On the Measures of Pseudorandomness of Binary Lattices

Károly Müllner

ELTE

Central European Conference on Cryptology

Outline

1. Introduction
2. Binary Lattices
3. Conclusion

Motivation

- Pseudorandom binary sequences are essential in cryptography, coding theory, and simulations.
- In 1997, Mauduit and Sárközy introduced measures in order to study the pseudorandom properties of finite binary sequences: well-distribution (W), correlation (C_k), and combined (Q_k).
- This work extends these concepts to multidimensional (2D and 3D) binary lattices.

Pseudorandom measures

Definition (Well-distribution measure)

For a binary sequence $E_N = (e_1, e_2, \ldots, e_N) \in \{-1, 1\}^N$ *of lenght* N*, write*

$$U(E_N, t, a, b) = \sum_{j=0}^{t} e_{a+jb}$$

Then the well-distribution measure of E_N *is defined as*

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

where the maximum is taken over all a, b, t *such that* $a, b, t \in \mathbb{N}$ *and* $1 \leq a \leq a + tb \leq N$.

Pseudorandom measures

The well-distribution measure studies how close are the frequencies of the $+1$'s and -1's in arithmetic progressions (for a binary sequence with strong pseudorandom properties these two quantities are expected to be very close.)

If the subsequence $(+1, +1)$ occurs much more frequently then the subsequence $(-1, -1)$, then it may cause problems in the applications, and we cannot say that our sequence has strong pseudorandom properties.

In order to study connections of this type Mauduit and Sárközy introduced the correlation and normality measures:

Pseudorandom measures

Definition (Correlation measure)

For a binary sequence $E_N = (e_1, e_2, \ldots, e_N) \in \{-1, 1\}^N$ *of lenght* N*, and for* $D = (d_1, \ldots, d_\ell)$ *with non-negative integers* $0 \leq d_1 \leq \cdots \leq d_\ell$*, write*

$$V(E_N, M, D) = \sum_{n=1}^{M} e_{n+d_1} \cdots e_{n+d_\ell}.$$

Then the correlation measure of order to ℓ *of* E_N *is defined as*

$$C_\ell(E_N) = \max_{M,D} |V(E_N, M, D)| = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} \cdots e_{n+d_\ell} \right|,$$

where the maximum is taken over all $D = (d_1, d_2, \ldots, d_\ell)$ *and* M *such that* $0 \leq d_1 < \cdots < d_\ell < M + d_\ell \leq N$.

Pseudorandom measures

Definition (Normality measure)

For a binary sequence $E_N = (e_1, e_2, \ldots, e_N) \in \{-1, 1\}^N$ *of lenght* N*, and for* $X = (x_1, \ldots, x_\ell) \in \{-1, +1\}^\ell$ *write*

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

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

$$N_\ell(E_N) = \max_{M,X} \left| T(E_N, M, X) - M/2^\ell \right|,$$

where the maximum is taken over all $X = (x_1, \ldots, x_\ell) \in \{-1, +1\}^\ell$ *and* M *such that* $0 < M \neq N - \ell + 1$.

Pseudorandom measures

- The combined (well-distribution-correlation) pseudorandom measure is a common generalization of the well-distribution and the correlation measures.
- This measure has an important role in the multidimensional extension of the theory of pseudorandomness.

Definition (Combined measure)

For a binary sequence $E_N = (e_1, e_2, \dots, e_N) \in \{-1, 1\}^N$ *of length* N, *and for* $D = (d_1, \dots, d_\ell)$ *with non-negative integers* $0 \le d_1 < \cdots < d_\ell$

$$Z(E_N, a, b, t, D) = \sum_{j=0}^{t} e_{a+jb+d_1} \cdots e_{a+jb+d_\ell}.$$

Definition (Cont.)

Then the combined (well-distribution-correlation) measure of order ℓ of E_N is defined as

$$Q_\ell(E_N) = \max_{a,b,t,D} |Z(E_N, a, b, t, D)| = \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} \cdots e_{a+jb+d_\ell} \right|,$$

where the maximum is taken over all a, b, t and $D = (d_1, ..., d_\ell)$ such that all the subscripts $a + jb + d_i$ belong to $\{1, 2, ..., N\}$.

