On the cross-combined measure of families of binary lattices and sequences

Katalin Gyarmati

ELTE Eötvös Loránd University, Institute of Mathematics, Department of Algebra and Number Theory and
MTA–ELTE Geometric and Algebraic Combinatorics Research Group,
H-1117 Budapest, Pázmány Péter Sétány 1/C, Hungary,
gykati@cs.elte.hu

Abstract. The cross-combined measure (which is a natural extension of cross-correlation measure) is introduced and important constructions of large families of binary lattices with optimal or nearly optimal cross-combined measures are presented. These results are also strongly related to the one-dimensional case: An easy method is showed obtaining strong constructions of families of binary sequences with nearly optimal cross-correlation measures based on the previous constructions of families of lattices. The important feature of this result is that so far there exists only one type of constructions of *very large* families of binary sequences with small cross-correlation measure, and this only type of constructions was based on one-variable irreducible polynomials. Since it is very complicated to construct one-variable irreducible polynomials over $\mathbb{F}_p$, it became necessary to show other types of constructions where the generation of sequences is much faster. Using binary lattices based on two-variable irreducible polynomials this problem can be avoided. (Since, contrary to one-variable polynomials, using Schöneman-Eisenstein criteria it is possible to generate two-variable irreducible polynomials over $\mathbb{F}_p$ fast.)

1 Introduction

Pseudorandom binary sequences and lattices have many applications in cryptography, they play a crucial role in modern cryptography. One of the main applications is the famous Vernam-cipher encrypting algorithm, where pseudorandom binary sequences are used as key-streams. If in place of a text we would like to encrypt an image by Vernam cipher, then the key-stream should be a pseudorandom binary lattice in place of a binary sequence. In the present paper I will study large families of binary sequences and lattices and I will extend an important family measure, the cross-correlation measure from families of binary sequences to family of binary lattices.

[0] 2010 Mathematics Subject Classification: Primary: 11K45.
Keywords and phrases: pseudorandom, cross-combined, cross-correlation, binary lattices, binary sequences.
Research partially supported by Hungarian National Research Development and Innovation Funds NK 104183 and K 119528.

1.1 Large families of pseudorandom binary sequences

The constructive and quantitative study of pseudorandomness started by the work of Mauduit and Sárközy [30]. They introduced the following pseudorandom measures in order to study the pseudorandom properties of *finite* binary sequences:

Definition 1.1 *For a binary sequence $E_N = (e_1, \dots, e_N) \in \{-1, +1\}^N$ of length 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 $1 \le a \le a + tb \le N$.

In order to study certain connections of between different elements of the sequence Mauduit and Sárközy [30] introduced the correlation measure:

Definition 1.2 *For a binary sequence $E_N = (e_1, \dots, e_N) \in \{-1, +1\}^N$ of length N, and for $D = (d_1, \dots, d_\ell)$ with non-negative integers $0 \le d_1 < \dots < d_\ell$, write $V(E_N, M, D) = \sum_{n=1}^{M} e_{n+d_1} \dots e_{n+d_\ell}$. Then the correlation measure of order ℓ of E_N is defined as*

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

where the maximum is taken over all $D = (d_1, \dots, d_\ell)$ and M such that $0 \le d_1 < \dots < d_\ell < M + d_\ell \le N$.

In [7] Cassaigne, Ferenczi, Mauduit, Rivat and Sárközy formulated the following principle: “The sequence E_N is considered a “good” pseudorandom sequence if these measures $W(E_N)$ and $C_\ell(E_N)$ (at least for “small” ℓ) are “small”.” This principle was justified by Cassaigne, Mauduit and Sárközy [8] they proved that for the majority of the sequences $E_N \in \{-1, +1\}^N$ the measures $W(E_N)$ and $C_\ell(E_N)$ are around $N^{1/2}$ (up to some logarithmic factors). Later Alon, Kohayakawa, Mauduit, Moreira and Rödl [4] improved on these bounds.

It is also important that we will be able to present constructions for which these pseudorandom measures are small. First Mauduit and Sárközy [30] studied the following construction:

Construction 1.A *Let p be a prime number, $N = p-1$ and define the Legendre-sequence $E_N = (e_1, e_2, \dots, e_N) \in \{-1, +1\}^N$ by*

$$e_n = \left(\frac{n}{p}\right),$$

where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol.

Then by Theorem 1 in [30] for the sequence E_N defined in Construction 1.A we have $W(E_N) \ll N^{1/2} \log N$ and $C_\ell(E_N) \ll N^{1/2} \log N$.

After their first paper [30] on pseudorandomness, Mauduit and Sárközy continued it by a series of papers and later many people continued to the work started by them. Since then numerous constructions have been given by several authors.

First for fixed N the most constructions produced only a single sequence of length N, however, in many applications one needs many pseudorandom binary sequences. In 2001 Hoffstein and Liemann [27] succeeded in constructing large families of pseudorandom binary sequences based on the Legendre symbol, but they did not prove anything on its pseudorandom properties. Their construction was the following:

Construction 1.B *Let $K \in \mathbb{N}$, p be a prime number, and denote by $\mathcal{P}_{\leq K}$ the set of monic polynomials $f(x) \in \mathbb{F}_p[x]$ of degree k, where $0 < k \leq K$. For $f \in \mathcal{P}_K$ define the binary sequence $E_p(f) = (e_1, \dots, e_p)$ by*

$$e_n = \begin{cases} \left(\frac{f(n)}{p}\right) & \text{for } (f(n), p) = 1, \\ +1 & \text{for } p \mid f(n). \end{cases} \tag{1.1}$$

Let $\mathcal{F}_{\leq K,\ Legendre} = \{E_p(f) :\ f \in \mathcal{P}_{\leq K}\}$.

Clearly $\mathcal{F}_{\leq K,\ Legendre}$ is a large family of pseudorandom binary sequences. Goubin, Mauduit and Sárközy [14] proved that, under some not too restrictive conditions on the polynomials f, the sequences $E_p(f)$ have strong pseudorandom properties:

Theorem 1.A *Let p, $\mathcal{P}_K$ and $\mathcal{F}_{\leq K,\ Legendre}$ be defined as in Construction 1.B and for $f \in \mathcal{P}_K$ define $E_p = E_p(f) \in \mathcal{F}$ by (1.1). Suppose that f has no multiple root in $\overline{\mathbb{F}}_p$ and denote by k the degree of f. Then*

$$W(E_p) \leq 10kp^{1/2} \log p.$$

Moreover, assume that for $\ell \in \mathbb{N}$ one of the following assumptions holds:
(i) $\ell = 2$;
(ii) $\ell < p$ *and 2 is a primitive root modulo* p;
(iii) $(4k)^\ell < p$.
Then we also have

$$C_\ell(E_p) \leq 10k\ell p^{1/2} \log p.$$

We remark that several important a posteriori tests (indicated by the 1.4-sts. package of the National Institute of Standards and Technology) were checked by Rivat and Sárközy [39] by computer for many sequences generated by Construction 1.B. In each cases they obtained that the sequence passes all these tests. This work was continued by Mérai, Rivat and Sárközy [37]. After the construction in Theorem 1.A many other constructions of large families of pseudorandom sequences have been given by several authors.

Although many constructions exist, Construction 1.B is one of the best: we have optimally good bounds for the pseudorandom measures and the elements of the sequences can be generated fast. In these constructions it is guaranteed that the individual sequences belonging to the family possess strong pseudorandom properties. However, in many applications it is not enough to know this; it can be much more important to know that the given family has a "rich", "complex" structure, there are many "independent" sequences in it. In order to handle this requirement Ahlswede, Khachatrian, Mauduit and Sárközy [1] (see also [2], [3], [16], [33]) introduced the notion of *family complexity* or briefly *f-complexity* (which can be especially useful in cryptography):

Definition 1.3 *The f-complexity $\Gamma(\mathcal{F})$ of a family $\mathcal{F}$ of binary sequences $E_N \in \{-1,+1\}^N$ is defined as the greatest integer j so that for any* specification

$$e_{i_1} = \varepsilon_1, \ \ldots, \ e_{i_j} = \varepsilon_j \ (1 \leq i_1 < \cdots < i_j \leq N)$$

(with $\varepsilon_1, \ldots, \varepsilon_j \in \{-1,+1\}$) there is at least one $E_N = (e_1, \ldots, e_N) \in \mathcal{F}$ which satisfies it. The f-complexity of $\mathcal{F}$ is denoted by $\Gamma(\mathcal{F})$. (If there is no $j \in \mathbb{N}$ with the property above then we set $\Gamma(\mathcal{F}) = 0$.)

Later other properties of large families were studied and other family measures were introduced, see e.g. *collision free* ([6], [34], [40], [41]), *avalanche effect* or a variant of Hamming-distance called our case as *distance-minimum* ([6], [11], [29], [40], [41]). These measures have multi-dimensional analogues (see the papers [19] and [20]) and in Section 1.2 these multi-dimensional versions of family measures will be presented.

