**Studia Scientiarum Mathematicarum Hungarica**
***Combinatorics, Geometry and Topology***
63 (2026) 1, 40–50
DOI: 10.1556/012.2026.04344

# FAST CONSTRUCTION OF PSEUDORANDOM BINARY SEQUENCES AND LATTICES

Károly Müllner[1,*]

[1] Eötvös Loránd University, Institute of Mathematics, Budapest, Hungary

*Communicated by L. Csirmaz*

**Original Research Paper**

**Received: Oct 3, 2025 • Accepted: Feb 17, 2026**



## ABSTRACT

In the practical application of pseudorandom binary sequences (e.g., in cryptography or signal processing), a need often arises for a long binary sequence while only much shorter binary sequences with suitable properties are readily available. In this paper, an $N^2$-element pseudorandom binary lattice is constructed from two shorter, $N$-length binary sequences with strong pseudorandom properties. Next, this $N^2$-element binary lattice is 'unrolled' (using a row-major order) to generate a significantly longer $N^2$-element pseudorandom sequence. While optimal upper bounds for the pseudorandom measures of this new lattice and sequence are not established, we provide non-trivial upper bounds for these measures, demonstrating their strong pseudorandom properties.

## KEYWORDS

**Pseudorandom lattices, pseudorandom binary sequences**

## MATHEMATICS SUBJECT CLASSIFICATION (2020)

Primary 11K45

* Corresponding author. E-mail: mullni@hotmail.com

## 1. INTRODUCTION

In 1997, Mauduit and Sárközy [11] introduced a new constructive approach to study the pseudorandomness of binary sequences

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

In particular, in [17], Mauduit and Sárközy introduced the following measures of pseudorandomness. The *well-distribution measure* of $E_N$ is defined by

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

where the maximum is taken over all $a, b, t \in \mathbb{N}$ with $1 \le a \le a + (t-1)b \le N$. 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 $D = (d_1, d_2, \dots, d_k)$ and $M$ such that $0 \le d_1 < d_2 < \cdots < d_k \le N - M$. They also introduced the *combined* (well-distribution-correlation) *pseudorandom measure* of order $k$:

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

where the maximum is taken over all $a, b, t$, and $D = (d_1, d_2, \dots, d_k)$ such that all $d_i$'s are different and all the indices $a + jb + d_i$ belong to $\{1, 2, \dots, N\}$. The sequence $E_N$ is considered a "good" pseudorandom sequence if both $W(E_N)$ and $C_k(E_N)$ are small in terms of $N$.

To study the multidimensional analogue of pseudorandomness, Hubert, Mauduit, and Sárközy [9] established the following definitions and terminology. The set of $n$-dimensional vectors with integer coordinates ranging from 0 to $N-1$ is denoted by $I_N^n$:

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

This set is often called an $n$-dimensional $N$-lattice, or simply an $N$-lattice. Hubert, Mauduit, and Sárközy [9] extended the concept of binary sequences to higher dimensions by defining functions of the form

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

For simplicity, when $\mathbf{x} = (x_1, x_2, \dots, x_n)$ and $\eta(\mathbf{x}) = \eta((x_1, x_2, \dots, x_n))$, we will use the shorter notation $\eta(\mathbf{x}) = \eta(x_1, x_2, \dots, x_n)$.

These functions can be visually represented by assigning the points of an $N$-lattice with either a + or a − symbol. Binary pseudorandom lattices in two or three dimensions have significant practical applications, such as in the encryption of digital images or maps.

To broaden the scope of the definition of $I_N^n$ and to define the multidimensional version of pseudorandom measures, it is also important to introduce more general box-lattices. These are introduced as follows. Let $\mathbf{u_1}, \mathbf{u_2}, \dots, \mathbf{u_n}$ be a set of $n$ linearly independent vectors. Each vector

$\mathbf{u_i}$ is defined such that its $i$-th coordinate is non-zero, while all other coordinates are zero. This means $\mathbf{u_i}$ has the form $(0, 0, \dots, 0, z_i, 0, \dots, 0)$. If $t_1, t_2, \dots, t_n$ are integers with $0 \le t_1, t_2, \dots, t_n < N$, then the set

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

is called an $n$-dimensional box $N$-lattice, or simply a box $N$-lattice. In [9], Hubert, Mauduit, and Sárközy introduced the following measure for the pseudorandomness of binary lattices.