Pseudorandom measures in 1-dimension

- Sequences $E_N = \{e_1, \ldots, e_N\} \in \{-1, 1\}^N$
- **Well-distribution measure:**

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

- **Correlation measure of order k:**

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

- **Combined measure:**

$$Q_k(E_N) = \max_{a,b,t,D} \left| \sum_{j=0}^{t-1} e_{a+jb+d_1} \cdots e_{a+jb+d_k} \right|$$

Binary Lattices

In order to study the multidimensional analog of pseudorandomness, Hubert, Mauduit, and Sárközy [3] introduced the following definitions and notations:

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

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

This set is called an n-dimensional N-lattice or, briefly, an N-lattice.

Binary Lattices

In [3], the definition of binary sequences is extended to more dimensions by considering functions of type

$$\eta(\mathbf{x}) : I_N^n \to \{-1, +1\}.$$

If $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ so that $\eta(\mathbf{x}) = \eta((x_1, x_2, \ldots, x_n))$ then we will slightly simplify the notation by writing $\eta(\mathbf{x}) = \eta(x_1, x_2, \ldots, x_n)$.

Such a function can be visualized as the lattice points of the N-lattice replaced by the two symbols $+$ and $-$; thus, they are called binary N-lattices. Binary 2- or 3 dimensional pseudorandom lattices also have many applications, e.g., in the encryption of digital images or maps.

Box N-lattice

The definition of I_N^n is extended to more general lattices in the following way: Let $\mathbf{u_1}, \mathbf{u_2}, \ldots \mathbf{u_n}$ be n linearly independent vectors, where the i-th coordinate of $\mathbf{u_i}$ is non-zero, and the other coordinates of $\mathbf{u_i}$ are 0, so $\mathbf{u_i}$ is of the form $(0, 0, \ldots, 0, z_i, 0, \ldots, 0)$. Let $t_1, t_2, \ldots, t_n$ be integers with $0 \leq t_1, t_2, \ldots, t_n < N$. Then we will call the set

$$B_N^n = \{\mathbf{x} = x_1\mathbf{u_1} + x_2\mathbf{u_2} + \cdots + x_n\mathbf{u_n} : 0 \leq x_i|\mathbf{u_i}| \leq t_i (< N) \text{ for } i = 1, 2, \ldots, n\}$$

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

Measures of Binary Lattices

In [3], Hubert, Mauduit and Sárközy introduced the following pseudorandom measure of binary lattices:

Definition

Let

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

The pseudorandom measure of order ℓ of η is defined by

$$Q_\ell(\eta) = \max_{B, d_1, \ldots, d_\ell} \left| \sum_{x \in B} \eta(\mathbf{x} + \mathbf{d_1}) \cdots \eta(\mathbf{x} + \mathbf{d}_\ell) \right|,$$

where the maximum is taken over all distinct $\mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d}_\ell \in I_N^n$ and all box N-lattices B such that $B + \mathbf{d_1}, \ldots, B + \mathbf{d}_\ell \subseteq I_N^n$.

Measures of Binary Lattices

Then, η is said to have strong pseudorandom properties, or, briefly, it is considered a good pseudorandom lattice if the measure $Q_\ell(\eta)$ is small (much smaller than the trivial upper bound N^n) for fixed n and ℓ and large N.

This terminology is justified by the fact that, as was proved in [3], for a truly random binary lattice defined on I_N^n and for fixed ℓ, the measure $Q_\ell(\eta)$ is small (less than $N^{n/2}$ multiplied by a logarithmic factor).

Measures of Binary Lattices

So far, numerous pseudorandom lattices have been generated with optimal pseudorandom measures, see

- K. Gyarmati, C. Mauduit, A. Sárközy *Pseudorandom binary sequences and lattices* Acta Arithmetica 135 (2008) 181-197.
- K. Gyarmati, A. Sárközy, C.L. Stewart *On Legendre symbol lattices*
- K. Gyarmati, C. Mauduit, A. Sárközy *On finite pseudorandom binary lattices*
- L. Mérai, *A construction of pseudorandom binary sequences using rational functions*, Unif. Distrib. Theory 4 (2009), no. 1, 35-49.
- L. Mérai, *Construction of pseudorandom binary lattices using elliptic curves*, Proc. Amer. Math. Soc. 139(2) (2011), 407-420.
- L. Mérai, J. Rivat, A. Sárközy, *The measures of pseudorandomness and the NIST tests*, Lecture Notes in Comput. Sci., 10737, Springer, Cham, 2018, 197-216.

Construction of Binary Lattices

For almost all constructions of pseudorandom binary lattices with strong pseudorandom properties the generation of the elements of the lattice is quite slow. However, in certain applications, we need to generate the elements of the lattice quickly.