In Section 3 of this paper I will introduce and focus on a new very general measure, the *cross-combined measure*. This new measure will be a natural extension of the one-dimensional cross-correlation measure defined by Mauduit, Sárközy and I in [21]:

Definition 1.4 *Let $N \in \mathbb{N}$, $\ell \in \mathbb{N}$, and for any ℓ binary sequences $E_N^{(1)}, \dots, E_N^{(\ell)}$ with*

$$E_N^{(i)} = \left(e_1^{(i)}, \dots, e_N^{(i)}\right) \in \{-1, +1\}^N \text{ (for } i = 1, 2, \dots, \ell)$$

and any $M \in \mathbb{N}$ and ℓ-tuple $D = (d_1, \dots, d_\ell)$ of non-negative integers with $0 \le d_1 \le \dots \le d_\ell < M + d_\ell \le N$, write

$$V_\ell\left(E_N^{(1)}, \dots, E_N^{(\ell)}, M, D\right) = \sum_{n=1}^{M} e_{n+d_1}^{(1)} \cdots e_{n+d_\ell}^{(\ell)}$$

Let

$$\widetilde{C}_\ell\left(E_N^{(1)}, \dots, E_N^{(\ell)}\right) = \max_{M,D} \left| V_\ell\left(E_N^{(1)}, \dots, E_N^{(\ell)}, M, D\right) \right|$$

where the maximum is taken over all $D = (d_1, \dots, d_\ell)$ and $M \in \mathbb{N}$ satisfying $0 \le d_1 \le \dots \le d_\ell < M + d_\ell \le N$ with the additional restriction that if $E_N^{(i)} = E_N^{(j)}$ for some $i \ne j$, then we must not have $d_i = d_j$. Then the cross-correlation measure of order ℓ *of the family $\mathcal{F}$ of binary sequences $E_N \in \{-1, +1\}^N$ is defined as*

$$\Phi_\ell(\mathcal{F}) = \max \widetilde{C}_\ell\left(E_N^{(1)}, \dots, E_N^{(\ell)}\right)$$

where the maximum is taken over all ℓ-tuples of binary sequences $\left(E_N^{(1)}, \dots, E_N^{(\ell)}\right)$ with $E_N^{(i)} \in \mathcal{F}$ for $i = 1, \dots, \ell$.

(Note that other cross-correlation type quantities also occur in [5], [13], [15].)

In [21] jointly with Mauduit and Sárközy we also studied main properties and connections of cross-correlation measure to other family measures. Later Mérai studied the average behaviour of the cross-correlation measure. Among others he proved that usually the cross-correlation measure Φ_ℓ of a family of binary lattices $\eta : I_N^n \to \{-1, +1\}$ is between two constant factors of $N^{1/2}(\log N)^{1/2}$. For more details see [35] and [36].

The goal of the present paper is to extend this measure to the multi-dimensional case. The multi-dimensional cross-combined measure will have all advantages then the one-dimensional cross-correlation measure.

1.2 Large families of binary lattices

Before introducing the definition of the multi-dimensional cross-combined measure we will need to present the standard terminology the multi-dimensional theory of pseudorandomness. This will follow in the next section. In [28] Hubert, Mauduit and Sárközy extended this theory of pseudorandomness to n dimensions.

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

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

This set is called an *n-dimensional N-lattice* or briefly an *N-lattice.* In [25] this definition was extended to more general lattices in the following way: Let $\mathbf{u_1}, \mathbf{u_2}, \dots, \mathbf{u_n}$ be n linearly independent n-dimensional vectors over the field of the real numbers such that the i-th coordinate of $\mathbf{u_i}$ is a positive integer and the other coordinates of $\mathbf{u_i}$ are 0, so that $\mathbf{u_i}$ is of the form $(0, \dots, 0, z_i, 0, \dots, 0)$ (with $z_i \in \mathbb{N}$). Let $t_1, t_2, \dots, t_n$ be integers with $0 \le t_1, t_2, \dots, t_n < N$. Then we call the set

$$\begin{aligned} B_N^n = \{\mathbf{x} = x_1\mathbf{u_1} + \dots + x_n\mathbf{u_n} :, \, x_i \in \mathbb{N} \cup \{0\}, \ 0 \le x_i \left|\mathbf{u_i}\right| \le t_i (< N) \\ \text{for } i = 1, \dots, n\} \end{aligned} \tag{1.2}$$

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

In [28] the definition of binary sequences was extended to more dimensions by considering functions of type

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

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

In [28] Hubert, Mauduit and Sárközy introduced the following measures of pseudorandomness of binary lattices (here we will present the definition in the same slightly modified but equivalent form as in [25]):

Definition 1.5 *Let $\eta : I_N^n \to \{-1, +1\}$ be a binary lattice. Define the combined pseudorandom measure of order ℓ of η by*

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

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

Note that in the one-dimensional special case $Q_1(\eta)$ is the well-distribution measure W.

Then η is said to have strong pseudorandom properties, or briefly, it is considered as a "good" pseudorandom binary lattice at least for small ℓ's and "large" N the measures $Q_\ell(\eta)$'s are "small" (much smaller, than the trivial upper bound N^n). This terminology is justified by the fact that, as it was proved in [28], for a truly random binary lattice defined on I_N^n and for fixed ℓ the measure $Q_\ell(\eta)$ is "small", more precisely, it is less than $N^{n/2}$ multiplied by a logarithmic factor. As in the one-dimensional case, many papers have been written on pseudorandomness of binary lattices, for further references see e.g. [22], [23] and [24].

In the application (similarly to the one-dimensional case) it is important that a large family $\mathcal{G}$ of binary lattices has a "rich", "complex" structure, there are many "independent" sequences, resp. lattices in it which are "far apart". Thus one needs quantitative measures for these properties of families of binary lattices. In case of binary sequences some of these measures were mentioned in Section 1.1.

Next few definitions of family measures of binary lattices introduced by Mauduit, Sárközy and I in [21] follow:

Definition 1.6 *If* $\mathcal{G}$ *is a family of binary lattices* η *is of the form*

$$\mathcal{G} = \mathcal{G}(\mathcal{S}) = \{\eta_s : \ s \in \mathcal{S}\}, \tag{1.3}$$

and for any $s \in \mathcal{S}$ *changing any element of* s *changes "many" elements of* $\eta_s : \ I_N^n \to \{-1, +1\}$*, then we speak about* avalanche effect*, and we say that* $\mathcal{F} = \mathcal{F}(\mathcal{S})$ *possesses the* avalanche property*. If for any* $s \in \mathcal{S}$*,* $s' \in \mathcal{S}$*,* $s \neq s'$ *at least* $\left(\frac{1}{2} - o(1)\right) N^n$ *elements of* η_s *and* $\eta_{s'}$ *are different, then* $\mathcal{F}$ *is said to possess the* strict avalanche property*.*

Definition 1.7 *If* $N \in \mathbb{N}$*,* $n \in \mathbb{N}$*,* $\eta : \ I_N^n \to \{-1, +1\}$ *and* $\eta' : \ I_N^n \to \{-1, +1\}$*, then the distance* $d(\eta, \eta')$ *between* η *and* η' *is defined by*

$$\begin{aligned} d(\eta, \eta') = |\{(x_1, x_2, \dots, x_n) : (x_1, \dots, x_n) \in \mathbb{I}_N^n, \\ \eta(x_1, \dots, x_n) \neq \eta'(x_1, \dots, x_n)\}|. \end{aligned}$$

If $\mathcal{G}$ is a family of binary lattices, then the distance minimum *$m(\mathcal{G})$ is defined by*

$$m(\mathcal{G}) = \min_{\substack{\eta,\eta'\in\mathcal{G}\\ \eta\neq\eta'}} d(\eta,\eta').$$

So that $\mathcal{G}$ is collision free if $m(\mathcal{G})>0$, and it possesses the strict avalanche property if

$$m(\mathcal{G}) \geq \left(\frac{1}{2}-o(1)\right)N^n. \tag{1.4}$$

2 The definition of cross-combined measure and its connection with other family measures

In this section I extend the cross-correlation measure to the multi-dimensional case. This new measure will be called as cross-combined measure:

Definition 2.1 *Let $N\in\mathbb{N}$, $\ell\in\mathbb{N}$, and for any ℓ binary sequences $\eta_1,\dots,\eta_\ell$ with*

$$\eta_i:\ I_N^n \to \{-1,+1\} \quad (i=1,2,\dots,\ell)$$

and for any B box-lattice of the form (1.2) and ℓ-tuple $D=(\mathbf{d}_1,\dots,\mathbf{d}_\ell)$ with $\mathbf{d}_i\in I_N^n$ $(i=1,2,\dots,\ell)$ write

$$V_\ell\left(\eta_1,\dots,\eta_\ell,B,D\right) = \sum_{\mathbf{x}\in B}\eta_1(\mathbf{x}+\mathbf{d}_1)\cdots\eta_\ell(\mathbf{x}+\mathbf{d}_\ell) \tag{2.1}$$

