \times \{0,1\}^{M-U} \times \{0,1\}^{rM} \times \{0,1\}^U \to \{0,1\}^{M-U}$ for which for every $\delta \in \mathcal{P}(r)$ we have

$$T(H_1(\delta), H_2(\delta), H_3(\delta), H_4(\delta)) = (y_U(\delta), y_{U+1}(\delta), \ldots, y_{M-1}(\delta)),$$

with

$$y_m(\delta) = \sum_{i=U-\tilde{L}+1}^{U} \sum_{j=0}^{r} c_{i,j}\delta(b-i, r+1-j)$$

for $U \le m \le M-1$.

By (3.21) for $\delta \in \mathcal{P}(r)$ we have

$$s(\delta, r) = H_1(\delta) \oplus (H_5(\delta) \boxplus T(H_1(\delta), H_2(\delta), H_3(\delta), H_4(\delta))).$$

Thus $A(r)$ can be estimated as

$$A(r) \le \sum_{V_1 \in \{0,1\}^U} \sum_{V_2 \in \{0,1\}^{M-U}} \sum_{\substack{V_3 \in \{0,1\}^{rU} \\ (V_1,V_2,V_3) \in \mathcal{V}}} \sum_{V_4 \in \{0,1\}^U} \sum_{\substack{V_5 \in \{0,1\}^{M-U} \\ L(V_1 \oplus (V_5 \boxplus T(V_1,V_2,V_3,V_4)) > \tilde{L}}} \sum_{V_6 \in \{0,1\}^{(N-r)M}} 1.$$

For fixed V_1, V_2, V_3, V_4, in the fifth sum we substitute $V_5 \boxplus T(V_1, V_2, V_3, V_4)$ by V_5' (indeed, if $V_5' = V_5 \boxplus T(V_1, V_2, V_3, V_4)$ then $V_5 = V_5' \boxplus T(V_1, V_2, V_3, V_4)$. Thus

$$\begin{aligned}
A(r) &\le \sum_{V_1 \in \{0,1\}^U} \sum_{V_2 \in \{0,1\}^{M-U}} \sum_{\substack{V_3 \in \{0,1\}^{rU} \\ (V_1,V_2,V_3) \in \mathcal{V}}} \sum_{V_4 \in \{0,1\}^U} \sum_{\substack{V_5' \in \{0,1\}^{M-U} \\ L(V_1 \oplus V_5') > \tilde{L}}} \sum_{V_6 \in \{0,1\}^{(N-r)M}} 1 \\
&\le \sum_{V_1 \in \{0,1\}^U} \sum_{V_2 \in \{0,1\}^{M-U}} \sum_{V_3 \in \{0,1\}^{rU}} \sum_{V_4 \in \{0,1\}^U} \sum_{\substack{V_5' \in \{0,1\}^{M-U} \\ L(V_1 \oplus V_5') > \tilde{L}}} \sum_{V_6 \in \{0,1\}^{(N-r)M}} 1 \\
&= \sum_{V_2 \in \{0,1\}^{M-U}} \sum_{V_3 \in \{0,1\}^{rU}} \sum_{V_4 \in \{0,1\}^U} \sum_{V_6 \in \{0,1\}^{(N-r)M}} \sum_{V_1 \in \{0,1\}^U} \sum_{\substack{V_5' \in \{0,1\}^{M-U} \\ L(V_1 \oplus V_5') > \tilde{L}}} 1.
\end{aligned} \tag{3.22}$$

Here by using Lemma 8 we get

$$\sum_{V_1 \in \{0,1\}^U} \sum_{\substack{V_5' \in \{0,1\}^{M-U} \\ L(V_1 \oplus V_5') > \tilde{L}}} 1 = \sum_{\substack{s \in \{0,1\}^M \\ L(s) > \tilde{L}}} 1 = H \leq \frac{\varepsilon}{N} 2^M.$$

Putting this in (3.22) we get

$$A(r) \leq \frac{\varepsilon}{N} 2^{NM}$$

which was to be proved.