In these cases, we recommend the following algorithm: Let $E = (e_1, e_2, \ldots, e_N)$ and $F = (f_1, f_2, \ldots, f_N) \in \{-1, +1\}^N$ be two pseudorandom binary sequences with strong pseudorandom properties; then, we define the binary lattice $\eta = \eta_{E \times F} : I_N^2 \to \{-1, 1\}$ by

$$\eta(x, y) = e_{x+1} f_{y+1}$$

Measure of Binary Lattices

Then, the elements of the lattice can be generated rapidly since each element can be obtained by a simple multiplication, where the multiplicands are all 1 or -1.

The question is, how large are the pseudorandom measures of the lattice? I can determine the exact values of Q_2 and Q_{2k+1} of the lattice, but unfortunately, the value of Q_{2k} is always large if $k \geq 2$:

Theorem (Case of odd k)

Let $E \in \{-1,+1\}^N$ and $F \in \{-1,+1\}^N$ be pseudorandom binary sequences. Then,

$$Q_{2\ell+1}(\eta_{E\times F}) = \max\{Q_1(E), Q_3(E), \ldots, Q_{2\ell+1}(E)\} \max\{Q_1(F), Q_3(F), \ldots, Q_{2\ell+1}(F)\}$$

Proof of Theorem

What is the situation in case of odd k? We are trying to estimate the Q combined measure with the maximum of pseudorandom measure of order $\ell+1$ combined measures, where $\ell = 1, 2, \ldots, k$.
In $k = 2\ell + 1$ we have box-lattice B and k pieces of coordinates
$\mathbf{d_1} = (d_{11}, d_{12}), \ldots, \mathbf{d_k} = (d_{k1}, d_{k2})$

$$
\begin{aligned}
&Q_k(\eta_{E\times F}) \leq \\
&\leq \left| \sum_{x_1,x_2 \in I_1 \times I_2} \eta\left((x_1,x_2)+(d_{11},d_{12})\right)\cdots\eta\left((x_1,x_2)+(d_{k1},d_{k2})\right) \right| \\
&= \left| \sum_{x_1=0}^{t_1} \eta(x_1+d_{11})\cdots\eta(x_1+d_{k1}) \right| \cdot \left| \sum_{x_2=0}^{t_2} \eta(x_2+d_{12})\cdots\eta(x_2+d_{k2}) \right| \\
&= \left| \sum_{x_1=0}^{t_1} e_{x_1+d_{11}}\cdots e_{x_1+d_{k1}} \right| \cdot \left| \sum_{x_2=0}^{t_2} f_{x_2+d_{12}}\cdots f_{x_2+d_{k2}} \right| \\
&= \max\{Q_1(E), Q_3(E), \ldots, Q_k(E)\} \cdot \max\{Q_1(F), Q_3(F)\ldots, Q_k(F)\}
\end{aligned}
$$

Proof of Theorem

Now we prove

$$Q_k(\eta_{E\times F}) \geq$$
$$\max\{Q_1(E), Q_3(E), \ldots, Q_k(E)\} \cdot \max\{Q_1(F), Q_3(F) \ldots, Q_k(F)\}$$

Consider the numbers $0 < d_{11}, d_{12}, \ldots, d_{k1}, d_{k2}$ for which

$$Q_k(E) = \sum_{x_1=0}^{t_1} e_{x_1+d_{11}} \cdots e_{x_1+d_{k1}}$$

and

$$Q_k(F) = \sum_{x_2=0}^{t_2} f_{x_2+d_{12}} \cdots f_{x_2+d_{k2}}$$

Define $\mathbf{d_1} = (d_{11}, d_{12}), \mathbf{d_2} = (d_{21}, d_{22}), \ldots \mathbf{d_k} = (d_{k1}, d_{k2})$. Then

Proof of Theorem

$$Q_k(\eta_{E\times F}) \geq \left|\sum_{x\in B} \eta(\mathbf{x}+\mathbf{d_1})\eta(\mathbf{x}+\mathbf{d_2})\cdots\eta(\mathbf{x}+\mathbf{d_k})\right| =$$

$$= \left|\sum_{x_1,x_2\in I_1\times I_2} \eta\left((x_1,x_2)+(d_{11},d_{12})\right)\cdots\eta\left((x_1,x_2)+(d_{k1},d_{k2})\right)\right|$$

$$= \left|\sum_{x_1=0}^{t_1} \eta\left((x_1+d_{11})\cdots\eta\left((x_1+d_{k1})\right)\right| \cdot \left|\sum_{x_2=0}^{t_2} \eta\left((x_2+d_{12})\cdots\eta\left((x_2+d_{k2})\right)\right|$$