Let

$$\widetilde{Q}_\ell\left(\eta_1,\dots,\eta_\ell\right) = \max_{B,D}\left|V_\ell\left(\eta_1,\dots,\eta_\ell,B,D\right)\right| \tag{2.2}$$

where the maximum is taken over all $D=(\mathbf{d}_1,\dots,\mathbf{d}_\ell)$ and B box-lattice satisfying $B+\mathbf{d}_1, B+\mathbf{d}_2,\dots,B+\mathbf{d}_\ell\subseteq I_N^n$ with the additional restriction that if $\eta_i=\eta_j$ for some $i\neq j$, then we must not have $\mathbf{d}_i=\mathbf{d}_j$. Then the cross-combined measure of order ℓ *of the family $\mathcal{G}$ of binary lattices $\eta\in\{-1,+1\}^N$ is defined as*

$$\mathit{\Phi}_\ell(\mathcal{G}) = \max\widetilde{Q}_\ell\left(\eta_1,\dots,\eta_\ell\right) \tag{2.3}$$

where the maximum is taken over all ℓ-tuples of binary lattices $(\eta_1,\dots,\eta_\ell)$ with

$$\eta_i\in\mathcal{G} \text{ for } i=1,\dots,\ell.$$

By the definition of $\tilde{Q}_\ell$, we have $\tilde{Q}_\ell(\eta,\dots,\eta)=Q_\ell(\eta)$, thus it follows from (2.3) that

Proposition 2.1 *We have*

$$\Phi_\ell(\mathcal{G})\geq\max_{\eta\in\mathcal{G}}Q_\ell(\eta).$$

This means that if we have a "good" upper bound for $\Phi_\ell(\mathcal{G})$, then this guarantees that *all lattices in $\mathcal{G}$ possesses strong pseudorandom properties.*

Next in this section I will study the connection of cross-combined measure with other family measures. As an a multi-dimensional analog of Proposition 2.2 in [21] now we obtain:

Proposition 2.2 *If $N,n\in\mathbb{N}$ and $\mathcal{G}$ is a large family of binary lattices $\eta:\ I_N^n\to\{-1,+1\}$ then for $\eta_1,\eta_2\in\mathcal{G}$ we have*

$$\left|d(\eta_1,\eta_2)-\frac{N^n}{2}\right|\leq\frac{1}{2}\tilde{Q}_2(\eta_1,\eta_2)\leq\frac{1}{2}\Phi_2(\mathcal{G}).\tag{2.4}$$

Proof. Clearly we have

$$d(\eta_1,\eta_2)=\sum_{\mathbf{x}\in I_N^n}\frac{(\eta_1(\mathbf{x})-\eta_2(\mathbf{x}))^2}{4}=\frac{N^n}{2}-\frac{1}{2}\sum_{\mathbf{x}\in I_N^n}\eta_1(\mathbf{x})\eta_2(\mathbf{x})$$

whence, by (2.1), (2.2) and (2.3),

$$\left|d(\eta_1,\eta_2)-\frac{N^n}{2}\right|=\frac{1}{2}\left|\sum_{\mathbf{x}\in I_N^n}\eta_1(\mathbf{x})\eta_2(\mathbf{x})\right|\leq\frac{1}{2}\tilde{Q}_2(\eta_1,\eta_2)\leq\Phi_2(\mathcal{G})$$

which proves (2.4).

If the cross-combined measure of order 2 of a family $\mathcal{G}$ of n-dimensional binary lattices is $o(N^n)$ then it follows from Definition 1.7 and (2.4) that

$$m(\mathcal{G})=\min_{\substack{\eta,\eta'\in\mathcal{F}\\ \eta\neq\eta'}}d(\eta_1,\eta_2)\geq\frac{N^n}{2}-\frac{1}{2}\Phi_2(\mathcal{G})=\frac{N^n}{2}-o(N^n)$$

so that (1.4) holds. This proves

Proposition 2.3 *If $N,n\in\mathbb{N}$, $\mathcal{G}$ is a large family of binary lattices $\eta:\ I_N^n\to\{-1,+1\}$ and $\Phi_2(\mathcal{G})=o(N^n)$ then the family $\mathcal{G}$ possesses the strict avalanche property.*

3 Cross-combined measure of a family of binary lattices constructed by using quadratic characters

Mauduit and Sárközy [31] constructed a large family of binary lattices with strong pseudorandom properties by using quadratic characters of finite fields (this construction generalizes the one dimensional constructions in [14] and [30]). They proved the following theorem:

Theorem 3.A *Assume that $q = p^n$ is the power of an odd prime, $f(x) \in \mathbb{F}_q[x]$ has degree k with*

$$0 < k < p.$$

Denote the quadratic character of $\mathbb{F}_q$ by γ (setting also $\gamma(0) = 0$). Consider the linear vector space formed by the elements of $\mathbb{F}_q$ over $\mathbb{F}_p$, and let $v_1, \dots, v_n$ be a basis of this vector space (i.e., assume that $v_1, v_2, \dots, v_n$ are linearly independent over $\mathbb{F}_p$). Define the n dimensional binary p-lattice $\eta : \ I_p^n \to \{-1, +1\}$ by

$$\eta(\mathbf{x}) = \eta((x_1, \dots, x_n)) = \begin{cases} \gamma(f(x_1v_1 + \cdots + x_nv_n)) \text{ for} \\ \qquad\qquad\qquad f(x_1v_1 + \cdots + x_nv_n) \neq 0 \\ +1 \text{ for } f(x_1v_1 + \cdots + x_nv_n) = 0. \end{cases} \tag{3.1}$$

Assume that and $f(x)$ has no multiple zero in $\overline{\mathbb{F}}_q$, $\ell \in \mathbb{N}$ and

$$4^{n(k+\ell)} < p.$$

Then we have

$$Q_\ell(\eta) < k\ell(q^{1/2}(1 + \log p)^n + 2).$$

Indeed this is a combination of Theorems 1 and 2 in [32].

Throughout this section p, n and $q = p^n$ will be fixed (except Corollary 3.B). We will denote the construction of Theorem 3.A by $\mathcal{G}_{\leq K,\ quadratic}$:

Construction 3.A *Denote by $\mathcal{P}_{\leq K}$ the set of monic polynomials $f \in \mathbb{F}_q[x]$ with degree $0 < \deg f \leq K$. Let $\mathcal{G}_{\leq K,\ quadratic}$ denote the family of the binary lattices η defined by* (3.1) *assigned to polynomials $f \in \mathcal{P}_{\leq K}$.*

It is clear that all lattices $\eta \in G_{\leq K,\ quadratic}$ satisfying the conditions of Theorem 3.A possess strong pseudorandom properties.

In order to simplify the notations we will introduce a function $\tau : \mathbb{F}_p^n \to \mathbb{F}_q$. We may assume that I_p^n represents the elements of $\mathbb{F}_p^n$ and thus we may also use τ as a function $\tau :\ I_p^n \to \mathbb{F}_q$. Let $v_1, v_2, \dots, v_n$ be the basis of the vectorspace $\mathbb{F}_q$ over $\mathbb{F}_p$ defined in Theorem 3.A. (Here $q = p^n$.) For an $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}_p^n$ let

$$\tau(\mathbf{x}) = x_1v_1 + x_2v_2 + \dots x_nv_n.$$

Then τ is a bijection. We also have for $\mathbf{a}, \mathbf{b} \in \mathbb{F}_p^n$ $\tau(\mathbf{a}+\mathbf{b}) = \tau(\mathbf{a}) + \tau(\mathbf{b})$. Then (3.1) in Theorem 3.A can be written the equivalent form

$$\eta(\mathbf{x}) = \begin{cases} \gamma(f(\tau(\mathbf{x}))) & \text{for } f(\tau(\mathbf{x})) \neq 0 \\ +1 & \text{for } f(\tau(\mathbf{x})) = 0. \end{cases} \tag{3.2}$$

In [19] jointly with Mauduit and Sárközy we proved that the family measure of $\mathcal{G}_{quadratic,\leq K}$ is optimal. The distance minimum was also estimated in [19] and If $K < \frac{1}{2}q^{1/2}$, then $\mathcal{G}_{\leq K,\ quadratic}$ is collision free. Moreover if $q \to \infty$, $K = o(q^{1/2})$, then $\mathcal{G}_{\leq K,\ quadratic}$ possesses the strict avalanche property.