4 On the k-error linear complexity

Aly, Meidl and Winterhof write in [1]: "The linear complexity is of fundamental importance as a complexity measure for periodic sequences. Motivated by security issues of stream ciphers, in [10] Stamp and Martin proposed a different measure of the complexity of periodic sequences, the *k-error linear complexity*, which is defined by

$$L_k(S) = \min_T L(T),$$

where the minimum is taken over all N-periodic sequences $T = (\tau_0, \tau_1, \dots)$ over $\mathbb{F}_p$ for which the Hamming distance of the vectors $(\sigma_0, \sigma_1, \dots, \sigma_{N-1})$ and $(\tau_0, \tau_1, \dots, \tau_{N-1})$ is at most k. Evidently we have

$$N \geq L_0(S) = L(S) \geq L_1(S) \geq L_2(S) \geq \cdots \geq L_N(S) = 0.'' \tag{4.1}$$

(See also the survey paper [12].)

Throughout both Parts I and II of this paper we consider finite bit sequences S_N of form (1.1), and we define their linear complexity over $\mathbb{F}_2$. In this situation the definition of the k-error linear complexity can be formulated in the following way:

Definition 7 *The* k-error linear complexity *of the* bit sequence $S_N = (s_0, s_1, \dots, s_{N-1})$ *is defined as*

$$L_k(S_N) = \min_T L(T_N)$$

where the minimum is taken over all bit sequences $T_N = (t_0, t_1, \dots, t_{N-1})$ *such that the Hamming distance of the vectors* $(s_0, s_1, \dots, s_{N-1})$ *and* $(t_0, t_1, \dots, t_{N-1})$ *is at most* k *(while the* k*-error linear complexity of the* binary sequence $E_N = (e_0, e_1, \dots, e_{N-1}) \in \{-1, +1\}^N$ *is defined as* $L_k(E_N) = L_k(\varphi^{-1}(E_N))$ *with the mapping* φ *given in* (1.4)*).*

(Note that (4.1) also holds in this situation.)

This definition can be extended to bit (and binary) lattices easily:

Definition 8 *The* k-error linear complexity of the bit (M, N) lattice $\delta = \delta(i, j)$ $(i \in \{0, 1, \dots, M-1\},\ j \in \{0, 1, \dots, N-1\})$ *is defined as*

$$L_k(\delta) = \min_\rho L(\rho)$$

where the minimum is taken over all bit (M, N)*-lattices* $\rho = \rho(i, j)$ *such that the Hamming distance*

$$d(\delta, \rho) = |\{(i, j):\ 1 \le i \le M,\ 1 \le j \le N,\ \eta(i, j) \ne \rho(i, j)\}| \tag{4.2}$$

of the lattices $\delta = \delta(i, j)$ *and* $\rho = \rho(i, j)$ *is at most* k *(while the* k*-error linear complexity of the* binary (M, N)-lattice $\eta = \eta(i, j)$ *is defined as* $L_k(\eta) = L(\mu^{-1}(\eta))$ *with the mapping* μ *given in* (1.7)*).*

Then clearly the 2 dimensional analogue of (4.1) also holds:

$$MN \ge L_0(\delta) = L(\delta) \ge L_1(\delta) \ge L_2(\delta) \ge \dots \ge L_{MN}(\delta) = 0. \tag{4.3}$$

By (4.3), the k-error linear complexity of a bit lattice is smaller (or at least not greater) than the linear complexity of it. The former can be much smaller than the latter:

Example 3 *Define the bit (M,N)-lattice δ by*

$$\delta(i,j)=\begin{cases}1 & \text{if } i=M-1,\ j=N-1\\ 0 & \text{if } 0\le i\le M-1,\ 0\le j\le N-1 \text{ and}\\ & \qquad\qquad (i,j)\ne(M-1,N-1).\end{cases}$$

Then $L(\delta)=MN$ by Definition 4. On the other hand, define the bit (M,N)-lattice ρ by

$$\rho(i,j)=0 \text{ for all } 0\le i\le M-1,\ 0\le j\le N-1.$$

Then by Definition 4 we have $L(\rho)=0$, and clearly the Hamming distance of δ and ρ is

$$d(\delta,\rho)=1.$$

It follows that

$$L_1(\delta)\le L(\rho)=0$$

whence $L_1(\delta)=0$.

