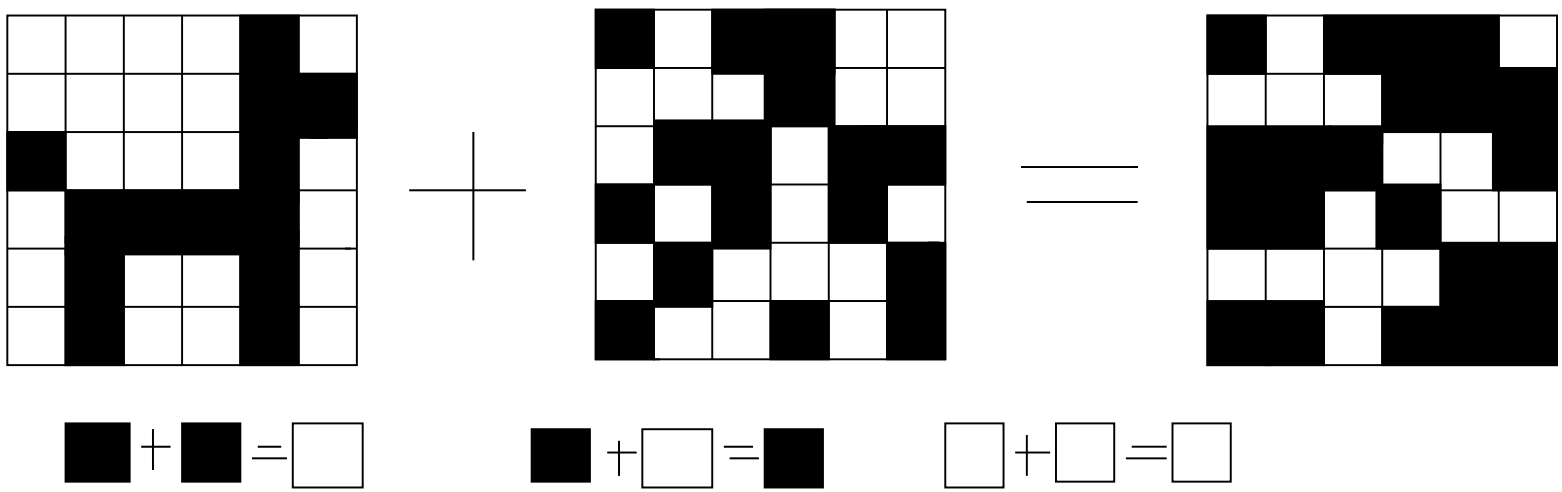
On pseudorandom binary lattices

Katalin Gyarmati

Eötvös Loránd University, Faculty of Siences,
Department of Algebra and Number Theory,
Hungary, Budapest

gykati@cs.elte.hu

In order to encrypt a 2-dimensional digital map or picture via the analog of the Vernam cipher, instead of a pseudorandom binary sequence (as a key stream) one needs a pseudorandom "binary lattice". Thus one needs the n-dimensional extension of the theory of pseudorandomness.