Unfortunately, it turned out that for $K \geq 2$, our new measure, the cross-combined measure of $\mathcal{G}_{\leq K,\ quadratic}$ is very bad:

Proposition 3.1 *For $K \geq 2$ we have $\Phi_3(G_{\leq K,\ quadratic}) \geq q-2$.*

Proof. Consider the following 3 polynomials: $f_1(x) = x,\ f_2(x) = x+1,\ f_3(x) = x(x+1) \in \mathbb{F}_q[x]$. Let η_i be the binary lattice defined by (3.1) with f_i in place of f for $i = 1, 2, 3$. Then using (3.2) we get:

$$\begin{aligned}\Phi_3(\mathcal{G}_{\leq K,\ quadratic}) &\geq \tilde{Q}_3(\eta_1, \eta_2, \eta_3) \geq V_3(\eta_1, \eta_2, \eta_3, I_p^n, (0,0,0)) = \sum_{\mathbf{x}\in I_p^n} \eta_1(\mathbf{x})\eta_2(\mathbf{x})\eta_3(\mathbf{x}) \\ &= \sum_{\substack{\tau(\mathbf{x})\in I_p^n \\ \tau(\mathbf{x})(\tau(\mathbf{x})+1)\neq 0}} \gamma(\tau(\mathbf{x}))\gamma(\tau(\mathbf{x})+1)\gamma(\tau(\mathbf{x})(\tau(\mathbf{x})+1)) + \gamma(1) + \gamma(-1) \\ &= \sum_{\substack{y\in\mathbb{F}_q \\ y(y+1)\neq 0}} \gamma(y^2(y+1)^2) + \gamma(1) + \gamma(-1) \geq q-2.\end{aligned}$$

Clearly Proposition 3.1. can be easily extended to cross-combined measures of higher order.

Thus we need to restrict the family $\mathcal{G}_{\leq K,\ quadratic}$ to a large subfamily of it such that this subfamily has a good cross-combined measure. In the one-dimensional case jointly with Mauduit and Sárközy [21] we have the following idea:

Construction 3.B *Consider the set of monic irreducible polynomials of the form* $f(x) = x^k + a_{k-2}x^{k-2} + a_{k-3}x^{k-3} + \dots + a_0$ *(so that the coefficient* $a_{k-1} = 0$*) with degree* $0 < k \le K$ *and let* $\mathcal{F}_{\le K,\ \mathit{irreducible},\ \mathit{Legendre}}$ $(\mathcal{F}_{\le K,\ \mathit{Legendre}})$ *the set of all binary sequences defined by* (1.1) *where the used monic irreducible polynomial* f *are in this form.*

Then by [21] the family $\mathcal{F}_{\le K,\ \mathit{irreducible},\ \mathit{Legendre}}$ has optimal cross-correlation measure:

Theorem 3.A

$$\varPhi_\ell(\mathcal{F}_{\le K,\ \mathit{irreducible},\ \mathit{Legendre}}) \le 10K\ell p^{1/2}\log p.$$

(This is Theorem 1 in [21]). Here the family $\mathcal{F}_{\le K,\ \mathit{irreducible},\ \mathit{Legendre}}$ is almost as large as $\mathcal{F}_{\le K,\ \mathit{Legendre}}$, and so far this is the only method to construct *very large* family of binary sequences with optimal cross-correlation measure. In Section 5 I will show another type of construction of a *very large* family of binary sequences for which the cross-correlation measure is nearly optimal.

Next I return to the cross-combined measure and the multi-dimensional case.

Construction 3.1 *Let* $\mathcal{G}_{\le K,\ \mathit{irreducible},\ \mathit{quadratic}}$ *denote the following subfamily of* $\mathcal{G}_{\le K,\ \mathit{quadratic}}$*: consider those* $\eta \in \mathcal{G}_{\le K,\ \mathit{quadratic}}$ *for which the used polynomials* f *in* (3.1) *are monic irreducible and of the form* $f(x) = x^k + a_{k-2}x^{k-2} + a_{k-3}x^{k-3} + \dots + a_0$ *(so that the coefficient* $a_{k-1} = 0$*) with degree* $0 < k \le K$ *and let* $\mathcal{G}_{\le K,\ \mathit{irreducible},\ \mathit{quadratic}}$ *the set of all binary lattices obtained in this way. Clearly* $G_{\le K,\ \mathit{irreducible},\ \mathit{quadratic}} \subset G_{\le K,\ \mathit{quadratic}}$*.*

Next I prove

Theorem 3.1

$$\varPhi_\ell(\mathcal{G}_{\le K,\ \mathit{irreducible},\ \mathit{quadratic}}) < K\ell q^{1/2}(\log p + 1)^n + 2\ell.$$

Proof. By the definition of cross-combined measure we have that there exist binary lattices $\eta_1, \eta_2, \dots, \eta_\ell \in \mathcal{G}_{\le K,\ \mathit{Legendre}}$ $D = (\mathbf{d}_1, \dots, \mathbf{d}_\ell)$ ℓ-tuple (where $\mathbf{d}_i \in \mathbb{I}_p^n$) and B box-lattice satisfying $B + \mathbf{d}_1, \dots, B + \mathbf{d}_\ell \subset I_p^n$ with the additional restriction that if $\eta_i = \eta_j$ for some $i \ne j$ then we must not have $\mathbf{d}_i = \mathbf{d}_j$ such that

$$\varPhi_\ell(\mathcal{G}_{\le K,\ \mathit{irreducible},\ \mathit{quadratic}}) = |V_\ell(\eta_1, \dots, \eta_\ell, B, D)| = \left| \sum_{\mathbf{x} \in B} \eta_1(\mathbf{x} + \mathbf{d}_1) \cdots \eta_\ell(\mathbf{x} + \mathbf{d}_\ell) \right| \quad (3.3)$$

Clearly by (3.2) there exists monic irreducible polynomials f_i $(i = 1, 2, \dots, \ell)$ such that all f_i can be written of the form the form

$$x^k + a_{k-2}x^{k-2} + a_{k-3}x^{k-3} + \dots + a_1 x + a_0 \tag{3.4}$$

for some $0 < k \le K$, $a_0, a_1, \dots, a_{k-2} \in \mathbb{F}_q$ (thus the coefficient of $x^{\deg f_i - 1}$ is always 0) and for the binary lattice η_i $(i = 1, 2, \dots, \ell)$ we have

$$\eta_i(\mathbf{x}) = \begin{cases} \gamma(f_i(\tau(\mathbf{x}))) & \text{for } f(\tau(\mathbf{x})) \neq 0 \\ +1 & \text{for } f_i(\tau(\mathbf{x})) = 0. \end{cases} \tag{3.5}$$

By (3.3), (3.5) and since irreducible polynomials may have only one zero (and only in the case of linear polynomials) we have

$$\begin{aligned} \varPhi_\ell(\mathcal{G}_{\le K,\ \mathit{irreducible},\ \mathit{quadratic}}) &\le \left| \sum_{\mathbf{x} \in B} \gamma(f_1(\tau(\mathbf{x} + \mathbf{d}_1))) \cdots \gamma(f_\ell(\tau(\mathbf{x} + \mathbf{d}_\ell))) \right| + 2\ell \\ &= \left| \sum_{\mathbf{y} \in \tau(B)} \gamma(f_1(y + \tau(\mathbf{d}_1)) \cdots f_\ell(y + \tau(\mathbf{d}_\ell))) \right| + 2\ell \end{aligned} \tag{3.6}$$

where the set $\tau(B)$ is defined by $\tau(B) \overset{\text{def}}{=} \{\tau(\mathbf{x}) : \ \mathbf{x} \in B\}$. Next we use Winterhof's Lemma [43]:

Lemma 3.1 *Let χ be a non-trivial multiplicative character of order d over $\mathbb{F}_q$ and $g \in \mathbb{F}_q[x]$ of a polynomial with s distinct zeros in $\overline{\mathbb{F}_q}$ and which is not of the form $ch(x)^d$ with $c \in \mathbb{F}_q$ and $h(x) \in \mathbb{F}_q[x]$. Then for $1 \le t_i < p$ $(i = 1, 2, \dots, n)$ and for a set C defined by*

$$C = C(t_1, t_2, \dots, t_n) = \{x_1 v_1 + x_2 v_2 + \dots + x_n v_n : \ 0 \le x_i \le t_i \text{ for } i = 1, 2, \dots, n\} \tag{3.7}$$

we have

$$\left| \sum_{y \in C} \chi(g(x)) \right| < s q^{1/2} (1 + \log p)^n \le \deg g \ q^{1/2} (1 + \log p)^n.$$

This is Theorem 2 in [43]. (The main tool in the proof is Weil theorem [42].)