It is a question of basic importance: for fixed k, M and N, and for a (truly) random bit (M,N)-lattice, how much smaller is the k-error linear complexity than the linear complexity? Namely, if in the random case the k-error linear complexity is also large as (by Theorem 1) the linear complexity is, than in the cryptographic applications we may use only bit lattices of large k-error linear complexity, while the lattices of small k-error linear complexity must be discarded. Indeed, it can be shown easily by using Lemma 1 that this is the case for small k (for $k<\varepsilon MN$):

Theorem 3 *For every $\varepsilon_1>0$ and $\varepsilon_2>0$ there are numbers $\varepsilon_3=\varepsilon_3(\varepsilon_1)$ (independent of ε_2) and $C'=C'(\varepsilon_1,\varepsilon_2,\varepsilon_3)$ such that if $M,N,k\in\mathbb{N}$, $MN>C'$, $k<\varepsilon_3 MN$, then choosing each bit (M,N)-lattice $\delta:\ I_{M,N}\to\{1,0\}$ with equal probability $\frac{1}{2^{MN}}$, we have*

$$P\left(L_k(\delta)>\left(\frac{1}{2}-\varepsilon_1\right)MN\right)>1-\varepsilon_2. \tag{4.4}$$

Proof of Theorem 3. Write $U = \left[\left(\frac{1}{2} - \varepsilon_1\right) MN\right]$. If $L_k(\delta) \leq U$, then by the definition of the k-error linear complexity there is a $\rho: \ I_{M,N} \to \{1,0\}$ with

$$L(\rho) = L_k(\delta) \leq U$$

and

$$d(\delta, \rho) \leq k. \tag{4.5}$$

If ρ with $L(\rho) \leq U$ is fixed, then a $\delta: \ I_{M,N} \to \{1,0\}$ satisfying (4.5) can be obtained from ρ by changing $\rho(i,j)$ for at most k of the MN pairs (i,j), and this can be done in $\sum_{\ell=0}^{k} \binom{MN}{\ell}$ ways for every ρ. Thus the number of the bit (M,N)-lattices δ satisfying $L_k(\delta) \leq U$ is

$$\begin{aligned} &|\{\delta: \ I_{M,N} \to \{1,0\}, \ L_k(\delta) \leq U\}| \\ &\leq |\{\rho: \ I_{M,N} \to \{1,0\}, \ L(\rho) \leq U\}| \sum_{\ell=0}^{k} \binom{MN}{\ell}. \end{aligned} \tag{4.6}$$

It follows from $k < \varepsilon_3 MN$ with a little computation that if ε_3 is small enough in terms of ε_1 and MN is large enough in terms of ε_1 and ε_3, then the last sum is

$$\sum_{\ell=0}^{k} \binom{MN}{\ell} < 2^{(\varepsilon_1/2)MN}.$$

Then using also Lemma 1, Wigert's theorem [11] and the definition of U, we obtain from (4.6) for MN large enough that

$$\begin{aligned}
&|\{\delta:\ I_{M,N}\to\{1,0\},\ L_k(\delta)\le U\}| \\
&\le \sum_{h=0}^{U}|\{\rho:\ I_{M,N}\to\{1,0\},\ L(\rho)=h\}|\cdot 2^{(\varepsilon_1/2)MN} \\
&= \Bigg(|\{\rho:\ I_{M,N}\to\{1,0\},\ L(\rho)=0\}| \\
&+\sum_{h=1}^{U}|\{\rho:\ I_{M,N}\to\{1,0\},\ L(\rho)=h\}|\Bigg)2^{(\varepsilon_1/2)MN} \\
&< 2^{(1+o(1))\frac{\log MN}{\log\log MN}+(1-2\varepsilon_1)MN+O(1)+(\varepsilon_1/2)MN} \\
&\le \left(1+\sum_{h=1}^{U}\tau(h+1)2^{2h}\right)2^{(\varepsilon_1/2)MN} \\
&< 2^{(1-\varepsilon_1)MN}
\end{aligned}$$

whence

$$\begin{aligned}
&P\left(L_k(\delta)>\left(\frac{1}{2}-\varepsilon_1\right)MN\right)=1-P(L_k(\delta)\le U) \\
&=1-\frac{1}{2^{MN}}|\{\delta:\ I_{M,N}\to\{1,0\},\ L_k(\delta)\le U\}|>1-\frac{1}{2^{\varepsilon_1 MN}}>1-\varepsilon_2
\end{aligned}$$

if MN is large enough in terms of ε_1 and ε_2 which completes the proof of Theorem 3.