Proof of Theorem

$$= \left| \sum_{x_1=0}^{t_1} e_{x_1+d_{11}} \cdots e_{x_1+d_{k1}} \right| \cdot \left| \sum_{x_2=0}^{t_2} f_{x_2+d_{12}} \cdots f_{x_2+d_{k2}} \right|$$

$$= \max\{Q_1(E), Q_3(E), \ldots, Q_k(E)\} \cdot \max\{Q_1(F), Q_3(F) \ldots, Q_k(F)\}$$

Measure of Binary Lattices

Theorem ($\ell = 2$)

Let $E \in \{-1, +1\}^N$ and $F \in \{-1, +1\}^N$ be pseudorandom binary sequences. Then,

$$Q_2(\eta_{E \times F}) = \max\{NQ_2(E), NQ_2(F)\}$$

Proof of Theorem

First we prove that

$$Q_2(\eta_{E\times F}) \le \max\{N \cdot Q_2(E), N \cdot Q_2(F)\}$$

Consider the box-lattice B and vectors $\mathbf{d_1} = (d_{11}, d_{12})$ and $\mathbf{d_2} = (d_{21}, d_{22})$ for which

$$Q_2(\eta_{E\times F}) = \left|\sum_{\mathbf{x}\in B} \eta(\mathbf{x}+\mathbf{d_1})\eta(\mathbf{x}+\mathbf{d_2})\right|.$$

Then write B of the form

$$B = \{(x_1z_1, x_2z_2) : 0 \le x_1z_1 \le t_1, 0 \le x_2z_2 \le t_2\} = I_1 \times I_2$$

where

$$I_1 = \{x_1z_1 : 0 \le x_1z_1 \le t_1\} \qquad I_2 = \{x_2z_2 : 0 \le x_2z_2 \le t_2\}.$$

Proof of Theorem

Then

$$Q_2(\eta_{E\times F}) =$$

$$= \left| \sum_{x_1,x_2 \in I_1 \times I_2} \eta\left((x_1,x_2)+(d_{11},d_{12})\right)\eta\left((x_1,x_2)+(d_{21},d_{22})\right) \right|$$

$$= \left| \sum_{x_1=0}^{t_1} \eta(x_1+d_{11})\eta(x_1+d_{21}) \right| \cdot \left| \sum_{x_2=0}^{t_2} \eta(x_2+d_{21})\eta(x_2+d_{22}) \right|$$

$$= \left| \sum_{x_1=0}^{t_1} e_{x_1+d_{11}} \cdot e_{x_1+d_{21}} \right| \cdot \left| \sum_{x_2=0}^{t_2} f_{x_2+d_{12}} \cdot f_{x_2+d_{22}} \right| \leq \max\{NQ_2(E), NQ_2(F)\}$$

Proof of Theorem

Next we prove the $Q_2(\eta_{E\times F}) \geq Q_2(E) \times Q_2(F)$ consider the sets

$$I_1 = \{x_1 z_1 : 0 \leq x_1 z_1 \leq t_1\} \quad \text{and} \quad I_2 = \{x_2 z_2 : 0 \leq x_2 z_2 \leq t_2\}$$

and numbers $0 \leq d_{11}, d_{21}, d_{12}, d_{22} \leq N$ for which

$$Q_2(E) = \sum_{0 \leq x_1 z_1 \leq t_1} e_{x_1+d_{11}} e_{x_1+d_{21}}$$

and

$$Q_2(F) = \sum_{0 \leq x_2 z_2 \leq t_1} f_{x_2+d_{12}} f_{x_2+d_{22}}.$$

Proof of Theorem

Define d_1 and d_2 by $d_1 = (d_{11}, d_{12})$ and $d_2 = (d_{21}, d_{22})$. Then

$$Q_2(\eta_{E\times F}) \geq \left|\sum_{x\in B} \eta(\mathbf{x}+\mathbf{d_1})\eta(\mathbf{x}+\mathbf{d_2})\right| =$$

$$\left|\sum_{x_1=0}^{t_1} \eta(x_1+d_{11})\eta(x_1+d_{21})\right| \cdot \left|\sum_{x_2=0}^{t_2} \eta(x_2+d_{12})\eta(x_2+d_{22})\right| =$$

$$\left|\sum_{x_1=0}^{t_1} e_{x_1+d_{11}} \cdot e_{x_1+d_{21}}\right| \cdot \left|\sum_{x_2=0}^{t_2} f_{x_2+d_{12}} \cdot f_{x_2+d_{22}}\right| = \max\{NQ_2(E), NQ_2(F)\}.$$

with this we proved that $Q_2(\eta_{E\times F}) = \max\{N \cdot Q_2(E), N \cdot Q_2(F)\}$ □