Clearly the set $\tau(B)$ is a set of the form (3.7). We will use Lemma 3.1 with the quadratic character γ in place of χ and with the polynomial $g(y) \overset{\text{def}}{=} f_1(y + \tau(\mathbf{d}_1)) \cdots f_\ell(y + \tau(\mathbf{d}_\ell))$. In order to use this lemma first we need to show $g(y)$ is not of the form $ch(y)^2$. If for some

$1 \leq i < j \leq \ell$ we have $f_i(y) \neq f_j(y)$ then

$$f_i(y + \tau(\mathbf{d}_i)) \neq f_j(y + \tau(\mathbf{d}_j)) \tag{3.8}$$

also holds since if

$$f_i(y + \tau(\mathbf{d}_i)) = f_j(y + \tau(\mathbf{d}_j)) \tag{3.9}$$

then $\deg f_i = \deg f_j = k$. Then the coefficient of the term x^{k-1} are the same both in $f_i(y + \tau(\mathbf{d}_i))$ and $f_j(y + \tau(\mathbf{d}_j))$ and by the special form of these polynomials (see (3.4)) we also have that (3.9) holds only if $\tau(\mathbf{d}_i) = \tau(\mathbf{d}_j)$. Since τ is a bijection then we have $\mathbf{d}_i = \mathbf{d}_j$. Writing this in (3.9) we get the polynomials f_i and f_j are the same, but then the lattices η_i and η_j are also the same. In the definition of cross-combined measure we have the additional restriction that if $\eta_i = \eta_j$ then we must have $\mathbf{d}_i \neq \mathbf{d}_j$, which is contradiction. Thus we proved (3.8). By (3.8) we get $g(y)$ is a product of different irreducible polynomials thus it cannot be of the form $ch(y)^2$. So we may use Lemma 3.1 for the character sum in (3.6) and we obtain

$$\Phi_\ell(\mathcal{G}_{\leq K,\ irreducible,\ quadratic}) < K\ell q^{1/2}(\log p + 1)^n + 2\ell$$

which was to be proved.

4 Cross-combined measure of a family of binary lattices constructed by using Legendre symbol

Next I study a natural construction of families of two-dimensional binary lattices based on Legendre symbol introduced by Sárközy, Stewart and I in [25], [26]. In the case of this construction we will have slightly weaker upper bounds both for the pseudorandom measures of the binary lattices and for the cross-combined measure of the family than the optimal. The reason of this is that in order to estimate the necessary character sums we would need the two-dimensional analogue of Weil theorem [42]. The multi-dimensional analogue of Weil theorem were studied by Delinge [9], [10], and however later Fouvry and Katz [12] simplified the requirements still an inconvenient assumption of nonsingularity is required in order to reach the optimal bounds, which in our cases are not applicable. However in the case of this construction we have weaker upper bounds for the pseudorandom measures, on the other hand the lattices of the family can be generated very fast, which makes the implementation easy. Our starting point is the following construction defined by Sárközy, Stewart and I in [25]:

Construction 4.A *Let p be an odd prime. Denote by $\mathcal{R}_{\leq K}$ the set of monic polynomials $f \in \mathbb{F}_p[x_1, x_2]$ with degree $0 < \deg f \leq K$. Let $\mathcal{G}_{\leq K,\ Legendre}$ denote the family all binary lattices $\eta: \ I_p^2 \to \{-1, +1\}$ which can be written of the form defined by*

$$\eta(x_1, x_2) = \begin{cases} \left(\frac{f(x_1,x_2)}{p}\right) & \text{if } (f(x_1, x_2), p) = 1, \\ 1 & \text{if } p \mid f(x_1, x_2). \end{cases} \tag{4.1}$$

with a polynomial $f \in R_{\leq K}$.

In [25] and [26] jointly with Sárközy and Stewart we proved that under some not too restricitve conditions on the polynomial f or the prime p we have:

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

Similarly to Section 3, it turned out that for $K \geq 2$, the cross-combined measure of $\mathcal{G}_{\leq K,\ Legendre}$ is very bad:

Proposition 4.1 *For $K \geq 2$ we have $\Phi_3(G_{\leq K,\ Legendre}) \geq p^2 - 2$.*

The proof of Proposition 4.1 is similar to Proposition 3.1 thus we leave the details to the reader. Thus again we need to restrict $G_{\leq K,\ Legendre}$ to a proper large subfamily which has good cross-correlation measure. Again we have the idea using irreducible polynomials. Here we need the following special case of Theorem 1 in [25]:

Theorem 4.A *Let p be an odd prime, $f \in \mathbb{F}_p[x_1, x_2]$ be an irreducible polynomial in two variables of degree k. Define $\eta: \ I_p^2 \to \{-1, +1\}$ by (4.1). If $f(x_1, x_2)$ is not of the form*

$$f(x_1, x_2) = \varphi(\gamma x_1 + \delta x_2) \tag{4.2}$$

with $\gamma, \delta \in \mathbb{F}_p$ and $\varphi \in \mathbb{F}_p[x]$.

Then for the binary p-lattice defined by (4.1) we have

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

Indeed the condition that $f(x_1, x_2)$ is not of the form (4.2) is necessary? The answer is affirmative since by Theorem 2 in [26] we have

Theorem 4.B *Let p be an odd prime, $f \in \mathbb{F}_p[x_1, x_2]$ be a polynomial in two variables of degree k. Define $\eta :\ I_p^2 \to \{-1, +1\}$ by (4.1). If $f(x_1, x_2)$ is of the form $f(x_1, x_2) = \varphi(\gamma x_1 + \delta x_2)$ with some $\gamma, \delta \in \mathbb{F}_p$ and $\varphi \in \mathbb{F}_p[x]$, hen for the binary p-lattice defined by (4.1) we have*

$$Q_2(\eta) \geq p^2 - 4p^{3/2} - 8kp.$$

By Theorem 4.A and Theorem 4.B we have the idea studying the following subfamily of $\mathcal{G}_{\leq K,\ Legendre}$:

Construction 4.1 *Let $\mathcal{G}_{\leq K,\ irreducible,\ Legendre}$ denote the following subfamily of $\mathcal{G}_{\leq K,\ Legendre}$: consider those $\eta \in \mathcal{G}_{\leq K,\ quadratic}$ for which the used monic polynomials f in (4.1) are irreducible and not of the form (4.2). Clearly $G_{\leq K,\ irreducible,\ quadratic} \subset G_{\leq K,\ quadratic}$.*

The cross-combined measure of this family is relatively small:

Theorem 4.1

$$\Phi_\ell(\mathcal{G}_{\leq K,\ irreducible,\ Legendre}) < 11K\ell p^{3/2} \log p.$$

Proof. The theorem is trivial for the cases $p \leq 7$ and $p \leq K$, thus throughout the proof we may assume $p \geq 11$ and $K < p$. Let $\eta_1, \eta_2, \dots, \eta_\ell \in \mathcal{G}_{\leq K,\ irreducible,\ Legendre}$ binary lattices, $D = (\mathbf{d}_1, \dots, \mathbf{d}_\ell)$ and B box-lattice satisfying $B + \mathbf{d}_1, \dots, B + \mathbf{d}_\ell \subset I_p^n$ with the additional restriction that if $\eta_i = \eta_j$ for some $i \neq j$ then we must not have $\mathbf{d}_i = \mathbf{d}_j$ for which we have

$$\Phi_\ell(\mathcal{G}_{\leq K,\ irreducible,\ Legendre}) = |V_\ell(\eta_1, \dots, \eta_\ell, B, D)| = \left| \sum_{\mathbf{x} \in B} \eta_1(\mathbf{x} + \mathbf{d}_1) \cdots \eta_\ell(\mathbf{x} + \mathbf{d}_\ell) \right|$$

Clearly by (4.1) there exists monic irreducible polynomials f_i $(i = 1, 2, \dots, \ell)$ which are not of the form (4.2) and

$$\eta_i(\mathbf{x}) = \begin{cases} \left(\frac{f_i(\mathbf{x})}{p}\right) & \text{for } f(\mathbf{x}) \neq 0 \\ +1 & \text{for } f_i(\mathbf{x}) = 0. \end{cases}$$

Since for fixed x_1 the polynomial $f(\mathbf{x}) = f(x_1, x_2)$ has at most K zeros in x_2, we have $f(\mathbf{x})$ has at most Kp zeros in $\mathbf{x}$. Then similarly to (3.6) we get

$$\Phi_\ell(\mathcal{G}_{\leq K,\ irreducible,\ Legendre}) = \left| \sum_{\mathbf{x} \in B} \left(\frac{(f_1(\mathbf{x} + \mathbf{d}_1)) \cdots f_\ell(\mathbf{x} + \mathbf{d}_\ell)}{p} \right) \right| + 2K\ell p. \qquad (4.3)$$

First we mention that by the following lemma from [25] the irreducible polynomials $f_1(\mathbf{x}+\mathbf{d_1}),\dots,f_\ell(\mathbf{x}+\mathbf{d}_\ell)$ are different.