**DEFINITION 1.** Let

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

The pseudorandom measure of order $\ell$ for $\eta$ is defined as

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

where the maximum is computed over all distinct vectors $\mathbf{d_1}, \mathbf{d_2}, \dots, \mathbf{d}_\ell \in I_N^n$ and all box $N$-lattices $B$ such that the translated lattices $B + \mathbf{d_1}, \dots, B + \mathbf{d}_\ell$ are subsets of $I_N^n$.

A lattice $\eta$ is then said to possess strong pseudorandom properties, or is briefly referred to as a good pseudorandom lattice, if the measure $Q_\ell(\eta)$ is small (significantly smaller than the trivial upper bound of $N^n$) for fixed $n$ and $\ell$ and large $N$. For the best constructions, an upper bound of $N^{n/2}(\log N)^c$ is achievable, but in practical applications, estimates of $N^{(1-\varepsilon)n}$ are also ideal.

A wide variety of pseudorandom lattices with optimal pseudorandom measures have been constructed to date. See, for instance, [1, 5, 7, 4, 8, 9, 12, 13] and [14, 16].

When a large lattice is required for a practical application, generating each element with a computer can be a time-consuming and computationally expensive process. Here, we introduce a novel lattice generation technique that instantly creates an $N^2$-element lattice from two $N$-length sequences. Although its pseudorandom measures may not be optimal, we can provide strong upper bounds for them. The method is as follows. Let $E = (e_1, e_2, \dots, e_N)$ and $F = (f_1, f_2, \dots, f_N) \in \{-1, +1\}^N$ 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

$$\eta(x, y) = e_{x+1} f_{y+1} \tag{1.1}$$

The elements of the lattice can be generated rapidly since each element is a simple product of factors that are either 1 or $-1$. This raises the question of how large the pseudorandom measures of the lattice are. We can determine the exact values of $Q_2$ and $Q_{2k+1}$ for this lattice. However, the value of $Q_{2k}$ is always large if $k \ge 2$, which is a drawback of this method.

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

$$Q_{2\ell+1}(\eta_{E\times F}) \le \max\{Q_1(E), Q_3(E), \dots, Q_{2\ell+1}(E)\} \max\{Q_1(F), Q_3(F), \dots, Q_{2\ell+1}(F)\} \tag{1.2}$$

*and*

$$Q_{2\ell+1}(\eta_{E\times F}) \ge Q_{2\ell+1}(E) Q_{2\ell+1}(F). \tag{1.3}$$

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

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

**THEOREM 3.** *Let $E \in \{-1,+1\}^N$ and $F \in \{-1,+1\}^N$ be pseudorandom binary sequences and $\ell \geq 2$. Then,*

$$Q_{2\ell}(\eta_{E\times F}) \geq (N-\ell+1)^2$$

This generation method is viable for applications where it's sufficient for the measures $Q_1$, $Q_2$, and $Q_3$ to be small (e.g., in Monte Carlo methods). However, if we also need $Q_4$ to be small (e.g., for encryption), we must use a different method.

## 2. AUGMENTATION OF SEQUENCES

We have already seen that an $N^2$-element lattice can be generated from two $N$-length sequences. Let the two original sequences be $E_N, F_N \in \{-1,+1\}^N$, and let the lattice constructed from them using (1.1) be denoted by $\eta$. Then, for $\eta$, the statements of Theorems 1, 2, and 3 from Section 1 hold. In [3], Gyarmati generated an $N^2$-length sequence from the lattice $\eta : I_N^2 \to \{-1,+1\}^2$ in the following way. $\widetilde{E}_{N^2} = \widetilde{E}_{N^2}(\eta) = (e_1, e_2, \dots, e_{N^2}) \in \{-1,+1\}^{N^2}$ by taking the first (from the bottom) row of the lattice then we continue the binary sequence by taking the second row of the lattice, then the third row follows, etc.; in general, we set

$$e_{iN+j} = \eta((j-1,i)) \text{ for } i = 0,1,\dots,N^2-1, \quad j = 1,2,\dots,N. \tag{2.1}$$

Gyarmati [3, Theorem 3] proved the following very general theorem.