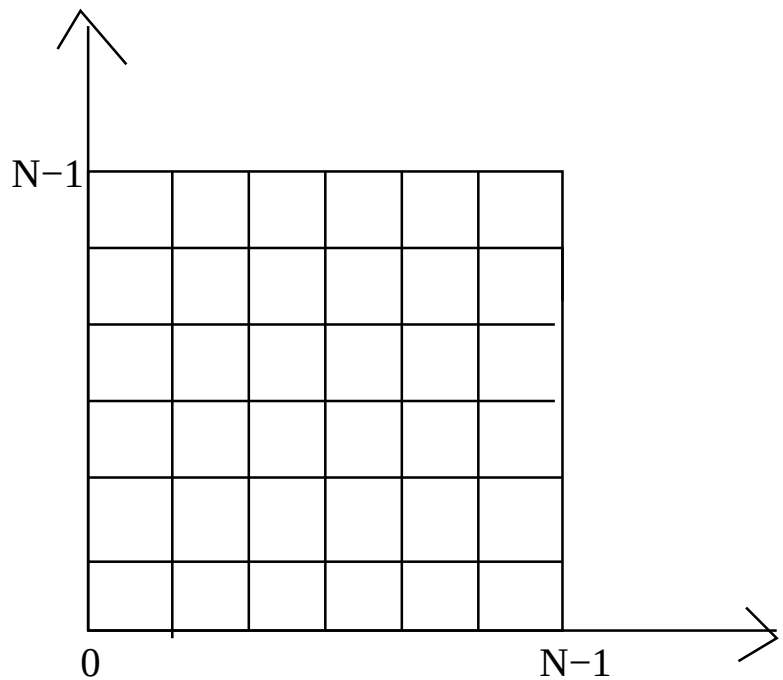


Such a theory has been developed recently by Hubert, Mauduit and Sárközy They introduced the following definitions:

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

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

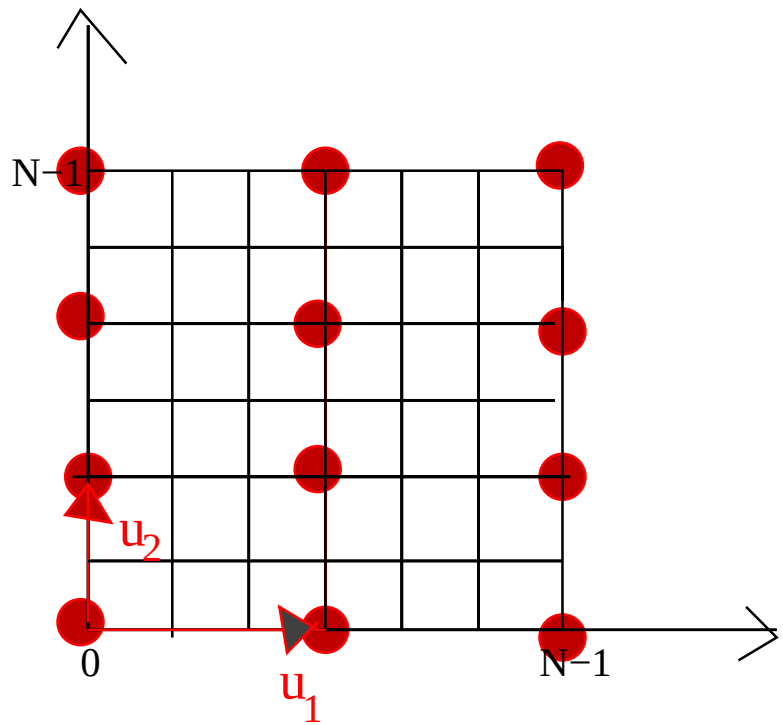
This set is called an *n-dimensional N-lattice* or briefly an *N-lattice*.



Here we will extend this definition 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 $(0, \ldots, 0, z_i, 0, \ldots, 0)$. 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

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

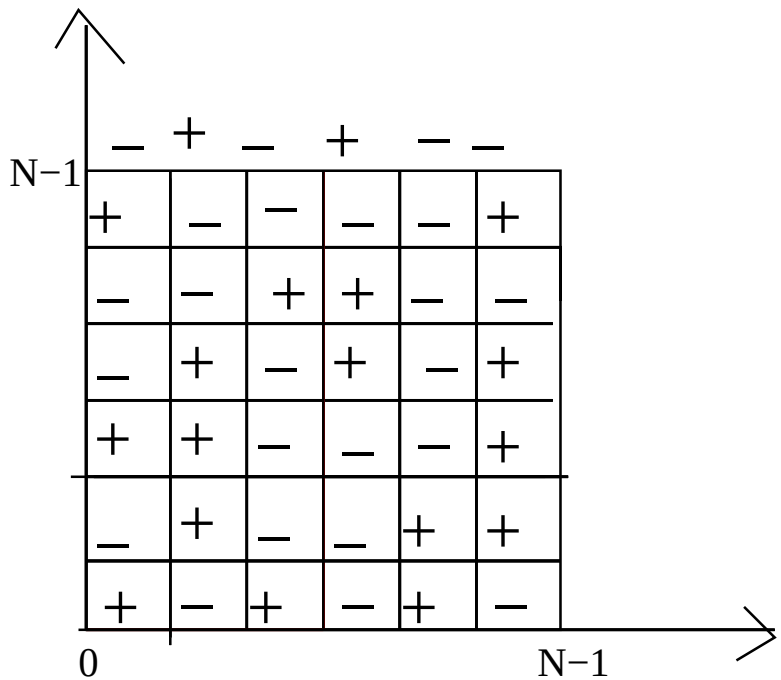
an *n-dimensional box N-lattice* or briefly a *box N-lattice*.