Lemma 4.1 *Let $\varphi(x_1,x_2)\in\mathbb{F}_p[x_1,x_2]$ be nonzero and let $c,a_1,a_2\in\mathbb{F}_p$ with $(a_1,a_2)\neq(0,0)$ be such that*

$$\varphi(x_1,x_2)=c\varphi(x_1+a_1,x_2+a_2),$$

for all (x_1,x_2) in $\mathbb{F}_p^2$. Suppose that the degree of $\varphi(x_1,x_2)$ is less than p. Then there is a polynomial $g\in F_p[x]$ such that

$$\varphi(x_1,x_2)=g(a_2x_1-a_1x_2).$$

This is Lemma 6 in [25]. We will also use the following lemma from [25]:

Lemma 4.2 *Let $p\geq 5$ be a prime and χ be a multiplicative character of order d. Suppose that $h(x_1,x_2)\in\mathbb{F}_p[x_1,x_2]$ is not of the form $cg(x_1,x_2)^d$ with $c\in\mathbb{F}_p$, $g(x_1,x_2)\in\mathbb{F}_p[x_1,x_2]$. Let k be the degree of $h(x_1,x_2)$. Then we have*

$$\sum_{\mathbf{x}\in B}\chi\left(h(\mathbf{x})\right)<10kp^{3/2}\log p$$

for every 2 dimensional box p-lattice $B\subseteq I_p^2$.

This is Lemma 2 in [25]. (The main tool in the proof is Weil theorem [42].)

Since by Lemma 4.1 the irreducible polynomials $f_1(\mathbf{x}+\mathbf{d_1}),\dots,f_\ell(\mathbf{x}+\mathbf{d}_\ell)$ are different, the product polynomial $g(\mathbf{x})=f_1(\mathbf{x}+\mathbf{d_1})\cdots f_\ell(\mathbf{x}+\mathbf{d}_\ell)$ cannot be of the form $cg(\mathbf{x})^2$. By (4.3) and using Lemma 4.2 we get

$$\Phi_\ell(\mathcal{G}_{\leq K,\ \textit{irreducible},\ \textit{Legendre}})<10K\ell p\log p+2K\ell p<11K\ell p\log p.$$

which was to be proved.

Corollary 4.1 *For all subfamily $\mathcal{G}_0$ of $\mathcal{G}_{\leq K,\ \textit{irreducible},\ \textit{Legendre}}$ we have*

$$\Phi_\ell(\mathcal{G}_0)<11K\ell p^{3/2}\log p..$$

This corollary is trivial and at first sight not very interesting. The important feature of it is that while the construction of one-variable irreducible polynomials is slow and complicated, then there is an easy way to construct two-variable irreducible polynomials using the Schöneman-Eisenstein criteria:

Lemma 4.3 *Let $f \in \mathbb{F}_p[x_1, x_2]$ be a polynomial of the form*

$$f(x_1, x_2) = x_1^k + x_1 x_2 g(x_1, x_2) + x_2 h(x_2) \tag{4.4}$$

with $g \in \mathbb{F}_p[x_1, x_2]$, $\deg g \leq k-3$, $h \in \mathbb{F}_p[x_2]$, $\deg h(x_2) \leq k-2$ and $x_2 \nmid h(x_2)$ Then $f(x_1, x_2)$ is irreducible and not of the form (4.2).

This lemma follows from the proof of Theorem 3 in [26] where the irreducibility of the polynomial was deduced from Theorem 282 in the book of Rédei [38].

Using polynomials of form (4.4) we can construct a large family of binary lattices such that its implementation is easy and fast:

Construction 4.2 *Let $\mathcal{G}_{\leq K,\ Sch-Eis,\ Legendre}$ denote the following subfamily of $\mathcal{G}_{\leq K,\ irreducible,\ Legendre}$: consider those $\eta \in \mathcal{G}_{\leq K,\ quadratic}$ for which the used polynomials f in (4.1) are of the form (4.4). Clearly $\mathcal{G}_{\leq K,\ Sch-Eis,\ Legendre} \subset G_{\leq K,\ irreducible,\ Legendre} \subset G_{\leq K,\ quadratic}$.*

Using Corollary 4.1 we immediately get

Corollary 4.2 *For all subfamily $\mathcal{G}_0$ of $\mathcal{G}_{\leq K,\ irreducible,\ Legendre}$ we have*

$$\Phi_\ell(\mathcal{G}_{\leq K,\ Sch-Eis,\ Legendre}) < 11K\ell p^{3/2} \log p.$$

Thus the family $\mathcal{G}_{\leq K,\ Sch-Eis,\ Legendre}$ has nearly optimal cross-combined measure, clearly is is very large (it contains more than $p^{K(K-1)/2}$ different binary lattices) and the binary lattices in it can be generated easily and very fast. In the next section we will show how is possible to generate a very large families of pseudorandom binary sequences with optimal or nearly optimal cross-correlation measure using these families of binary lattices.

5 Constructions of binary sequences with optimal or nearly optimal cross-correlation measures based on lattices and multi-dimensional theory

In [18] jointly with Mauduit and Sárközy we reduced the two dimensional case to the one-dimensional one by the following way: To any 2-dimensional binary N-lattice

$$\eta: \ I_N^2 \rightarrow \{-1, +1\} \tag{5.1}$$

we may assign a unique binary sequence $E_{N^2} = E_{N^2}(\eta) = \{e_1, e_2, \dots, e_{N^2}\} \in \{-1, +1\}^N$ 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

$$e_{iN+j} = \eta((j-1, i)) \text{ for } i = 0, 1, \dots, N^2 - 1, \ j = 1, 2, \dots, N. \tag{5.2}$$

We will denote the sequence defined by this way by $\overline{E}(\eta)$. In [18] with Mauduit and Sárközy we asked if it is true that if $\overline{E}(\eta)$ is a "good" pseudorandom binary *sequence* then η is a "good" pseudorandom 2-dimensional lattice? The answer to this question is negative; in [18] it is showed that it may occur that the pseudorandom measures of the sequence $E_{N^2}(\eta)$ are small, however, the corresponding pseudorandom measures of the lattice η are large. On the other hand, in [17] I proved the following: if the lattice η has small combined measure, then the corresponding $\overline{E}(\eta)$ sequence has small correlation measure as well.

Theorem 5.A *Let η be an arbitrary binary lattice. Then*

$$C_\ell(\overline{E}(\eta)) \le (\ell + 2) Q_\ell(\eta).$$

Here I generalize this result to families of binary sequences and lattices and the cross-correlation and cross-combined measure.

Definition 5.1 *Let $\mathcal{F}$ be a two-dimensional family of binary lattices $\eta : \ I_N^2 \to \{1-, +1\}$. Define the family $\overline{E}(\mathcal{G})$ of binary sequences of length N^2 by*

$$\overline{E}(\mathcal{G}) \overset{\text{def}}{=} \{\overline{E}(\eta) : \ \eta \in \mathcal{G}\}.$$

Next I will prove that if a family $\mathcal{G}$ of two-dimensional binary lattices has good cross-combined measure than the family of binary sequences $\overline{E}(\mathcal{G})$ also has good cross-correlation measure. The proof of this fact will be very similar to the proof of Theorem 5.A in [17].

Theorem 5.1 *Let $\mathcal{G}$ be a family of two-dimensional binary lattices $\eta : \ I_N^2 \to \{-1, +1\}$. Then*

$$\Phi_\ell(\overline{E}(\mathcal{G})) \le (\ell + 2)\Phi_\ell(\mathcal{G})$$

Proof. By the definition of the cross-correlation measure we have that there exist binary sequences $\overline{E}(\eta_1), \overline{E}(\eta_2), \dots, \overline{E}(\eta_\ell) \in \overline{E}(\mathcal{G})$ (where $\eta_1, \eta_2, \dots, \eta_\ell \in \mathcal{G}$), $M \in \mathbb{N}$ and ℓ-tuple $D = (d_1, d_2, \dots, d_\ell)$ of non-negative integers with $0 \le d_1 \le d_2 \le \dots \le d_\ell < M + d_\ell$ with the additional restriction that if $\overline{E}(\eta_i) = \overline{E}(\eta_j)$ (in other words $\eta_i = \eta_j$) for some $i \ne j$

then we must not have $d_i = d_j$ and for which

$$\varPhi_\ell(\overline{E}(\mathcal{G})) = \left|V_\ell(\overline{E}(\eta_1), \dots, \overline{E}(\eta_\ell), M, D)\right|. \tag{5.3}$$

Write $\overline{E}(\eta_i)$ of the form $\overline{E}(\eta_i) = (e_1^{(i)}, e_2^{(i)}, \dots, e_{N^2}^{(i)})$ for $i = 1, 2, \dots, \ell$. Then by (5.3)

$$\varPhi_\ell(\overline{E}(\mathcal{G})) = \left|\sum_{n=1}^{M} e_{n+d_1}^{(1)} \cdots e_{n+d_\ell}^{(\ell)}\right|. \tag{5.4}$$

Next few definitions will follow: For $x \in \mathbb{Z}$ let

$$x = r_N(x)N + m_N(x)$$

where $m_N(x) \equiv x \pmod N$, $0 \le m_N(x) \le N-1$ and $r_N(x) = \left[\frac{x}{N}\right]$.

