On an inequality between pseudorandom measures of lattices

Katalin Gyarmati
Eötvös Loránd University
Department of Algebra and Number Theory
H-1117 Budapest, Pázmány Péter sétány 1/C
E-mail: gykati@cs.elte.hu

Richárd Sebők
Eötvös Loránd University
Department of Algebra and Number Theory
H-1117 Budapest, Pázmány Péter sétány 1/C
E-mail: sebokrichard.hun@gmail.com

Abstract

Mauduit and Sárközy proved the following inequality between the well-distribution measure and the correlation measure of order 2: $W(E_N) \leq 3\sqrt{NC_2(E_N)}$. This result has been generalized to inequalities between the combined pseudorandom measures and correlation measures of even order by the authors of the present paper. Here

Supported by National Research Development and Innovation Office, NKFIH KKP133819 and K119528.

2010 *Mathematics Subject Classification*: Primary 11K45

Key words and phrases: binary sequences, pseudorandomness, well-distribution, correlation.

the multidimensional case is studied, and this inequality is extended further to the case of binary lattices.

1 Introduction

In 1997 Mauduit and Sárközy [8] introduced new pseudorandom measures of finite binary sequences in order to study the pseudorandom properties of these sequences. These pseudorandom measures are the following: For a binary sequence $E_N = (e_1, \dots, e_N) \in \{-1, +1\}^N$ of length N, the *well-distribution measure of* E_N is defined as

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

where the maximum is taken over all $a \in \mathbb{Z}$, $b, t \in \mathbb{N}$ such that $1 \leq a \leq a + b(t-1) \leq N$.

The *correlation measure of order* k *of* E_N is defined as

$$C_k(E_N) = \max_{M,D} \left| V(E_N, M, D) \right| = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \dots e_{n+d_k} \right|,$$

where the maximum is taken over all $D = (d_1, \dots, d_k)$ with non-negative integers $d_1 < \dots < d_k$ and $M \in \mathbb{N}$ such that $M + d_k \leq N$.

Mauduit and Sárközy [8] showed that a finite binary sequence can be considered as a good pseudorandom sequence if both the well-distribution measure and the correlation measures are small. For more details see e.g., the survey paper [4].

The *combined* (well-distribution-correlation) *pseudorandom measure of order* k *of* E_N is defined as

$$\begin{aligned} Q_k(E_N) &= \max_{a,b,t,D} \left| Z(a, b, t, D) \right| \\ &= \max_{a,b,t,D} \left| \sum_{j=0}^{t-1} e_{a+jb+d_1} e_{a+jb+d_2} \dots e_{a+jb+d_k} \right|, \end{aligned}$$

where the maximum is taken over all $a, b, t, D = (d_1, d_2, \dots, d_k)$ such that all the subscripts $a + jb + d_\ell$ belong to $\{1, \dots, N\}$.

In [9] Mauduit and Sárközy proved a sharp inequality between the well-distribution measure of E_N and the correlation measure of order 2 of E_N for every $E_N \in \{-1, +1\}^N$.

Theorem A (Mauduit and Sárközy)**.** *For $N \geq 1$ and $E_N = (e_1, \dots, e_N) \in \{-1, +1\}^N$ we have*

$$W(E_N) \leq 3\sqrt{NC_2(E_N)}. \tag{1.1}$$

Later in [3] the first author of the present paper generalized Theorem A to a similar inequality between W and C_{2k}. In 2015 the second author of the present paper generalized further this inequality, namely he proved the following result:

Theorem B (Sebők)**.** *For $N \geq 1$ and $E_N = (e_1, \dots, e_N) \in \{-1, +1\}^N$, $k \in \mathbb{N}$ and for $1 \leq l \leq k$ we have*

$$Q_k(E_N) \leq 2\sqrt{N \max_{1 \leq l \leq k} C_{2l}(E_N)}. \tag{1.2}$$

Note that an important consequence of Theorems A and B is that if one needs only nontrivial upper bounds for the measures W and Q_k (but one does not need possibly sharp upper bounds), then this sort of bounds can be obtained by just estimating C_{2k} (for k not very large), thus the computation can be shortened considerably; besides, it often occurs that one can find estimates in the literature for the corresponding "complete correlation" (see the references in [10] for complete correlation estimates in both one dimensional and multidimensional cases) and there is a standard technique to deduce the "incomplete" correlation estimates used in the study of pseudorandom measures from the complete ones, which may reduce the computation further.