Note that by (4.3), Theorem 2 also gives an upper bound of $L_k(\delta)$ for a truly random lattice δ.

Example 4 *By Dirichlet's approximation theorem there are infinitely many positive integers q such that there is also a positive integer p with*

$$\left|\frac{1}{\sqrt{2}}-\frac{p}{q}\right|<\frac{1}{q^2}. \tag{4.7}$$

Consider a q large enough with this property, and define the $q\times q$ bit lattice δ by

$$\delta(i,j)=s_{i,j}=\begin{cases}1 & \textit{if } i=j\ne p-2\\ 0 & \textit{if } i\ne j \textit{ or } i=j=p-2\end{cases}$$

for $i, j \in \{0, 1, \dots, q-1\}$. *Then* (1.8) *becomes*

$$s_{m+p-1,n+p-1} = s_{m,n}$$

for the pairs (m, n) *defined in* (1.9) *with*

$$U = V = p - 1$$

and we have

$$f(x, y) = \sum_{\substack{0 \le n < N \\ n \ne p-2}} (xy)^n$$

and

$$g(x, y) = (xy)^{p-1}.$$

Thus it follows from (4.7) that

$$L(\delta) = (U+1)(V+1) - 1 = p^2 - 1 = \left(\frac{q}{\sqrt{2}} + O\left(\frac{1}{q}\right)\right)^2 = \frac{q^2}{2} + O(1). \tag{4.8}$$

If our Conjecture 1 is true (and Theorems 1 and 2 point in this direction), then the linear complexity of a random $q \times q$ bit lattice is also $\left(\frac{1}{2} + o(1)\right) q^2$. Thus by (4.8) our bit lattice δ mimics the behaviour of a (truly) random $q \times q$ bit lattice ideally as far as the linear complexity is concerned so that if we test its applicability in cryptography by computing its linear complexity, then we may conclude that our lattice is just ideal for this purpose. However, taking a look at this lattice we can feel immediately that it is of too special structure for using it in cryptography and, indeed, we can show that this is the case if we go just one step beyond linear complexity by studying the 1-error linear complexity of the lattice. Let ρ denote the lattice defined in Example 2 with q and 1 in place of N and d, respectively:

$$\rho(i, j) = \begin{cases} 0 & \text{if } i \ne j \\ 1 & \text{if } i = j \end{cases}$$

(for $i, j \in \{0, 1, \dots, q-1\}$). Then the Hamming distance of δ and ρ is

$$d(\delta, \rho) = 1$$

since $\delta(i, j) \neq \rho(i, j)$ holds only if $i = j = p-2$. Moreover, by (1.11) we have

$$L(\rho) = 1^2 + 2 \cdot 1 = 3.$$

Thus by Definition 8 we have

$$L_1(\delta) \leq L(\rho) = 3$$

so that, indeed, $L_1(\delta)$ is very small thus the bit lattice δ is useless in the applications.

5 Alternative extensions of the notion of linear complexity

First we write the definition of the one dimensional linear complexity in Definition 1. Consider again the bit sequence S_N in (1.1), and let $(0 \leq) k_1 < k_2 < \cdots < k_t \; (\leq L-1)$ denote the subscripts of the coefficients c with $c = 1$ in (1.2). Then writing also $k_{t+1} = L$, (1.2) can be rewritten in the following form over $\mathbb{F}_2$:

$$s_{n+k_1} + s_{n+k_2} + \cdots + s_{n+k_t} + s_{n+k_{t+1}} = 0 \text{ for } n = 0, 1, \dots, N-L-1. \quad (5.1)$$