By definition $e_{yN+x+1}^{(i)} = \eta_i(x, y)$ for $0 \le x \le N-1,\ 0 \le y \le N-1$ and $i = 1, \dots, \ell$ and thus

$$e_n^{(i)} = \eta_i(m_N(n-1), r_N(n-1)).$$

Then for $1 \le i \le \ell$

$$e_{n+d_i}^{(i)} = \eta(m_N(n+d_i-1), r_N(n+d_i-1)). \tag{5.5}$$

Here

$$n + d_i - 1 = (r_N(n-1) + r_N(d_i))N + m_N(n-1) + m_N(d_i).$$

Thus if $0 \le m_N(n-1) + m_N(d_i) \le N-1$ then

$$r_N(n+d_i-1) = r_N(n-1) + r_N(d_i), \qquad m_N(n+d_i-1) = m_N(n-1) + m_N(d_i)$$

and if $N \le m_N(n-1) + m_N(d_i)$ then

$$r_N(n+d_i-1) = r_N(n-1) + r_N(d_i) + 1, \qquad m_N(n+d_i-1) = m_N(n-1) + m_N(d_i) - N.$$

Thus we get that there exists an $a_i \overset{\text{def}}{=} N - 1 - m_N(d_i)$ such that for $m_N(n-1) \le a_i$

$$r_N(n+d_i-1) = r_N(n-1) + r_N(d_i), \qquad m_N(n+d_i-1) = m_N(n-1) + m_N(d_i) \tag{5.6}$$

and for $a_i + 1 \le m_N(n-1)$

$$r_N(n+d_i-1) = r_N(n-1) + r_N(d_i) + 1, \qquad m_N(n+d_i-1) = m_N(n-1) + m_N(d_i) - N. \tag{5.7}$$

Then $\{1, a_1+1, a_2+1, \dots, a_\ell+1, m_N(M-1)+1, N\}$ is a multiset which contains integers $1 = c_1 < c_2 < \dots < c_m \le N$ where $m \le \ell + 3$. By (5.6) and (5.7) we get that for $c_j \le n \le c_{j+1} - 1$ there exist numbers $b_{i,j}$ and $f_{i,j}$ such that

$$r_N(n+d_i-1) = r_N(n) + r_N(d_i-1) + b_{i,j}, \quad m_N(n+d_i-1) = m_N(n) + m_N(d_i-1) - f_{i,j} \tag{5.8}$$

where $b_{i,j} \in \{0,1\}$ and $f_{i,j} \in \{0, N\}$. Moreover, if $b_{i,j} = 0$ then $f_{i,j} = 0$ and if $b_{i,j} = 1$ then $f_{i,j} = N$. Now

$$\begin{aligned}
&[1, M] = \\
&= \{n = TN + x + 1 : \ T = 0, 1, \dots, \left[\frac{M-1}{N}\right], \ x = 0, 1, \dots, m_N(M-1)\} \\
&\cup \{n = TN + x + 1 : \ T = 0, 1, \dots, \left[\frac{M-1}{N}\right] - 1, \ x = m_N(M-1) + 1, \\
&\dots, N-1\}.
\end{aligned}$$

Thus

$$\begin{aligned}
[1, M] = \cup_{j=1}^{m-1} \{n : \ & n = r_N(N-1)N + m_N(n-1) + 1, \\
& c_j \le m_N(n-1) \le c_{j+1} - 1, \ r_N(n-1) \in \{0, 1, 2, \dots, T_j\}\}
\end{aligned} \tag{5.9}$$

where $T_j = \left[\frac{M-1}{N}\right]$ if $c_{j+1} \le m_N(M-1)+1$ and $T_j = \left[\frac{M-1}{N}\right] - 1$ if $m_N(M-1)+1 \le c_j$. (Since $m_N(M-1)+1 \in \{c_1, c_2, \dots, c_m\}$ and $c_1 < c_2 < \dots < c_m$ thus $c_j < m_N(M-1)+1 < c_{j+1}$ is not possible.) By this, (5.4), (5.5) and (5.6)

$$\begin{aligned}
\Phi_\ell(\overline{E}(\mathcal{G})) &= \sum_{n=1}^{M} e_{n+d_1}^{(1)} \cdots e_{n+d_\ell}^{(\ell)} = \sum_{j=1}^{m-1} \sum_{\substack{c_j \le m_N(n-1) \le c_{j+1}-1 \\ 1 \le n \le M}} e_{n+d_1}^{(1)} \dots e_{n+d_\ell}^{(\ell)} \\
&= \sum_{j=1}^{m-1} \sum_{\substack{c_j \le m_N(n-1) \le c_{j+1}-1 \\ 1 \le n \le M}}
\end{aligned}$$

$$\prod_{i=1}^{\ell} \eta_i(m_N(n-1)+m_N(d_i)-f_{i,j}, r_N(n-1)+r_N(d_i)+b_{i,j}) \tag{5.10}$$

By (5.9)

$$\{(m_N(n-1), r_N(n-1)) :\ 1 \le n \le M \text{ and } c_j \le m_N(n-1) \le c_{j+1}-1\} =$$
$$\{(x,y) :\ 0 \le x \le T_j \text{ and } c_j \le y \le c_{j+1}-1\}.$$

Using this, (5.8) and (5.10) we get

$$\begin{aligned}\varPhi_\ell(\overline{E}(\mathcal{G})) &= \sum_{j=1}^{m-1}\sum_{x=0}^{T_j}\ sum_{y=c_j}^{c_{j+1}-1}\prod_{i=1}^{\ell}\eta_i(x+m_N(d_i)-f_{i,j}, y+r_N(d_i)+b_{i,j}) \le (m-1)\varPhi_\ell(\mathcal{G})\\ &\le (\ell+2)\varPhi_\ell(\mathcal{G})) \end{aligned} \tag{5.11}$$

which was to be proved. Let us see whether the pairs $(m_N(d_i)-f_{i,j},\ r_N(d_i)+b_{i,j})$ are different for fixed j as i runs over $1,2,\dots,\ell$. Indeed if for fixed j there exist i_1 and i_2 with

$$(m_N(d_{i_1})-f_{i_1,j},\ r_N(d_{i_1})+b_{i_1,j}) = (m_N(d_{i_2})-f_{i_2,j},\ r_N(d_{i_2})+b_{i_2,j}),$$

then

$$N(r_N(d_{i_1})+b_{i_1,j})+m_N(d_{i_1})-f_{i_1,j} = N(r_N(d_{i_2})+b_{i_2,j})+m_N(d_{i_2})-f_{i_2,j}.$$

Since if $b_{i,j}=0$ then $f_{i,j}=0$ and if $b_{i,j}=1$ then $f_{i,j}=N$, from this we get

$$\begin{aligned} Nr_N(d_{i_1})+m_N(d_{i_1}) &= Nr_N(d_{i_2})+m_N(d_{i_2})\\ d_{i_1} &= d_{i_2}\end{aligned}$$

By the definition of cross-correlation measure $d_{i_1}=d_{i_2}$ is possible only if $\overline{E}(\eta_{i_1}) \ne \overline{E}(\eta_{i_2})$. Then clearly we have $\eta_{i_1} \ne \eta_{i_2}$, so indeed

$$\left|\sum_{x=0}^{T_j}\sum_{y=c_j}^{c_{j+1}-1}\prod_{i=1}^{\ell}\eta_i(x+m_N(d_i)-f_{i,j}, y+r_N(d_i)+b_{i,j})\right|$$

can be estimated by $\varPhi_\ell(\mathcal{G})$ in (5.11). This completes the proof of Theorem 5.1

Using Theorems 3.1, 4.1, Corollary 4.2 and Theorem 5.A we immediately get the following:

Corollary 5.1 *Let $q = p^2$ where p is a prime and define $\mathcal{G}_{\leq K,\ irreducible,\ quadratic}$ as in Construction 3.1. Then*

$$\Phi_\ell(\overline{E}(\mathcal{G}_{\leq K,\ irreducible,\ quadratic})) < K\ell(\ell+2)p(\log p+1)^n + 2\ell.$$

Corollary 5.2 *Let p be a prime and define $\mathcal{G}_{\leq K,\ irreducible,\ Legendre}$ as in Construction 4.1. Then*

$$\Phi_\ell(\overline{E}(\mathcal{G}_{\leq K,\ irreducible,\ Legendre})) < 11K\ell(\ell+2)p^{3/2}\log p.$$