Hubert, Mauduit and Sárközy extended the definition of binary sequences to more dimensions by considering functions of type

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

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 can be used in encryption of digital images.



Hubert, Mauduit and Sárközy introduced the following pseudorandom measure of binary lattices (here we will present the definition in a slightly modified but equivalent form):

Definition

Let

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

The pseudorandom measure of order ℓ of η is defined by

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

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

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

This terminology is justified by the fact that Hubert Mauduit and Sárközy proved that for a truly random binary lattice defined on I_N^n and for fixed ℓ the measure $Q_\ell(\eta)$ is small: It is less than $N^{n/2}$ multiplied by a logarithmic factor.

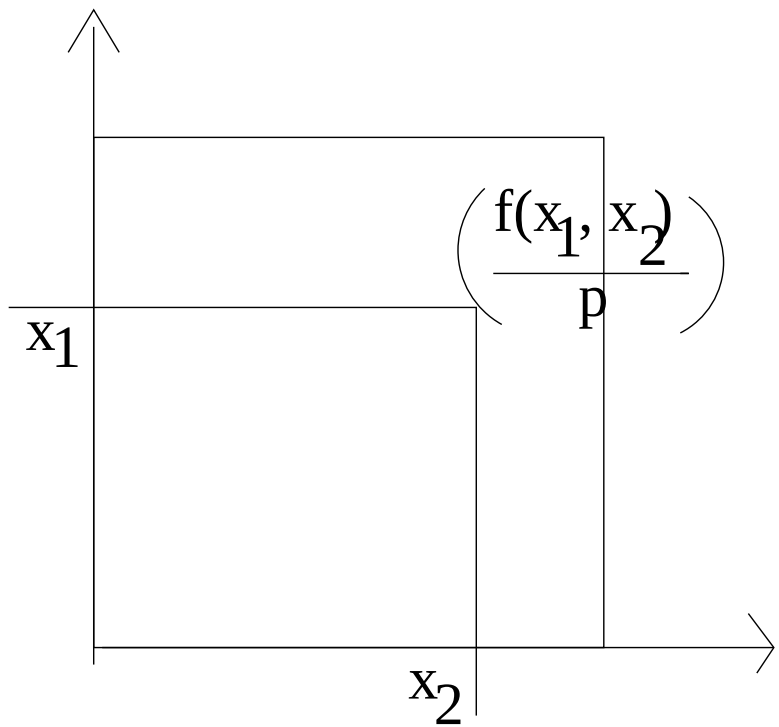
In one dimension, hence in the case of binary sequences, many good constructions have been given. Typically, the really good constructions involve $\mathbb{F}_p$, additive or multiplicative characters and polynomials, and the crucial tool in the estimation of the pseudorandom measures is Weil's theorem.

With András Sárközy and Cameron L. Stewart we decide to introduce an new construction of pseudorandom binary lattices. Our construction is much more natural and flexible than the earlier ones, and it can be implemented more easily. However, there is a price paid for this: to give upper bounds for the pseudorandom measures one needs the flexibility and generality of Weil's theorem, and here in the two dimensional situation this approach leads to weaker bounds than the optimal ones.

Construction (Sárközy, Stewart, Gy.)

Let p be an odd prime, $f(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ be a polynomial in two variables. Define $\eta : I_p^2 \to \{-1, +1\}$ by

$$\eta((x_1, x_2)) = \begin{cases} \left(\frac{f(x_1,x_2)}{p}\right) & \text{if } (f(x_1, x_2), p) = 1, \\ +1 & \text{if } p \mid f(x_1, x_2). \end{cases} \tag{1}$$



Definition

The polynomial $f(x_1, x_2)$ *is called* degenerate *if it is of the form*

$$f(x_1, x_2) = \left(\prod_{j=1}^{r} f_j(\alpha_j x_1 + \beta_j x_2) \right) g(x_1, x_2)^2, \qquad (2)$$

where $\alpha_j, \beta_j \in \mathbb{F}_p$, $f_j(x) \in \mathbb{F}_p[x]$ *for* $j = 1, \ldots, r$, *and* $g(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$.