**LEMMA 1.**

$$C_\ell(\widetilde{E}_{N^2}) \leq (\ell+2)C_\ell(\eta).$$

In our case, this implies that if $E_N$ and $F_N$ denote the two $N$-length sequences, then by Theorem 1 we have

$$C_{2\ell+1}(\widetilde{E}_{N^2}) \leq (2\ell+3)\max\{Q_1(E_N),\dots,Q_{2\ell+1}(E_N)\}\max\{Q_1(F_N),\dots,Q_{2\ell+1}(F_N)\}.$$

By Theorem 2, we have

$$C_2(\widetilde{E}_{N^2}) \leq 4\max\{NQ_2(E_N), NQ_2(F_N)\}.$$

Thus, the new sequence $\widetilde{E}_{N^2}$ is significantly longer than the two original sequences, $E_N$ and $F_N$. By Theorems 1 and 2, we can provide non-trivial upper bounds for measures such as $C_2(\widetilde{E}_{N^2})$ and $C_3(\widetilde{E}_{N^2})$. In essence, this technique allows for the fast augmentation of even a short sequence. We take two equally long subsequences (e.g., the beginning and the end of the sequence) and use cross-multiplication (see (1.1)) to generate a lattice. From this lattice, we then generate a new sequence based on formula (2.1). The length of this new sequence increases quadratically throughout the process. Nevertheless, we can still provide a sharp upper bound for the $C_2$ and $C_3$ values. For example, if $Q_1(E_N), Q_1(F_N), Q_2(E_N), Q_2(F_N), Q_3(E_N), Q_3(F_N) \leq \sqrt{N}(\log N)^c$, then

$$Q_2(\widetilde{E}_{N^2}) \leq 4N^{3/2}(\log N)^c.$$

$$Q_3(\widetilde{E}_{N^2}) \leq 5N(\log N)^{2c}.$$

To be able to apply the method described in this section, it is necessary to construct large families of binary sequences where the sequences have a small $Q_2$ measure. In [15] I provide a method showing that if certain types of families of binary sequences satisfy the condition that their sequences have a small $C_2$ measure, then their $Q_2$ measure is also small. For instance, it can be shown that in each of the constructions of length $N$ in [2, 6, 10] the $Q_2$ measure is below $\sqrt{N}(\log N)^c$ (see [15]).

This construction facilitates the rapid augmentation of binary sequences by generating an $N^2$-length sequence from two components of length $N$ via a lattice-based cross-multiplication. By applying Theorems 1 and 2, we can establish non-trivial upper bounds for the correlation measures of the augmented sequence, such as $C_2(\widetilde{E}_{N^2})$ and $C_3(\widetilde{E}_{N^2})$, based on the pseudorandom properties of the initial segments. Notably, even with a quadratic increase in length, the pseudorandom measures remain sharp, provided that the underlying sequences belong to families with sufficiently small $Q_2$ measures. This relationship motivates the search for generalized methods that could maintain low $Q_\ell$ measures for higher orders of $\ell$ during the augmentation process.

I find it important to ask the following.

**PROBLEM 1.** *Does a similar method exist for generating an $N^2$-element lattice, and subsequently an $N^2$-element sequence, from two $N$-long sequences, such that not only the $Q_2$ and $Q_3$ measures are low, but also other $Q_\ell$ measures are low, at least for small $\ell$?*

## 3. PROOFS

First, we prove Theorem 1 concerning the odd order.