Measure of Binary Lattices

Theorem (Even case)

Let $E \in \{-1,+1\}^N$ *and* $F \in \{-1,+1\}^N$ *be pseudorandom binary sequences and* $\ell \geq 2$. *Then,*

$$Q_{2\ell}(\eta_{E\times F}) \geq (N-\ell+2)^2$$

Proof of Theorem

Let's consider the $Q_{2\ell}$. Let $\mathbf{x} = (x_1, x_2)$, $\mathbf{d_1} = (0,0)$, $\mathbf{d_2} = (0,1)$, $\mathbf{d_3} = (1,1)$, $\ldots$,$\mathbf{d_{2\ell}} = (\ell - 1, 0)$

$$Q_{2\ell}(\eta_{E\times F}) \geq \left| \sum_{x \in I_{N-1}^2} \eta(\mathbf{x}+\mathbf{d_1})\eta(\mathbf{x}+\mathbf{d_2})\ldots\eta(\mathbf{x}+\mathbf{d_{2\ell}}) \right|$$

$$= \left| \sum_{x_1=0}^{N-\ell+1} \sum_{x_2=0}^{N-\ell+1} \eta(x_1,x_2)\eta(x_1,x_2+1)\ldots\eta(x_1,x_2+\ell-1) \right|$$

$$= \left| \sum_{x_1=0}^{N-\ell+1} \sum_{x_2=0}^{N-\ell+1} e_{x_1+1} f_{x_2+1} e_{x_1+1} f_{x_2+2} e_{x_1+2} f_{x_2+1} \cdots e_{x_1+\ell-1} f_{x_2+1} \right|$$

Proof of Theorem

$$= \left| \sum_{x_1=0}^{N-\ell+1} e_{x_1+1}^2 \cdot e_{x_1+2}^2 \cdots e_{x_1+\ell-1}^2 \right| \cdot \left| \sum_{x_2=0}^{N-\ell+1} f_{x_2+1}^2 f_{x_2+2}^2 \cdots f_{x_2+\ell-1}^2 \right|$$

$$= \left| \sum_{x_1} \sum_{x_2} 1 \right| = (N-\ell+2)^2$$

□

Binary Lattices

What method should we use to choose coordinate points for any ℓ? If we plot the points $\ell = 2, 3, \ldots$ we can notice some regularity. Consider the following coordinates:

$$\begin{aligned} &(i, i+1) && \text{if} \quad i = 0, 1, \ldots, \ell - 2 \\ &(i, i) && \text{if} \quad i = 0, 1, \ldots, \ell - 1 \\ &(\ell - 1, 0) \end{aligned}$$