Thus Definition 1 is equivalent with the following one:

Definition 1' *The linear complexity $L(S_N)$ (over the field $\mathbb{F}_2$) of the finite bit sequence* (1.1) *is defined as the smallest positive integer L such that there are pairwise distinct non-negative integers $k_1, k_2, \dots, k_t, k_{t+1} = L$:*

$$k_i \neq k_j \text{ for } 1 \leq i, j, \leq t+1,\ i \neq j \quad (5.2)$$

such that

$$k_i < k_{t+1} = L \text{ for } i = 1, 2, \dots, t \quad (5.3)$$

and

$$s_{n+k_1} + s_{n+k_2} + \cdots + s_{n+k_t} + s_{n+L} = 0 \text{ for } n = 0, 1, \ldots, N-L-1.$$

(with the conventions at the end of Definition 1).

If one tries to extend this definition to 2 dimensions (to bit lattices), then the difficulty is that the plane vectors are not ordered, thus we cannot speak on the smallest of certain vectors, and it is not clear how to extend inequality (5.3) to vectors. The situation can be saved in the first case by comparing the *length* of the vectors not the vectors themselves, and in the second case by using the partial ordering.

$$\mathbf{u} = (u_1, u_2) < \mathbf{v} = (v_1, v_2) \text{ if and only if } u_1 \leq v_1,\ u_2 \leq v_2 \text{ and } \mathbf{u} \neq \mathbf{v}. \quad (5.4)$$

Definition 9 The linear complexity $L^{(1)}(\delta)$ *(over the field* $\mathbb{F}_2$*) of the bit* (M, N)*-lattice* δ *is defined as the* length *of the shortest vector* $\mathbf{L} = (\ell_1, \ell_2) \neq (0, 0)$ *with* $(\ell_1, \ell_2) \in I_{M,N}$ *such that there are pairwise distinct vectors* $\mathbf{k_1}, \mathbf{k_2}, \ldots, \mathbf{k_t}, \mathbf{k_{t+1}} = \mathbf{L}$*:*

$$\mathbf{k_i} \neq \mathbf{k_j} \textit{ for } 1 \leq i, j, \leq t+1,\ i \neq j$$

such that

$$\mathbf{k_i} < \mathbf{k_{t+1}} = \mathbf{L} \textit{ for } i = 1, 2, \ldots, t \quad (5.5)$$

in terms of partial ordering (5.4)*, and*

$$\delta(\mathbf{h} + \mathbf{k_1}) + \delta(\mathbf{h} + \mathbf{k_2}) + \cdots + \delta(\mathbf{h} + \mathbf{k_t}) + \delta(\mathbf{h} + \mathbf{k_{t+1}}) = 0 \quad (5.6)$$

(over $\mathbb{F}_2$*) for every* $\mathbf{h} = (m, n)$ *such that*

$$0 \leq m,\ 0 \leq n \quad (5.7)$$

and

$$\mathbf{h} + \mathbf{k_i} \in I_{M,N} \textit{ for } i = 1, 2, \ldots, t+1 \quad (5.8)$$

(with the conventions at the end of Definition 4).

Note that it is easy to see that this definition of 2 dimensional linear complexity (in the same way as Definition 4 does) includes the one dimensional definition (Definition 1) as a special case so that, indeed, the former is an extension of the latter.

While in the other definitions the linear complexity is always an integer, here (by using the above notation) the linear complexity is

$$L^{(1)}(\delta) = |\mathbf{L}| = |(\ell_1, \ell_2)| = \left(\ell_1^2 + \ell_2^2\right)^{1/2}$$

which is not necessarily an integer. If we want to use an integral valued linear complexity, then we may replace quantity $|\mathbf{L}|$ by its square, and we get another definition of linear complexity:

$$L^{(2)}(\delta) = |\mathbf{L}|^2 = |(\ell_1, \ell_2)|^2 = \ell_1^2 + \ell_2^2.$$

This definition also has the advantage that if the order of magnitude of M and N is the same then it makes the order of magnitude of the linear complexity MN which is the same as in case of Definitions 4 and 4' (on the other hand, it has disadvantage that in the special case of $M \times 1$ lattices it makes the order of magnitude of the linear complexity very much different from the one dimensional linear complexity).