A polynomial $f \in \mathbb{F}_p[x, y]$ which can be expressed in the form (2) is said to be degenerate and otherwise it is said to be non-degenerate.

If f is degenerate then it may be that the associated binary p-lattice (1) has weak pseudorandom properties. With Cameron L. Stewart and András Sárközy right now we are studying the situation when f is degenerate. In this talk we restrict our attention to binary p-lattices (1) for which f is non-degenerate.

Sufficient conditions

Theorem (Sárközy, Stewart, Gy.)

Let $f(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ be a polynomial of degree k which is non degenerate. Suppose that and one of the following 5 conditions holds:

a) $f(x_1, x_2)$ is irreducible in $\mathbb{F}_p[x_1, x_2]$,

b) $\ell = 2$,

c) 2 is a primitive root modulo p,

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

e) ℓ and the degree of the polynomial $f(x_1, x_2)$ in x_1 (or in x_2) are odd.

Then for the binary p-lattice η defined in (1) we have

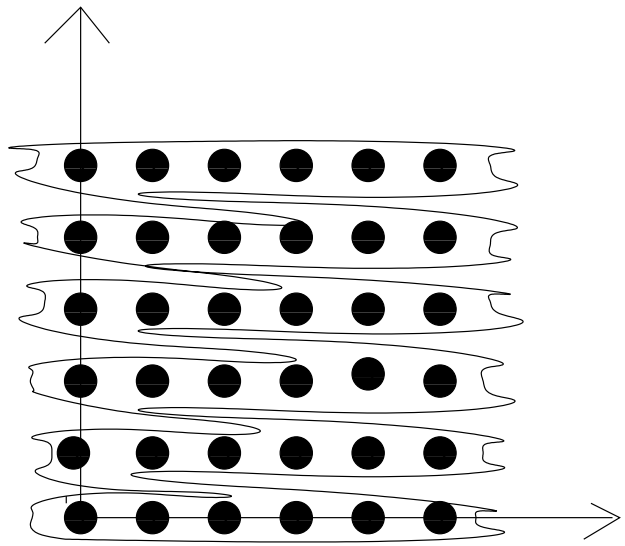
$$Q_\ell(\eta) \leq 11k\ell p^{3/2} \log p.$$

Connections between pseudorandom binary sequences and lattices

The simplest and more natural way to reduce the two dimensional case to the one dimensional one is the following:
With Mauduit and Sárközy we assigned to any 2-dimensional binary N-lattice

$$\eta(\underline{x}): \ I_N^2 \to \{-1, +1\} \tag{3}$$

a unique binary sequence
$E_{N^2} = E_{N^2}(\eta) = (e_1, e_2, \ldots, e_{N^2}) \in \{-1, +1\}^N$ by taking the first (from the bottom) row of the lattice (3) then we continue the binary sequence by taking the second row of the lattice, then the third row follows, etc.



It is a natural question to ask: is it true that if $E_{N^2}(\eta)$ is a "good" PR binary *sequence* then η is a "good" PR 2-dimensional lattice? Namely, then "good" PR binary *sequences* would generate "good" PR-binary lattices automatically?

The answer for this question is negative, with Mauduit and Sárközy we gave counterexamples for this.

Further pseudorandom measures of binary lattices

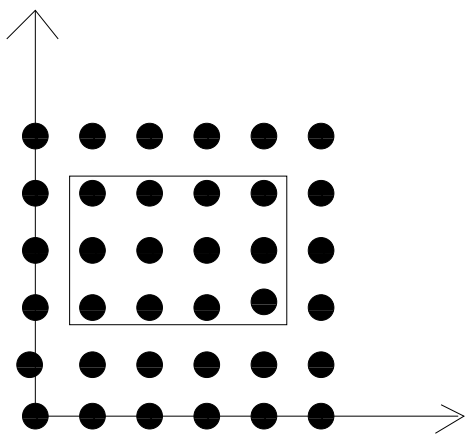
In certain cases the measure $Q_k(\eta)$ is not enough to study pseudorandom properties. Next we study symmetry properties of binary lattices.