Binary Lattices

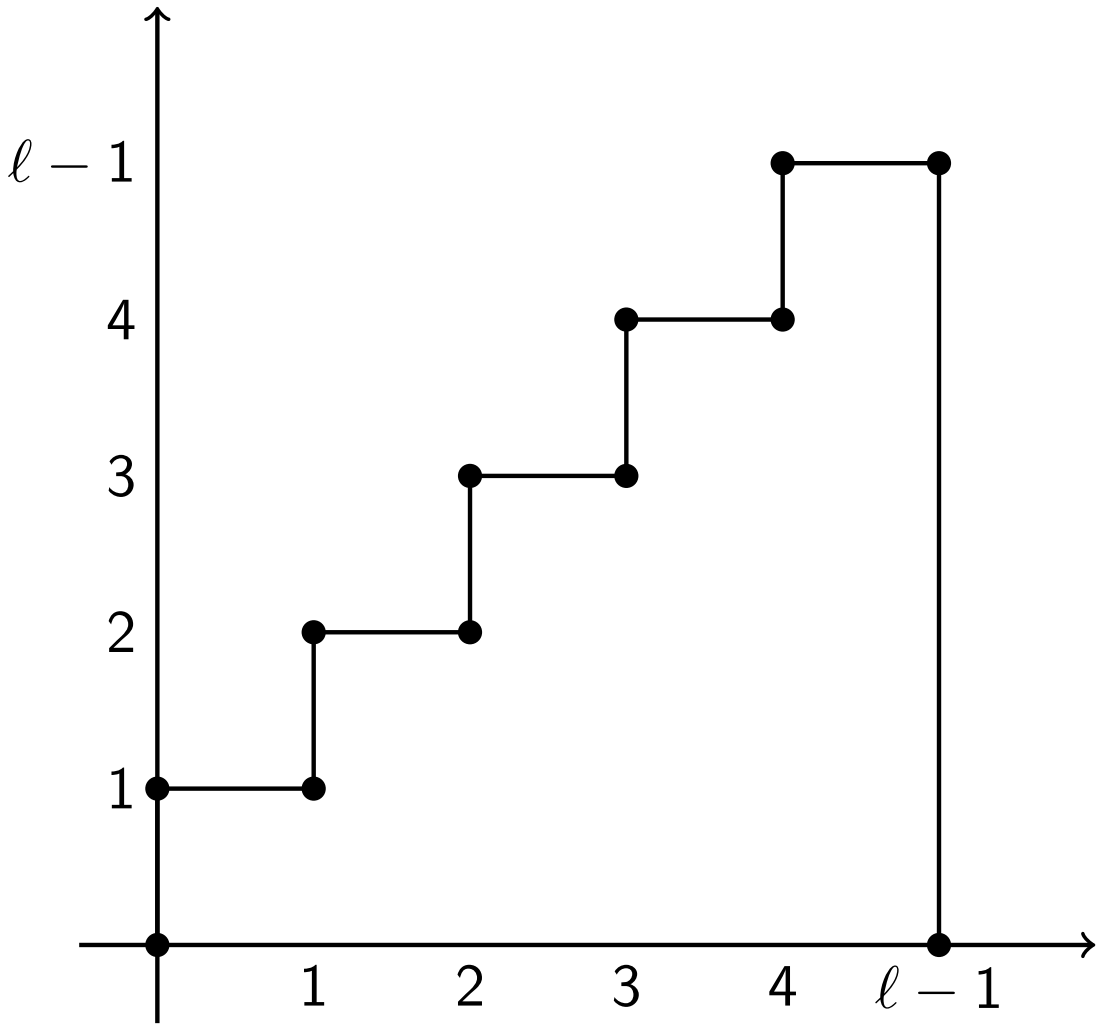

Figure: Step function shape in the coordinate system

Measure of Binary Lattices

This generation method is viable when we want to use the lattices in applications where it is sufficient that the measures Q_1, Q_2, and Q_3 are small (e.g., Monte Carlo methods).

If we still need Q_4 to be small (e.g., in encryptions), we need to look for another method.

Note also that Gyarmati [1] generated a sequence of length N^2 from the lattice $\eta : I_N^2 \to \{-1, +1\}$, by writing the rows of the lattice consecutively from the bottom up to the top. She proved that if, for the lattice $\eta : I_n^2 \to \{-1, +1\}$, Q_k is small, then the resulting sequence of length N^2 has a small C_k measure.

Measure of Binary Lattices

By incorporating this method into our previous construction, we can generate a lattice from two sequences E and $F \in \{-1, +1\}^N$, and then a sequence of length N^2, by writing the rows of the lattice consecutively in sequence from the bottom up to the top.

Then, the resulting sequence of length N^2 has small pseudorandom measures W, C_2, and C_3 if the measures $Q_2(E), Q_2(F), Q_3(E)$, and $Q_3(F)$ of the original sequences of length N are small. With this technique, we obtained a much longer sequence (length N^2) from two short sequences (length N), such that the low-order pseudorandomness measures W, C_2, and C_3 are close to optimal.

Binary Lattices

Remark

We saw that Q_1, Q_2, Q_3 are small and Q_4 (and $Q_{2\ell}$) for $\ell \geq 2$ are large.

In case of $k \geq 5$ the calculation of Q_k is hopelessly slow with computer as well, but in this paper we focus on that applications in which Q_1, Q_2, Q_3 are small because this garanties the pseudorandomness of the applications. Summarize above results we have:

- $Q_1 = W(E) \cdot W(F)$
- $Q_2 = \max\{NQ_2(E), NQ_2(F)\}$
- $Q_3 = \max\{Q_1(E), Q_3(E)\} \cdot \max\{Q_1(F), Q_3(F)\}$
- $Q_4 \geq (N - \ell + 1)^2$