There is a third option to define the linear complexity of the lattice δ studied in Definition 9: instead of defining $L(\delta)$ as the *length* of the vector $\mathbf{L} = (\ell_1, \ell_2)$, we may take the *area* $\ell_1\ell_2$ of the rectangle R_1 of vertices $(0,0),\ (0,\ell_1),\ (\ell_1,\ell_2),\ (\ell_2,0)$:

$$L^{(3)}(\delta) = \ell_1\ell_2.$$

(Moreover we may modify Definition 9 further by replacing the *shortest* vector $\mathbf{L}$ by the vector $\mathbf{L} = (\ell_1, \ell_2)$ for which the area $\ell_1\ell_2$ of the rectangle R_1 is minimal.) It is easy to see that all the linear complexity notions $L^{(1)}(\delta), L^{(2)}(\delta), L^{(3)}(\delta)$ introduced in this section plus the one $L(\delta)$ introduced in Definitions 4 and 4' are pairwise *distinct.*

Note that (5.6) can be rewritten in an algebraic form similar to (1.8). Indeed, again we write $\delta(i,j) = s_{i,j}$ for $i = 0, 1, \ldots, M-1$, $j = 0, 1, \ldots, N-1$, and define the coefficients $c_{i,j}$ by

$$c_{i,j} = \begin{cases} 1 & \text{if } (i,j) \in \{\mathbf{k_1}, \mathbf{k_2}, \ldots, \mathbf{k_t}\} \\ 0 & \text{if } (i,j) \notin \{\mathbf{k_1}, \mathbf{k_2}, \ldots, \mathbf{k_t}\} \end{cases}$$

for

$$i \in \{0, 1, \ldots, \ell_1\},\ j \in \{0, 1, \ldots, \ell_2\}, (i,j) \neq (\ell_1, \ell_2).$$

Then (5.6) can be rewritten as

$$\delta(\mathbf{h} + \mathbf{k_{t+1}}) = \delta(\mathbf{h} + \mathbf{k_1}) + \delta(\mathbf{h} + \mathbf{k_2}) + \cdots + \delta(\mathbf{h} + \mathbf{k_t}),$$

in other words,

$$s_{m+\ell_1, n+\ell_2} = \sum_{\substack{0 \leq i \leq \ell_1 \\ 0, \leq j \leq \ell_2 \\ (i,j) \neq (\ell_1, \ell_2)}} c_{i,j} s_{m+i, n+j}. \tag{5.9}$$

for all integers (m, n) with

$$(m,n) \in \{(m,n) :\ 0 \leq m < M - \ell_1,\ 0 \leq n < N - \ell_2\}. \tag{5.10}$$

Observe that the recursive formula in (5.9) is much simpler than the recursion (1.8) in Definition 4 (since here the conditions on i and j are simpler), and the condition on m and n in (5.10) is much simpler than condition (1.9) in Definition 4 (this is due to assumption (5.5)); namely, by this assumption it suffices to ensure that (5.8) holds for $i = t+1$, from this it also follows from $i = 1, 2, \ldots, t$). This simplicity and transparency of (5.9) and (5.10) is the greatest advantage of the approach used in this section. However, there is a price paid for this. Namely, observe that (5.9) and (5.10) say that the δ values assumed at the points (i,j) belonging to the rectangle $R_1 = R_1(\delta) = \{(i,j) : 0 \leq i \leq \ell_1,\ 0 \leq j \leq \ell_2\}$ determine the values of δ assumed at the points (i,j)

belonging to the rectangle $R_2 = R_2(\delta) = \{(i,j) : \ \ell_1 \le i < M, \ \ell_2 \le j < N\}$ uniquely but nothing is said on the values of δ assumed at the points with