Corollary 5.3 *Let p be a prime and define $\mathcal{G}_{\leq K,\ Sch-Eis,\ Legendre}$ as in Construction 4.2. Then*

$$\Phi_\ell(\overline{E}(\mathcal{G}_{\leq K, Sch-Eis,\ Legendre})) < 11K\ell(\ell+2)p^{3/2}\log p.$$

Thus each family of binary sequences in Corollaries 1,2 and 3 have optimal or nearly optimal cross-combined measure. Between them we were able to prove the strongest bound for cross-correlation measure in the case of the family of $\overline{E}(\mathcal{G}_{\leq K,\ irreducible,\ quadratic})$. The weak point of this construction is that it is based on one-variable irreducible polynomials over $\mathbb{F}_{p^2}$, which have slow and complicated generation. Using binary lattices based on two-variable irreducible polynomials and Legendre symbol this problem can be avoided, however a slightly weaker upper bound is obtained for the cross-correlation measure than in the original construction. But, contrary to one-variable polynomials, using Schöneman-Eisenstein criteria it is very easy to construct two-variable irreducible polynomials over $\mathbb{F}_p$ (e.g. see Lemma 4.3). Indeed by Construction 4.2 the binary lattices in $\mathcal{G}_{\leq K,\ Sch-Eis,\ Legendre}$ can be implemented easily and fast, and thus the binary sequences in $\overline{E}(\mathcal{G}_{\leq K, Sch-Eis,\ Legendre})$ also can be implemented easily and fast. However we do not have the strongest bound $cp\log p$, we have only $cK\ell^2 p^{3/2}\log p$ for the cross-correlation measure of this family, it is much better than than the trivial bound p^2. Moreover, the family $\overline{E}(\mathcal{G}_{\leq K, Sch-Eis,\ Legendre})$ is very big, it contains more than $p^{K(K-1)/2}$ pieces of binary sequences, which is also important in the applications.

References

1. R. Ahlswede, L. H. Khachatrian, C. Mauduit and A. Sárközy, *A complexity measure for families of binary sequences*, Period. Math. Hungar. 46 (2003), 107-118.

2. R. Ahlswede, C. Mauduit and A. Sárközy, *Large families of pseudorandom sequences of k symbols and their complexity. I*, Lecture Notes in Comput. Sci. 4123, General Theory of Information Transfer and Combinatorics, Springer, Berlin, 2006; pp. 293-307.
3. R. Ahlswede, C. Mauduit and A. Sárközy, *Large families of pseudorandom sequences of k symbols and their complexity. II*, Lecture Notes in Comput. Sci. 4123, General Theory of Information Transfer and Combinatorics, Springer, Berlin, 2006; pp. 308-325.
4. N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, *Measures of pseudorandomness for finite sequences: typical values*, Proc. London Math. Soc. 95 (2007), 778-812.
5. V. Anantharam, *A technique to study the correlation measures of binary sequences*, Discrete Math. 308 (2008), 6203-6209.
6. A. Bérczes, J. Ködmön and A. Pethő, *A one-way function based on norm form equations*, Period. Math. Hungar. 49 (2004), 1-13.
7. J. Cassaigne, S. Ferenczi, C. Mauduit, J. Rivat and A. Sárközy, *On finite pseudorandom binary sequences III: The Liouville function, I*, Acta Arith. 87 (1999), 367-384.
8. J. Cassaigne, C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences VII: The measures of pseudorandomness*, Acta Arith. 103 (2002), 97-118.
9. P. Delinge, *La conjecture de Weil, I*, Pub. Math. I. H. E. S. 43 (1974), 273-307.
10. P. Delinge, *La conjecture de Weil, II*, Pub. Math. I. H. E. S. 43 (1980), 137-250.
11. H. Feistel, W. A. Notz and J. L. Smith, *Some cryptographic techniques for machine -to- machine data communications*, Proc. IEEE 63 (1975), 1545-1554.
12. E. Fouvry, N. Katz, *A general stratification theorem for exponential sums, and applications*, J. Reine Angew. Math. 540 (2001), 115-166.
13. G. Gong, *Character Sums and Polyphase Sequence Families with Low Correlation, Discrete Fourier Transform (DFT), and Ambiguty*, in: Finite Fields and Their Applications, Radon Series on Computational and Applied Mathematics 11, eds. C. Pascale et al., 2013, de Gruyter, Berlin; 1-42.
14. L. Goubin, C. Mauduit and A. Sárközy, *Construction of large families of pseudorandom binary sequences*, J. Number Theory 106 (2004), 56-69.
15. K. Gyarmati, *Concatenation of pseudorandom binary sequences*, Period. Math. Hungar. 58 (2009), 99-120.
16. K. Gyarmati, *On the complexity of a family related to the Legendre symbol*, Period. Math. Hungar. 58 (2009), 209-215.
17. K. Gyarmati, *On the correlation of subsequences*, Unif. Distrib. Theory 7 (2012), 169-195.
18. K. Gyarmati, C. Mauduit, A. Sárközy, *Pseudorandom binary sequences and lattices*, Acta Arith. **135** (2008), 181-197.
19. K. Gyarmati, C. Mauduit and A. Sárközy, *Measures of pseudorandomness of finite binary lattices, I (The measures Q_k, normality.)*, Acta Arith. 144 (2010), 295-313.
20. 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.
21. K. Gyarmati, C. Mauduit and A. Sárközy, *The cross-correlation measure for families of binary sequences*, Applications of Algebra and Number Theory (Lectures on the occasion of Harald Niederreiter's 70th Birthday) 2014, eds.: G. Larcher, F. Pillichshammer, A. Winterhof and C. Xing.
22. K. Gyarmati, C. Mauduit and A. Sárközy, *Measures of pseudorandomness of finite binary lattices, I. (The measures Q_k, normality.)*, Acta Arith. 144 (2010), 295-313.
23. K. Gyarmati, C. Mauduit and A. Sárközy, *Measures of pseudorandomness of finite binary lattices, II. (The symmetry measures.)*, Ramanujan J. 25 (2011), 155-178 .
24. 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.

25. K. Gyarmati, A. Sárközy and C. L. Stewart, *On Legendre symbol lattices*, Unif. Distrib. Theory 4 (2009), 81-95.
26. K. Gyarmati, A. Sárközy and C. L. Stewart, *On Legendre symbol lattices, II*, Unif. Distrib. Theory 8 (2013), 47-65.
27. J. Hoffstein and D. Lieman, *The distribution of the quadratic symbol in function fields and a faster mathematical stream cipher*, Progress in Computer Science and Applied Logic, Vol. 20, Birkhäuser, Verlag, Basel, 2001; pp. 59-68.
28. P. Hubert, C. Mauduit and A. Sárközy, *On pseudorandom binary lattices*, Acta Arith. 125 (2006), 51-62.
29. J. Kam and G. Davida, *Structured design of substitution-permutation encryption networks*, IEEE Transactions on Computers 28 (1979), 747-753.
30. C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences I: Measures of pseudorandomness, the Legendre symbol*, Acta Arith. 82 (1997), 365-377.
31. C. Mauduit and A. Sárközy, *Construction of pseudorandom binary sequences by using the multiplicative inverse*, Acta Math. Hungar. 108 (2005), 239-252.
32. C. Mauduit and A. Sárközy, *On large families of pseudorandom binary lattices*, Unif. Distr. Theory 2 (2007), 23-37.
33. C. Mauduit and A. Sárközy, *Family Complexity and VC-dimension*, in: Ahlswede Festschrift, eds. H. Aydinian et al., LNCS 7777, Springer, Berlin, 2013; pp. 346-363.
34. A. Menezes, P. C. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRS Press, Boca Raton, 1997.
35. L. Mérai, *On the typical values of the cross-correlation measure*, Monatsh. Math. 180 (2016) no. 1, 83-99.
36. L. Mérai, *The cross-correlation measure of families of finite binary sequences: limiting distributions and minimal values*, Discrete Appl. Math. 214 (2016) 153–168.
37. L. Mérai, J. Rivat and A. Sárközy, *The measures of pseudorandomness and the NIST tests*, submitted.
38. L. Rédei, *Algebra*, Pergamon Press, Oxford-New York-Toronto, Ont. 1967.
39. J. Rivat and A. Sárközy, *On pseudorandom sequences and their application*, Lecture Notes in Comput. Sci. 4123, General theory of information transfer and combinatorics, Springer, Berlin / Heidelberg, 2006, 343-361.
40. V. Tóth, *Collision and avalanche effect in families of pseudorandom binary sequences*, Period. Math. Hungar. 55 (2007), 185-196.
41. V. Tóth, *The study of collision and avalanche effect in a family of pseudorandom binary sequences*, Period. Math. Hungar. 59 (2009), 1-8.
42. A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Act. Sci. Ind. 1041, Hermann, Paris, 1948.
43. A. Winterhof, *Some Estimates for Character Sums and Applications*, Designs, Codes and Cryptography 22 (2001), 123-131.