3-dimension lattices

Let $\mathbf{x} = (x_1, x_2, x_3)$, $\mathbf{d_1} = (d_{11}, d_{12}, d_{13})$ and $\mathbf{d_2} = (d_{21}, d_{22}, d_{23})$. Let B, d_1, d_2 fixed and

$$B_N^3 = \{(x_1 z_1, x_2 z_2, x_3 z_3) : x_1, x_2, x_3 \in \{0, 1, \cdots, N-1\}\} = I_1 \times I_2 \times I_3$$

where

$$I_1 = \{x_1 z_1 : 0 \leq x_1 z_1 \leq t_1\},$$
$$I_2 = \{x_2 z_2 : 0 \leq x_2 z_2 \leq t_2\},$$
$$I_3 = \{x_3 z_3 : 0 \leq x_3 z_3 \leq t_3\}$$

3-dimension lattices – $Q_2(\eta)$

Consider the following pseudorandom measure of order 2 of η:

$$Q_2(\eta_{E\times F\times G}) = \max \left| \sum_{x_1,x_2,x_3 \in I_1\times I_2\times I_3} \eta\left(\mathbf{x}+\mathbf{d_1}\right)\eta\left(\mathbf{x}+\mathbf{d_2}\right) \right|$$

Theorem

$$Q_2(\eta_{E\times F\times G}) = \max\{N^2\cdot Q_2(E_N), N^2\cdot Q_2(F_N), N^2\cdot Q_2(G_N)\}$$

3-dimension lattices – Proof

At first we prove that

$$Q_2(\eta_{E\times F\times G}) \le N^2 Q_2(E_N)\cdot N^2 Q_2(F_N)\cdot N^2\cdot Q_2(G_N)$$

Let B a box lattice and $d_1=(d_{11},d_{12},d_{13})$ and $d_2=(d_{21},d_{22},d_{23})$ vectors and let

$$\begin{aligned} B &= \{x_1z_1, x_2z_2, x_3z_3 : 0\le x_1z_1\le t_1, 0\le x_2z_2\le t_2, 0\le x_3z_3\le t_3\}\\ &= I_1\times I_2\times I_3 \end{aligned}$$

where

$$\begin{aligned} &I_1=\{x_1z_1 : 0\le x_1z_1\le t_1\},\quad I_2=\{x_2z_2 : 0\le x_2z_2\le t_2\},\\ &I_3=\{x_3z_3 : 0\le x_3z_3\le t_3\} \end{aligned}$$

3-dimension lattices – Proof

Then

$$Q_2(\eta_{E\times F\times G}) = \left| \sum_{x_1,x_2,x_3\in I_1\times I_2\times I_3} \eta\left(\mathbf{x}+\mathbf{d_1}\right)\eta\left(\mathbf{x}+\mathbf{d_2}\right)\right| =$$

$$= \left|\sum_{x_1=0}^{t_1} \eta(x_1+d_{11})\eta(x_1+d_{21})\right| \cdot \left|\sum_{x_2=0}^{t_2} \eta(x_2+d_{12})\eta(x_2+d_{22})\right|$$

$$\cdot \left|\sum_{x_3=0}^{t_3} \eta(x_3+d_{13})\eta(x_2+d_{23})\right|$$

3-dimension lattices – Proof

$$= \left| \sum_{x_1=0}^{t_1} e_{x_1+d_{11}} \cdot e_{x_1+d_{21}} \right| \cdot \left| \sum_{x_2=0}^{t_2} f_{x_2+d_{12}} \cdot f_{x_2+d_{22}} \right| \cdot \left| \sum_{x_3=0}^{t_3} g_{x_3+d_{13}} \cdot g_{x_3+d_{23}} \right|$$

$$\leq Q_2(E_N) \cdot Q_2(F_N) \cdot Q_2(G_N)$$

3-dimension lattices – Proof

On the other hand to satisfy the $Q_2(\eta_{E\times F\times G}) = Q_2(E)Q_2(F)Q_2(G)$ let us consider that

$$I_1 = \{x_1z_1 : 0 \le x_1z_1 \le t_1\}, \quad I_2 = \{x_2z_2 : 0 \le x_2z_2 \le t_2\},$$
$$I_3 = \{x_3z_3 : 0 \le x_3z_3 \le t_3\}$$

sets and $0 \le d_{11}, d_{12}, d_{13}, d_{21}, d_{22}, d_{23} \le N$ numbers (coordinates) for which