$$(i,j) \in I_{M.N} \setminus (R_1 \cup R_2). \tag{5.11}$$

Thus the values of the linear complexities $L^{(1)}(\delta)$, $L^{(2)}(\delta)$, $L^{(3)}(\delta)$ are independent of the $\delta(i,j)$ values assumed at the points (i,j) satisfying (5.11). On the other hand, the recursion described by (1.8) and (1.9) in Definition 4 determines $\delta(i,j)$ uniquely for every $(i,j) \in I_{M,N}$ so that the linear complexity $L(\delta)$ introduced in Section 1 gives a more complete information on the bit lattice δ than the ones introduced in this section. Thus in general we propose to use the linear complexity $L(\delta)$ introduced in Section 1, but in some simple applications the study of $L^{(1)}(\delta)$, $L^{(2)}(\delta)$, $L^{(3)}(\delta)$ can be also useful.

Example 5 *Consider first the $d = 2$ special case of the bit lattice δ studied in Example 2. In other words, let $M \in \mathbb{N}$, $N = 2M$, and define the $N \times N$ bit lattice δ by*

$$\delta(i,j) = s_{i,j} = \begin{cases} 0 & \textit{if } i \neq j \textit{ or } i = j \textit{ and } i,j \textit{ are odd} \\ 1 & \textit{if } i = j \textit{ and } i,j \textit{ are even} \end{cases} \tag{5.12}$$

for $i,j \in \{0,1,\ldots,N-1\}$. Then δ satisfies the recursion (1.10)*:*

$$s_{m+2,n+2} = s_{m,n} \tag{5.13}$$

for all integers m,n with

$$\begin{aligned}(m,n) \in &\{(m,n) : \ 0 < m < N-2, \ -2 \le n < N-2\} \\ &\cup \{(m,n) : 0 < n < N-2, \ -2 \le m < N-2\} \cup \{(0,0)\},\end{aligned} \tag{5.14}$$

and by (1.11) *the linear complexity $L(\delta)$ defined in Section 1 of this lattice is*

$$L(\delta) = 2^2 + 2 \cdot 2 = 8 \tag{5.15}$$

which is very small.

If we specify the recursion (5.9), (5.10) in Section 5 to this bit lattice δ then (5.9) also becomes (5.13), but condition (5.10) becomes

$$(m,n) \in \{(m,n) : \ 0 \le m < N-1, \ 0 \le n < N-1\},$$

and we have $\ell_1 = \ell_2 = 1$, $\mathbf{L} = (\ell_1, \ell_2) = (1,1)$ so that

$$L^{(1)}(\delta) = |\mathbf{L}| = \sqrt{2}, \tag{5.16}$$

$$L^{(2)}(\delta) = |\mathbf{L}|^2 = 2, \tag{5.17}$$

and

$$L^{(3)}(\delta) = \ell_1 \ell_2 = 1, \tag{5.18}$$

so that the linear complexities $L^{(1)}$, $L^{(2)}$, $L^{(3)}$ introduced in Section 5 are also small.

Now we modify this bit lattice δ by changing its values assumed at the points $(0, N-1)$, $(N-1, 0)$ from 0 to 1. Denote the lattice obtained in this way by ρ:

$$\rho(i,j) = \begin{cases} 0 & \text{if either } i \ne j \text{ and } (i,j) \ne (0, N-1),\ (i,j) \ne (N-1, 0) \\ & \text{or } i = j \text{ and } i, j \text{ are odd} \\ 1 & \text{if either } i = j \text{ and } i, j \text{ are even or one of} \\ & (i,j) = (0, N-1) \text{ and } (i,j) = (N-1, 0) \text{ holds} \end{cases}$$

for $i, j \in \{0, 1, \dots, N-1\}$. For the lattice δ defined by (5.12) the rectangles R_1, R_2 defined earlier in this section are

$$R_1 = R_1(\delta) = \{(i,j) : \ 0 \le i \le 1, \ 0 \le j \le 1\}$$

and

$$R_2 = R_2(\delta) = \{(i,j) : \ 1 \le i \le N-1, \ 1 \le j \le N-1\}.$$

Clearly, for $(i,j) \in R_1 \cup R_2$ we have $\delta(i,j) = \rho(i,j)$; the only points (i,j) with $\delta(i,j) \ne \rho(i,j)$ are the points $(0, N-1)$, $(N-1, 0)$ which satisfy (5.11).