In [9] Mauduit and Sárközy also showed that their upper bound for $W(E_N)$ in terms of $C_2(E_N)$ is sharp, namely in the range

$$N^{3/4}(\log N)^{1/4} \ll W(E_N) \leq N$$

(1.1) is best possible apart from a constant factor:

Theorem C (Mauduit and Sárközy). *If $m, N \in \mathbb{N}$, $N > N_0$ and*

$$N^{3/4} \ll m \leq N,$$

then there is a sequence $E_N \in \{-1,+1\}^N$ with

$$W(E_N) \geq m$$

and

$$C_2(E_N) \leq 120 \max \left\{ \frac{m^2}{N}, (N \log N)^{1/2} \right\}. \tag{1.3}$$

Note that it follows from (1.3) that if $m \geq N^{3/4} (\log N)^{1/4}$ then

$$m \leq W(E_N) \leq 3(NC_2(E_N))^{1/2} < 33m$$

so that, indeed, the lower and upper bounds coincide apart from a constant factor.

In case of *multidimensional* binary lattices the computation of the pseudorandom measures is much more complicated, than in the one dimensional case, so that in the multidimensional case a generalization of inequality (1.2) to lattices might be even more useful than (1.2) in one dimension. Thus here our goal is to present such a generalization of (1.2). First, we will present the definitions of the multidimensional measures. The study of the multidimensional case was started by the work of Hubert, Mauduit and Sárközy. In [7] they introduced the following definitions.

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

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

This set is called an *n-dimensional N-lattice* or briefly an *N-lattice*. Hubert, Mauduit and Sárközy [7] extended the definition of binary sequences to more dimensions by considering functions of type

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

called *binary lattices.*

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 by writing $\eta(\mathbf{x}) = \eta(x_1, \dots, x_n)$.

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, writing $z_i = |\mathbf{u_i}|$, $\mathbf{u_i}$ 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

$$B_N^n = \{\mathbf{x} = x_1\mathbf{u_1} + \dots + x_n\mathbf{u_n} : 0 \le x_i z_i \le t_i (< N) \text{ for } i = 1, \dots, n\} \quad (1.4)$$

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

Hubert, Mauduit and Sárközy [7] introduced the following measures of pseudorandomness of binary lattices (here we present the definitions in a slightly modified form as in [6] but equivalent with the ones in [7]). Let η be a binary lattice

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

Define the combined pseudorandom measure of order k of η by

$$Q_k(\eta) = \max_{B, \mathbf{d_1}, \mathbf{d_2}, \dots, \mathbf{d_k}} \left| \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d_1}) \dots \eta(\mathbf{x} + \mathbf{d_k}) \right|,$$

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

The combined measures of binary lattices are natural extensions of the combined measures of binary sequences. In certain applications one may also need the extension of the correlation measures for the multidimensional theory. These new measures were introduced by Gyarmati, Mauduit and Sárközy [5]. They introduced the following measure of pseudorandomness of binary lattices: the *correlation measure of order l* of the lattice $\eta : I_N^n \to \{-1, +1\}$ is defined by

$$C_\ell(\eta) = \max_{B', \mathbf{d_1}, \dots, \mathbf{d_\ell}} \left| \sum_{\mathbf{x} \in B'} \eta(\mathbf{x} + \mathbf{d_1}) \dots \eta(\mathbf{x} + \mathbf{d_\ell}) \right|,$$

where the maximum is taken over all distinct $\mathbf{d_1}, \dots, \mathbf{d}_\ell \in I_N^n$ and all box lattices B' of the special form

$$B' = \{\mathbf{x} = (x_1, \dots, x_n) : 0 \le x_1 \le t_1(< N), \dots, 0 \le x_n \le t_n(< N)\}$$

such that $B' + \mathbf{d_1}, \dots, B' + \mathbf{d}_\ell \subseteq I_N^n$.

In this paper, we will generalize Theorem B to n dimension.

Theorem 1. *For $1 \le k, n, N \in \mathbb{N}$ and binary lattice $\eta : I_N^n \to \{-1, +1\}$ we have*

$$Q_k(\eta) \le \sqrt{(2^n + k^2)\, N^n C_{2k}(\eta)}.$$

As in the case of sequences this result shows that in order to get a "good" (but not necessarily optimal) upper bound for the combined measure it is enough to estimate the correlation measures.

We will also show that Theorem 1 is sharp, namely we will prove the following result:

Theorem 2. *For $1 \le k, n \in \mathbb{N}$ and $3/4 < c \le 1$ there are infinitely many $N \in \mathbb{N}$ such that there exists a binary lattice $\eta : I_N^n \to \{-1, +1\}$ for which*

$$N^{cn} \gg Q_k(\eta) \gg \sqrt{N^n C_{2k}(\eta)} \gg N^{cn},$$

where the implied constant factors depend only on n and k.

(Here $\gg$ is Vinogradov's notation so that e.g. $f(N) \gg g(N)$ means that there is a positive constant C such that for all N we have $|f(N)| \ge C\,|g(N)|$.)

2 Proof of Theorem 1

We will prove that for every box lattice B we have

$$\left| \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d_1}) \cdots \eta(\mathbf{x} + \mathbf{d_k}) \right| \le \sqrt{(2^n + k^2)\, N^n C_{2k}(\eta)},$$

in other words, we will prove

$$\left|\sum_{\mathbf{x}\in B}\eta(\mathbf{x}+\mathbf{d_1})\cdots\eta(\mathbf{x}+\mathbf{d_k})\right|^2 \leq \left(2^n+k^2\right)N^nC_{2k}(\eta),$$

from which the theorem follows.