*Proof of Theorem 1.* Let $k = 2\ell + 1$. First we prove (1.2). Consider the box lattice $B$ and the vectors $d_1 = (d_{11}, d_{12}), d_2 = (d_{21}, d_{22}), \dots, d_k = (d_{k1}, d_{k2})$ with $B + d_1, \dots, B + d_k \subseteq I_N^2$, such that

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

Write $B$ in the form $B = \{(x_1z_1, x_2z_2 : 0 \le x_1z_1 \le t_1, 0 \le x_2z_2 < t_2)\} = I_1 \times I_2$, where

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

and $z_1, z_2$ are positive integers. Then,

$$\begin{aligned} Q_k(\eta_{E\times F}) &= \left|\sum_{(x_1z_1, x_2z_2)\in I_1\times I_2} \eta\left((x_1z_1, x_2z_2) + (d_{11}, d_{12})\right)\cdots\eta\left((x_1z_1, x_2z_2) + (d_{k1}, d_{k2})\right)\right| \\ &= \left|\sum_{\substack{0\le x_1z_1\le t_1\\ 0\le x_2z_2\le t_2}} e_{x_1z_1+d_{11}+1} f_{x_2z_2+d_{12}+1} e_{x_1z_1+d_{21}+1} f_{x_2z_2+d_{22}+1} \dots e_{x_1z_1+d_{k1}+1} f_{x_2z_2+d_{k2}+1}\right| \end{aligned}$$

$$= \left| \sum_{0 \le x_1 z_1 \le t_1} e_{x_1 z_1 + d_{11} + 1} \cdots e_{x_1 z_1 + d_{k1} + 1} \right| \cdot \left| \sum_{0 \le x_2 z_2 \le t_2} f_{x_2 z_2 + d_{12} + 1} \cdots f_{x_2 z_2 + d_{k2} + 1} \right|. \tag{3.1}$$

We know that if $d_{i1} = d_{j1}$, then $e_{x_1 z_1 + d_{i1} + 1} e_{x_1 z_1 + d_{j1} + 1} = 1$, and similarly, if $d_{i2} = d_{j2}$, then $e_{x_2 z_2 + d_{i2} + 1} e_{x_2 z_2 + d_{j2} + 1} = 1$. Since $k$ is odd, if we consider the elements $d_{i1}$ in the multiset $\{d_{11}, d_{21}, \dots, d_{k1}\}$ that appear an odd number of times, and their set is $\{d^*_{i1}, \dots, d^*_{v1}\}$, then $v$ is also odd and

$$\begin{aligned} \left| \sum_{0 \le x_1 z_1 \le t_1} e_{x_1 z_1 + d_{11} + 1} \dots e_{x_1 z_1 + d_{k1} + 1} \right| &= \left| \sum_{0 \le x_1 z_1 \le t_1} e_{x_1 z_1 + d^*_{11} + 1} \dots e_{x_1 z_1 + d^*_{v1} + 1} \right| \le Q_v(E) \\ &\le \max\{Q_1(E), Q_3(E), \dots, Q_k(E)\}. \end{aligned}$$

Similarly, it can be shown that

$$\left| \sum_{0 \le x_2 z_2 \le t_2 + 1} f_{x_2 z_2 + d_{21} + 1} \dots f_{x_2 z_2 + d_{k2} + 1} \right| \le \max\{Q_1(F), Q_3(F), \dots, Q_k(F)\}$$

Thus, by (3.1),

$$Q_e(\eta_{E \times F}) \le \max\{Q_1(E), Q_3(E), \dots, Q_e(E)\} \cdot \max\{Q_1(F), Q_3(F), \dots, Q_k(F)\}.$$

Next we prove (1.3). Consider the integers $0 < z_1, z_2, t_1, t_2 \le N,\ 0 \le d_{11}, d_{12}, \dots, d_{k1}, d_{k2} \le N-1$ for which

$$Q_k(E) = \left| \sum_{0 \le x_1 z_1 \le t_1} e_{x_1 z_1 + d_{11} + 1} \cdot e_{x_1 z_1 + d_{k1} + 1} \right|$$

and

$$Q_k(F) = \left| \sum_{0 \le x_2 z_2 \le t_2} f_{x_1 z_1 + d_{12} + 1} \cdot f_{x_2 z_2 + d_{k2} + 1} \right|$$