Thus by the discussion above the linear complexities $L^{(1)}$, $L^{(2)}$, $L^{(3)}$ of δ and ρ are equal so that by (5.16), (5.17) and (5.18) we have

$$L^{(1)}(\rho) = L^{(1)}(\delta) = \sqrt{2},$$
$$L^{(2)}(\rho) = L^{(2)}(\delta) = 2$$

and

$$L^{(3)}(\rho) = L^{(3)}(\delta) = 1.$$

On the other hand the situation is very much different if we compare $L(\rho)$ and $L(\delta)$ (where $L(\dots)$ is the linear complexity introduced in Section 1). Indeed, in order to determine $L(\rho)$ we start out from formulas (1.8) and (1.9) in Section 1. Substituting $m = -U$ we get from (1.8) that

$$s_{0,n+V} = \sum_{j=0}^{V-1} c_{U,j} s_{0,n+j} \tag{5.19}$$

(note that by the condition $\max(0, -m) = \max(0, U) \leq i \leq U$ we must have $i = U$ in (1.8), and by the condition $(i, j) = (U, j) \neq (U, V)$) here j cannot assume the value V) where by (1.9) the subscript n may assume any integer value with

$$0 < n < N - V. \tag{5.20}$$

If

$$N - V - 1 > 0$$

or, in equivalent form,

$$V < N - 1, \tag{5.21}$$

then the number

$$n = N - V - 1$$

satisfies inequality (5.20), thus we may substitute this n value in (5.19). Then on the left hand side we get

$$s_{0,n+V} = s_{0,N-1} = \rho(0, N-1) = 1. \tag{5.22}$$

On the other hand, the last sum on the right hand side of (5.19) becomes

$$\sum_{0\le j\le V-1} c_{U,j} s_{0,N-V-1+j} = \sum_{0\le j\le V-1} c_{U,j} \rho(0, N-V-1+j). \tag{5.23}$$

By (5.21), for every $0 \le j \le V-1$ we have

$$1 \le N-V-1 \le N-V-1+j \le N-V-1+V-1 = N-2,$$

thus the second factor in each term of the last sum is of the form

$$\rho(0,k) \text{ with } k \in \{1,2,\dots,N-2\}.$$

By the definition of the bit lattice ρ each of these values is 0, thus the sum in (5.23) is 0 which contradicts (5.19) and (5.22). This contradiction shows that (5.21) cannot hold, in other words, we have

$$V \ge N-1.$$

By symmetry reasons it can be proved in the same way

$$U \ge N-1.$$

Thus we may conclude that

$$L(\rho) = (U+1)(V+1) - 1 \ge N^2 - 1$$

so that the linear complexity introduced in Section 1 is very large for the bit lattice ρ; compare this with the small values of $L^{(1)}(\rho)$, $L^{(2)}(\rho)$ and $L^{(3)}(\rho)$ in (5.16), (5.17) and (5.18).

References

[1] H. Aly, W. Meidl and A. Winterhof, *On the k-error linear complexity of cyclomatic sequences*, J. Math. Crypt. 1 (2007), 283-296.

[2] K. Gyarmati, C. Mauduit and A. Sárközy, *On linear complexity of binary lattices*, Ramanujan J., to appear.

[3] 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.

[4] 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.

[5] 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.

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

[7] E. Landau, *Handbuch der Lehre der Verteilung der Primzahlen, I-II*, 2nd ed., Chelsea Publ. Ca, New York 1953.

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

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

[10] M. Stamp and C. F. Martin, *An algorithm for the k-error linear complexity of binary sequences with period 2*, IEEE Transactions on Information Theory 39 (1993).

[11] S. Wigert, Sur l'ordre de grandeur du nombre des diviseurs d'un entier, Arkiv för matematik, astronomi och. fysik, Bd. 3, No 18., 9S; 1906-1907.

[12] A. Winterhof, *Linear complexity and related complexity measures*, in: Woungang, I. (Hrsg.), Selected Topics in Information and Coding Theory 7, Singapore: World Scientific 2010, 3-40.