It is a natural idea to study the symmetry only on rectangles whose sides are vertical or horizontal. We will call these rectangles parallel rectangles.

Definition (Mauduit, Sárközy, Gy.)

$R \subseteq I_N^2$ *is a* parallel rectangle *if* R *is of the form*

$$R = \{\mathbf{x} = (x_1, x_2) : \ x_1, x_2 \in \mathbb{N}_0, \ a_1 \leq x_1 \leq b_1, \ a_2 \leq x_2 \leq b_2\}$$



Clearly a parallel rectangle R of the form (4) has two symmetry axis: the lines $x_1 = \frac{a_1+b_1}{2}$ and $x_2 = \frac{a_2+b_2}{2}$. The rectangle R also has a symmetry center $\left(\frac{a_1+b_1}{2}, \frac{a_2+b_2}{2}\right)$. Let $H(R)$ denote the set of symmetry transformations which leave R in its original position, so

$$\tau((x_1, x_2)) = (a_1 + b_1 - x_1, x_2) \text{ for all } (x_1, x_2) \in I_N^2,$$
$$\tau((x_1, x_2)) = (x_1, a_2 + b_2 - x_2) \text{ for all } (x_1, x_2) \in I_N^2,$$
$$\tau((x_1, x_2)) = (a_1 + b_1 - x_1, a_2 + b_2 - x_2) \text{ for all } (x_1, x_2) \in I_N^2.$$

We define the rectangle-symmetry measure by the following:

Definition (Mauduit, Sárközy, Gy.)

Let $\eta : I_N^2 \to \{-1, +1\}$ be a binary lattice. The rectangle-symmetry measure of η *is defined by*

$$S_r(\eta) = \max_{R, \tau \in H(R)} \left| \sum_{\mathbf{x} \in R} \eta(\mathbf{x}) \eta(\tau(\mathbf{x})) \right|$$

where the maximum is taken over all parallel rectangles R of I_N^2 and all symmetry transformation $\tau \in H(R)$.

With Mauduit and Sárközy we also studied two further symmetry measures. We gave constructions of binary lattices with strong symmetry properties.

The convex measure

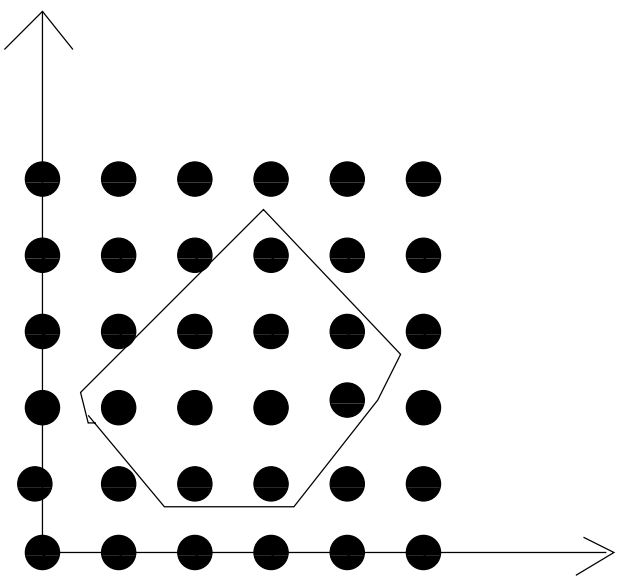
The shape of the box-lattices B in the definition $Q_\ell(\eta)$ is very restricted. Clearly, one need an assumption of the shape of the sets B, but it should not be too specific. In the following definition we will take the maximum over convex polytopes, which is a natural candidate for defining a new measure.

Definition (Gy.)

Let $\eta : I_N^n \to \{-1, +1\}$ *be a binary lattice. The* convex measure of order ℓ *of* η *is defined by*

$$X_\ell(\eta) = \max_{K, \mathbf{d_1}, \ldots, \mathbf{d}_\ell} \left| \sum_{\mathbf{x} \in K \cap I_N^n} \eta(\mathbf{x} + \mathbf{d_1}) \ldots \eta(\mathbf{x} + \mathbf{d}_\ell) \right|, \qquad (4)$$

where the maximum is taken over all distinct $\mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d}_\ell \in I_N^n$ *and all convex polytopes* $K \subseteq \mathbb{R}^n$ *such that* $K + \mathbf{d_1}, \ldots, K + \mathbf{d}_\ell \subseteq I_N^n$



We think that the convex measure $X_\ell(\eta)$ and the pseudorandom measure $Q_\ell(\eta)$ are independent of each other. However it seems very difficult to prove this, we do not go here to the details.