Let $\mathbf{d_1} = (d_{11}, d_{12})$, $\mathbf{d_2} = (d_{21}, d_{22})$, …, $\mathbf{d_k} = (d_{k1}, d_{k2})$, and define the box-lattice $B$ by $B = I_1 \times I_2$, where

$$\begin{aligned} I_1 &= \{x_1 z_1 :\ 0 \le x_1 z_1 \le t_1\}, \\ I_2 &= \{x_2 z_2 :\ 0 \le x_2 z_2 \le t_2\}. \end{aligned}$$

Then,

$$\begin{aligned} Q_k(\eta_{E \times F}) &\ge \left| \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d_1}) \eta(\mathbf{x} + \mathbf{d_2}) \cdots \eta(\mathbf{x} + \mathbf{d_k}) \right| = \\ &= \left| \sum_{(x_1 z_1, x_2 z_2) \in I_1 \times I_2} \eta\left((x_1 z_1, x_2 z_2) + (d_{11}, d_{12})\right) \cdots \eta\left((x_1 z_1, x_2 z_2) + (d_{k1}, d_{k2})\right) \right| \\ &= \left| \sum_{\substack{0 \le x_1 z_1 \le t_1 \\ 0 \le x_2 z_2 \le t_2}} e_{x_1 z_1 + d_{11} + 1} f_{x_2 z_2 + d_{12} + 1} e_{x_1 z_1 + d_{21} + 1} f_{x_2 z_2 + d_{22} + 1} \dots e_{x_1 z_1 + d_{k1} + 1} f_{x_2 z_2 + d_{k2} + 1} \right| \end{aligned}$$

$$
\begin{aligned}
&= \left| \sum_{0 \le x_1 z_1 \le t_1} e_{x_1 z_1 + d_{11} + 1} \cdots e_{x_1 z_1 + d_{k1} + 1} \right| \cdot \left| \sum_{0 \le x_2 z_2 \le t_2} f_{x_2 z_2 + d_{12} + 1} \cdots f_{x_2 z_2 + d_{k2} + 1} \right| \\
&= Q_k(E) Q_k(F),
\end{aligned}
$$

which completes the proof. □

Proof of Theorem 2. First we prove that

$$
Q_2(\eta_{E \times F}) \le \max\{N \cdot Q_2(E), N \cdot Q_2(F)\}. \tag{3.2}
$$

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

$$
B = \{(x_1 z_1, x_2 z_2) : \ 0 \le x_1 z_1 \le t_1, 0 \le x_2 z_2 \le t_2\} = I_1 \times I_2,
$$

where

$$
I_1 = \{x_1 z_1 : \ 0 \le x_1 z_1 \le t_1\} \qquad I_2 = \{x_2 z_2 : \ 0 \le x_2 z_2 \le t_2\}.
$$

Then

$$
\begin{aligned}
Q_2(\eta_{E \times F}) &= \left| \sum_{(x_1 z_1, x_2 z_2) \in I_1 \times I_2} \eta\left((x_1 z_1, x_2 z_2) + (d_{11}, d_{12})\right) \eta\left((x_1 z_1, x_2 z_2) + (d_{21}, d_{22})\right) \right| \\
&= \left| \sum_{\substack{0 \le x_1 z_1 \le t_1 \\ 0 \le x_2 z_2 \le t_2}} e_{x_1 z_1 + d_{11} + 1} f_{x_2 z_2 + d_{12} + 1} \cdot e_{x_1 z_1 + d_{21} + 1} f_{x_2 z_2 + d_{22} + 1} \right| \\
&= \left| \sum_{0 \le x_1 z_1 \le t_1} e_{x_1 z_1 + d_{11} + 1} \cdot e_{x_1 z_1 + d_{21} + 1} \right| \cdot \left| \sum_{0 \le x_2 z_2 \le t_2} f_{x_2 z_2 + d_{12} + 1} \cdot f_{x_2 z_2 + d_{22} + 1} \right|.
\end{aligned} \tag{3.3}
$$