3-dimension lattices – Proof

$$Q_2(E_N) = \sum_{0 \le x_1 z_1 \le t_1} e_{x_1+d_{11}} e_{x_1+d_{21}}$$

and

$$Q_2(F_N) = \sum_{0 \le x_2 z_2 \le t_2} f_{x_2+d_{12}} f_{x_2+d_{22}}$$

and

$$Q_2(G_N) = \sum_{0 \le x_3 z_3 \le t_3} g_{x_3+d_{13}} f_{x_3+d_{23}}$$

Let $d_1 = (d_{11}, d_{12}, d_{13})$ and $d_2 = (d_{21}, d_{22}, d_{23})$. Then

3-dimension lattices – Proof

$$Q_2(\eta_{E\times F\times G}) \le \left|\sum_{x\in B} \eta\left(\mathbf{x}+\mathbf{d_1}\right)\eta\left(\mathbf{x}+\mathbf{d_2}\right)\right| = \left|\sum_{x_1=0}^{t_1} \eta(x_1+d_{11})\eta(x_1+d_{21})\right| \cdot$$

$$\cdot \left|\sum_{x_2=0}^{t_2} \eta(x_2+d_{12})\eta(x_2+d_{22})\right| \cdot \left|\sum_{x_3=0}^{t_3} \eta(x_3+d_{13})\eta(x_2+d_{23})\right| =$$

$$= \left|\sum_{x_1=0}^{t_1} e_{x_1+d_{11}}\, e_{x_1+d_{21}}\right| \cdot \left|\sum_{x_2=0}^{t_2} f_{x_2+d_{12}}\, f_{x_2+d_{22}}\right| \cdot \left|\sum_{x_3=0}^{t_3} g_{x_3+d_{13}}\, g_{x_3+d_{23}}\right|$$

$$= N^2 Q_2(E_N) \cdot N^2 Q_2(F_N) \cdot N^2 Q_2(G_N)$$

3-dimension lattices – $Q_3(\eta)$

Consider the following pseudorandom measure of order 3 of η:

$$Q_3(\eta) = \sum_{x_1,x_2,x_3 \in I_1 \times I_2 \times I_3} \eta\left(\mathbf{x} + \mathbf{d_1})\right) \eta\left(\mathbf{x} + \mathbf{d_2}\right) \eta\left(\mathbf{x} + \mathbf{d_3}\right)$$

Theorem

$$Q_3(\eta_{E \times F \times G}) =$$

$$\max\{Q_1(E), Q_3(E)\} \cdot \max\{Q_1(F), Q_3(F)\} \cdot \max\{Q_1(G), Q_3(G)\}$$

3-dimension lattices – $Q_4(\eta)$

Let $x_1, x_2, x_3 \in I_1 \times I_2 \times I_3$ and consider the following pseudorandom measure of order 4 of η:

$$Q_4(\eta) = \sum_{x_i} \eta\left(\mathbf{x} + \mathbf{d_1}\right) \eta\left(\mathbf{x} + \mathbf{d_2}\right) \eta\left(\mathbf{x} + \mathbf{d_3}\right) \eta\left(\mathbf{x} + \mathbf{d_4}\right)$$

Theorem

$$Q_4(\eta_{E \times F \times G}) \geq (N - \ell)^3$$

Conclusion

- New constructions for binary lattices based on pseudorandom sequences
- Explicit bounds for Q_k measures in 2D and 3D
- Trade-off: efficient generation vs. high-order pseudorandomness
- Useful for cryptography and Monte Carlo simulations

End

Thank you for your attention!

References

- K. Gyarmati, C. Mauduit, A. Sárközy *On finite pseudorandom binary lattices*
- K. Gyarmati, A. Sárközy, C.L. Stewart *On Legendre symbol lattices*
- P. Hubert, C. Mauduit and A. Sárközy, *On pseudorandom binary lattices*, Acta Aritmetica 125.1 (2006)
- K. Gyarmati, C. Mauduit, A. Sárközy *Pseudorandom binary sequences and lattices* Acta Arithmetica 135 (2008) 181-197.

References

- K. Gyarmati, *Measures of pseudorandomness*
- L. Mérai, *A construction of pseudorandom binary sequences using rational functions*, Unif. Distrib. Theory 4 (2009), no. 1, 35-49.
- L. Mérai, *Construction of pseudorandom binary lattices using elliptic curves*, Proc. Amer. Math. Soc. 139(2) (2011), 407-420.
- L. Mérai, J. Rivat, A. Sárközy, *The measures of pseudorandomness and the NIST tests*, Lecture Notes in Comput. Sci., 10737, Springer, Cham, 2018, 197-216.
- A. Sárközy, *A finite pseudorandom binary sequence*, Studia Sci. Math. Hungar. 38 (2001), 377-384.