The line-measure

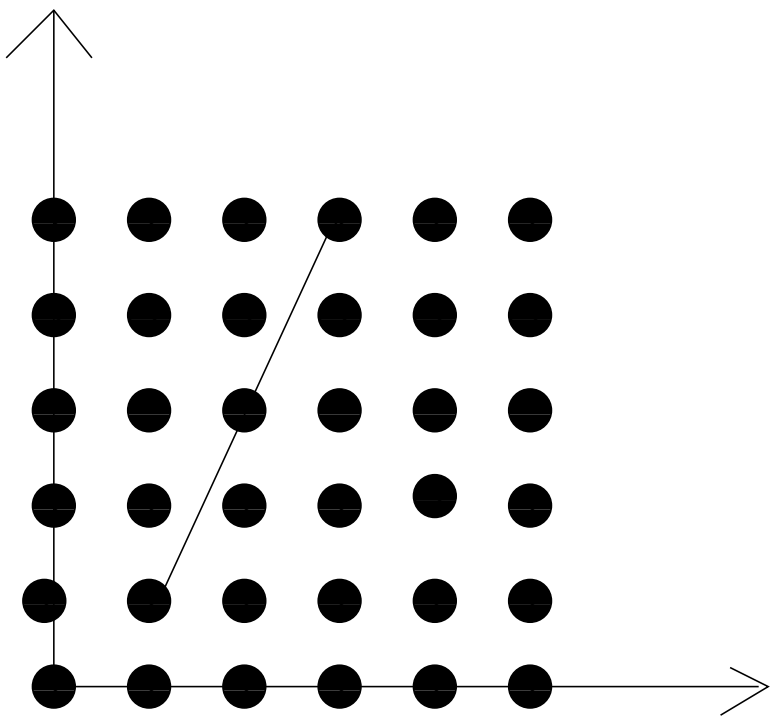
Both the convex measure and pseudorandom measure can be estimated by the line measure defined below. In order to introduce this new measure we need the following definition

Definition (Gy.)

$L \subseteq I_N^n$ is a segment *if L is of the form*

$$L = \{\mathbf{x} = (x_1, \ldots, x_n) : x_1 = a_1 t + b_1, \ldots, x_n = a_n t + b_n, \\ t \in \{0, 1, \ldots, M-1\}\}$$

(with $M \leq N$) where $a_i, b_i \in \mathbb{Z}$ for $i = 1, 2, \ldots, n$ and $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$.



Definition

Let $I_N^n \to \{-1, +1\}$ be a binary lattice. The line-measure of order ℓ of η is defined by

$$L_\ell(\eta) = \max_{L, \mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d}_\ell} |V(\eta, L, D)|$$

$$= \max_{L, \mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d}_\ell} \left| \sum_{\mathbf{x} \in \mathbf{L}} \eta(\mathbf{x} + \mathbf{d_1}) \ldots \eta(\mathbf{x} + \mathbf{d}_\ell) \right|$$

where the maximum is taken over all distinct $\mathbf{d_1}, \ldots, \mathbf{d}_\ell$ and all segments L such that $L + \mathbf{d_1}, \ldots, L + \mathbf{d}_\ell \subseteq I_N^n$.

The line measure is the most demanding of the previously defined measures, indeed we will prove:

Theorem

For every binary lattice η : $I_N^n \to \{-1, +1\}$ we have

$$X_\ell(\eta) \leq N^{n-1} L_\ell(\eta).$$

Theorem

For every binary lattice $\eta : I_N^n \to \{-1, +1\}$ *we have*

$$Q_\ell(\eta) \leq N^{n-1} L_\ell(\eta).$$

Finally, I proved that

Theorem

For every odd prime p *and* $\ell \in \mathbb{N}$*, there is a binary lattice* $\eta : I_p^2 \to \{-1, +1\}$ *we have*

$$L_\ell(\eta) \ll \ell^5 p^{1/2} \log p.$$