Since the vectors $\mathbf{d_1}$ and $\mathbf{d_2}$ are not equal, at least one of the following inequalities holds: $d_{11} \ne d_{21}$ and $d_{21} \ne d_{22}$. Let us first consider the case where $d_{11} \ne d_{21}$. In this case, we have

$$
\left| \sum_{0 \le x_1 z_1 \le t_1} e_{x_1 z_1 + d_{11} + 1} \cdot e_{x_1 z_1 + d_{21} + 1} \right| \le Q_2(E),
$$

while for the other factor in (3.3) we apply the trivial estimate

$$\left|\sum_{0\le x_2z_2\le t_2} f_{x_2z_2+d_{12}+1}\cdot f_{x_2z_2+d_{22}+1}\right|\le 1+t_2\le N.$$

Thus, according to (3.3),

$$Q_2(\eta_{E\times F})\le NQ_2(E).$$

Similarly, if $d_{21}\neq d_{22}$, we obtain the inequality

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

from which (3.2) immediately follows.

Next we prove the

$$.Q_2(\eta_{E\times F})\ge \max\{N\cdot Q_2(E), N\cdot Q_2(F)\} \tag{3.4}$$

Consider the numbers $0<z_1,t_1,\ 0\le d_{11},d_{21}\le N$ for which

$$Q_2(E)=\left|\sum_{0\le x_1z_1\le t_1} e_{x_1+d_{11}+1}e_{x_1+d_{21}+1}\right|.$$

and let $z_2=1, t_2=N-1$ Define the sets

$$I_1=\{x_1z_1:\ 0\le x_1z_1\le t_1\}\qquad\text{and}\qquad I_2=\{x_2z_2:\ 0\le x_2z_2\le t_2\}=\{0,1,2,\dots,N-1\}$$

and $B=I_1\times I_2$. Moreover, let $d_{12}=0$, $d_{22}=0$, and define $\mathbf{d_1}$ and $\mathbf{d_2}$ by $\mathbf{d_1}=(d_{11},d_{12})=(d_{11},0)$ and $\mathbf{d_2}=(d_{21},d_{22})=(d_{21}.0)$. Then

$$\begin{aligned}
Q_2(\eta_{E\times F}) &\ge \left|\sum_{\mathbf{x}\in B}\eta(\mathbf{x}+\mathbf{d_1})\eta(\mathbf{x}+\mathbf{d_2})\right| =\\
&=\left|\sum_{\substack{0\le x_1z_1\le t_1\\ 0\le x_2z_2\le t_2}} e_{x_1z_1+d_{11}+1}f_{x_2z_2+d_{12}+1}\cdot e_{x_1z_1+d_{21}+1}f_{x_2z_2+d_{22}+1}\right|\\
&=N\left|\sum_{0\le x_1z_1\le t_1} e_{x_1z_1+d_{11}+1}\cdot e_{x_1z_1+d_{21}+1}\right|\\
&=NQ_2(E).
\end{aligned}$$

It can be proven similarly that

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

which completes the proof of (3.4) and the theorem. □

Proof of Theorem 3. Consider the vectors $\mathbf{d}_1,\mathbf{d}_2,\dots,\mathbf{d}_{2\ell}$ are the vertices of the following plane figure.

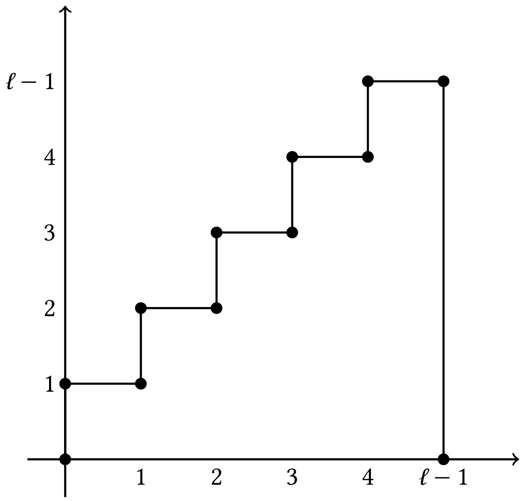


Figure 1. Step function algorithm for coordinates selection

Written out with a formula, the vectors $\mathbf{d_j}$'s are

$$\begin{array}{ll} (i, i+1) & \text{if } i = 0, 1, \dots, \ell - 2 \\ (i, i) & \text{if } i = 0, 1, \dots, \ell - 1 \\ (\ell - 1, 0), & \end{array}$$

so $\mathbf{d_1} = (0,0)$, $\mathbf{d_2} = (0,1)$, $\mathbf{d_3} = (1,1)$, … , $\mathbf{d}_{2\ell} = (0, \ell - 1)$. Then,

$$\begin{aligned} Q_{2\ell}(\eta_{E\times F}) &\geq \left| \sum_{\mathbf{x}\in I^2_{N-\ell+1}} \eta(\mathbf{x} + \mathbf{d_1})\eta(\mathbf{x} + \mathbf{d_2}) \dots \eta(\mathbf{x} + \mathbf{d}_{2\ell}) \right| \\ &= \left| \sum_{x_1=0}^{N-\ell} \sum_{x_2=0}^{N-\ell} \eta(x_1, x_2)\eta(x_1, x_2 + 1) \dots \eta(x_1, x_2 + \ell - 1) \right| \\ &= \left| \sum_{x_1=0}^{N-\ell} \sum_{x_2=0}^{N-\ell} e_{x_1+1} f_{x_2+1} e_{x_1+1} f_{x_2+2} e_{x_1+2} f_{x_2+2} \dots e_{x_1+\ell} f_{x_2+1} \right| \\ &= \left| \sum_{x_1=0}^{N-\ell} e^2_{x_1+1} \cdot e^2_{x_1+2} \dots e^2_{x_1+\ell} \right| \cdot \left| \sum_{x_2=0}^{N-\ell} f^2_{x_2+1} f^2_{x_2+2} \dots f^2_{x_2+\ell} \right| \\ &= \left| \sum_{x_1=0}^{N-\ell} \sum_{x_2=0}^{N-\ell} 1 \right| = (N - \ell + 1)^2 \end{aligned}$$ □

## 4. 3-DIMENSION LATTICES

Nowadays, 3-dimensional lattices are coming to the forefront more and more. In this case, the following three theorems can be proven similarly to the preceding ones. Let $E = (e_1, e_2, \dots, e_N)$, $F = (f_1, f_2, \dots, f_N)$ and $G = (g_1, g_2, \dots, g_N) \in \{-1, +1\}^N$ be three pseudorandom binary sequences with strong pseudorandom properties. Then, we define the binary lattice $\eta = \eta_{E\times F\times G} : I_N^3 \to \{-1, +1\}$ by

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

Then similarly to Theorems 1–3, the following holds.

**THEOREM 4.** *Let $E, F, G \in \{-1, +1\}^N$ be pseudorandom binary sequences. Then,*

$$Q_{2\ell+1}(\eta_{E\times F\times G}) \le \max\{Q_1(E), Q_3(E), \dots, Q_{2\ell+1}(E)\} \max\{Q_1(F), Q_3(F), \dots, Q_{2\ell+1}(F)\} \cdot \max\{Q_1(G), Q_3(G), \dots, Q_{2\ell+1}(G)\}$$

*and*

$$Q_{2\ell+1}(\eta_{E\times F\times G}) \ge Q_{2\ell+1}(E) Q_{2\ell+1}(F) Q_{2\ell+1}(G).$$

**THEOREM 5.** *Let $E$, $F$, $G \in \{-1, +1\}^N$ be pseudorandom binary sequences. Then,*

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

**THEOREM 6.** *Let $E, F, G \in \{-1, +1\}^N$ be pseudorandom binary sequences and $\ell \ge 2$. Then,*

$$Q_{2\ell}(\eta_{E\times F\times G}) \ge (N - \ell + 1)^2.$$

We leave the detailed proof to the reader. Again, this generation method is viable for applications where it's sufficient for the measures $Q_1$, $Q_2$, and $Q_3$ to be small (e.g., in Monte Carlo methods). However, if we also need $Q_4$ to be small (e.g., for encryption), we must use a different method.

## 5. OPEN PROBLEM: 3D EXTENSION OF THE LATTICE CONSTRUCTION

We propose a three-dimensional extension of the binary lattice construction originally studied in two dimensions. Let $p$ be a prime such that $p - 1 = 3N$, and let a pseudorandom binary sequence $S \in \{-1, +1\}^{p-1}$ be partitioned into three subsequences $E, F$, and $G$ of equal length $N$. A three-dimensional lattice is then defined by $\eta(x, y, z) = e_{x+1} f_{y+1} g_{z+1}$ for $x, y, z \in \{0, 1, \dots, N-1\}$. This construction allows for the investigation of the relationship between the combined pseudorandom measures of the lattice, $Q_k(\eta)$, and the correlation measure, $C_\ell(E(\eta))$, of the sequence obtained by flattening the cube into one dimension.

Numerical experiments for small primes ($p = 31, 37, 43$) indicate that $C_2(E(\eta))$ remains close in magnitude to $Q_2(\eta)$, suggesting that the ratio between these measures may be bounded by a constant or a slowly growing function, such as $c \log N$. The fundamental open problem is to theoretically establish whether an inequality of the form $C_k(E(\eta)) \le c \cdot Q_k(\eta)$ holds in general for $k = 2$ or 3. These empirical results motivate further research into higher-order correlation measures and the potential for a formal proof of these bounds in higher-dimensional constructions.

## REFERENCES

[1] X. L. Chen. Constructions of pseudorandom binary lattices using cyclotomic classes in finite fields. *Open Math.*, 18:1606–1614, 2020.

[2] L. Goubin, C. Mauduit, and A. Sárközy. Construction of large families of pseudorandom binary sequences. *J. Number Theory*, 106(1):56–69, 2004.

[3] K. Gyarmati. On the correlation of subsequences. *Uniform Distribution Theory*, 7(2):169–195, 2012.

[4] K. Gyarmati, C. Mauduit, and A. Sárközy. Pseudorandom binary sequences and lattices. *Acta Arithmetica*, 135(2):181–197, 2008.

[5] K. Gyarmati, C. Mauduit, and A. Sárközy. On finite pseudorandom binary lattices. *Discrete Appl. Math.*, 216:589–597, 2017.

[6] K. Gyarmati, A. Pethő, and A. Sárközy. On linear recursion and pseudorandomness. *Acta Arith.*, 118(4):359–374, 2005.

[7] K. Gyarmati, A. Sárközy, and C. L. Stewart. On Legendre symbol lattices. *Uniform Distribution Theory*, 4(1):81–95, 2009.

[8] R. Hofer, L. Mérai, and A. Winterhof. Measures of pseudorandomness: Arithmetic autocorrelation and correlation measure. In *Number Theory - Diophantine problems, uniform distribution and applications. Festschrift in honour of Robert F. Tichy's 60th birthday*, pages 303–312. Springer, Cham, 2017.

[9] P. Hubert, C. Mauduit, and A. Sárközy. On pseudorandom binary lattices. *Acta Arithmetica*, 125(1):51–62, 2006.

[10] C. Mauduit, J. Rivat, and A. Sárközy. Construction of pseudorandom binary sequences using additive characters. *Monatsh. Math.*, 141:197–208, 2004.

[11] C. Mauduit and A. Sárközy. On finite pseudorandom binary sequence I: Measure of pseudorandomness, the Legendre symbole. *Acta Arithmetica*, 82(4):365–377, 1997.

[12] L. Mérai. A construction of pseudorandom binary sequences using rational functions. *Uniform Distribution Theory*, 4(1):35–49, 2009.

[13] L. Mérai. Construction of pseudorandom binary lattices using elliptic curves. *Proc. Amer. Math. Soc.*, 139(2):407–420, 2011.

[14] L. Mérai, J. Rivat, and A. Sárközy. The measures of pseudorandomness and the NIST tests. In *Number-Theoretic Methods in Cryptology, NuTMiC 2017*, volume 10737 of *Lecture Notes in Computer Science*, pages 197–216. Springer, Cham, 2018.

[15] K. Müllner. Unlocking the strength of the combined measure via correlation. submitted.

[16] Y. Qi and H. Liu. Binary sequences and lattices constructed by discrete logarithms. *AIMS Mathematics*, 7(3):4655–4671, 2022.

[17] A. Sárközy. A finite pseudorandom binary sequence. *Studia Scientiarum Mathematicarum Hungarica*, 38:377–384, 2001.