Let

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

be a fixed box lattice. If $\mathbf{x}\notin I_N^n$, then we define $\eta(\mathbf{x})=0$. Now we define the boxes A and C as

$$A=\{\mathbf{x}\in I_N^n: 0\leq x_i<z_i(<N) \text{ for } i=1,\ldots,n\} \tag{2.1}$$

and

$$C=\{\mathbf{x}=x_1\mathbf{u_1}+\cdots+x_n\mathbf{u_n}: -t_i\leq x_iz_i\leq t_i(<N) \text{ for } i=1,\ldots,n\}.$$

Then

$$|C|<2^n|B|\leq 2^nN^n. \tag{2.2}$$

We will use the notation of addition and subtraction of box lattices as the usual set addition and subtraction, namely $B_1+B_2=\{\mathbf{b_1}+\mathbf{b_2}: \ \mathbf{b_1}\in B_1,\ \mathbf{b_2}\in B_2\}$ and $B_1-B_2=\{\mathbf{b_1}-\mathbf{b_2}: \ \mathbf{b_1}\in B_1,\ \mathbf{b_2}\in B_2\}$. Note that

$$C=B-B$$

for the box lattices B and C defined above. It is also possible to consider the difference of a box lattice B and a vector $\mathbf{x}$:

$$B-\mathbf{x}=\{\mathbf{b}-\mathbf{x}:\mathbf{b}\in B\ \}.$$

Consider the sum

$$S=\sum_{\mathbf{m}\in A}\left(\sum_{\mathbf{x}\in B}\eta(\mathbf{x}+\mathbf{d_1}+\mathbf{m})\ldots\eta(\mathbf{x}+\mathbf{d_k}+\mathbf{m})\right)^2.$$

It is clear that

$$\left| \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d}_1) \cdots \eta(\mathbf{x} + \mathbf{d}_k) \right|^2 \leq S,$$

thus in order to prove the theorem we have to prove that

$$S \leq \left(2^n + k^2\right) N^n C_{2k}(\eta).$$

Clearly,

$$\begin{aligned}
S &= \sum_{\mathbf{m} \in A} \left(\sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d_1} + \mathbf{m}) \ldots \eta(\mathbf{x} + \mathbf{d_k} + \mathbf{m}) \right)^2 \\
&= \sum_{\mathbf{m} \in A} \left(\sum_{\mathbf{x} \in B} \prod_{i=1}^{k} \eta(\mathbf{x} + \mathbf{d_i} + \mathbf{m}) \right) \left(\sum_{\mathbf{y} \in B} \prod_{j=1}^{k} \eta(\mathbf{y} + \mathbf{d_j} + \mathbf{m}) \right) \\
&= \sum_{\mathbf{m} \in A} \sum_{\mathbf{x}, \mathbf{y} \in B} \prod_{i=1}^{k} \eta(\mathbf{x} + \mathbf{d}_i + \mathbf{m}) \prod_{j=1}^{k} \eta(\mathbf{y} + \mathbf{d}_j + \mathbf{m})
\end{aligned}$$

Next by the identity

$$\prod_{i=1}^{k} a_i \prod_{j=1}^{k} b_j = a_1 a_2 \cdots a_k b_1 b_2 \cdots b_k = a_1 b_1 a_2 b_2 \cdots a_k b_k = \prod_{i=1}^{k} a_i b_i$$

we get

$$S = \sum_{\mathbf{m} \in A} \left(\sum_{\substack{\mathbf{x}, \mathbf{y} \\ \mathbf{x}, \mathbf{y} \in B}} \prod_{i=1}^{k} \eta(\mathbf{x} + \mathbf{d_i} + \mathbf{m}) \eta(\mathbf{y} + \mathbf{d_i} + \mathbf{m}) \right).$$

Then

$$S = \sum_{\mathbf{m}\in A}\sum_{\mathbf{x}\in B}\left(\prod_{i=1}^{k}\eta(\mathbf{x}+\mathbf{d_i}+\mathbf{m})\right)^2 + $$
$$+ \sum_{\mathbf{m}\in A}\sum_{\mathbf{x}\in B}\sum_{\substack{\mathbf{c}\in B-\mathbf{x}\\ \mathbf{c}\neq\mathbf{0}}}\prod_{i=1}^{k}\eta(\mathbf{x}+\mathbf{d_i}+\mathbf{m})\eta(\mathbf{x}+\mathbf{c}+\mathbf{d_i}+\mathbf{m})$$
$$= \sum_{\mathbf{m}\in A}\sum_{\mathbf{x}\in B}\left(\prod_{i=1}^{k}\eta(\mathbf{x}+\mathbf{d_i}+\mathbf{m})\right)^2 + $$
$$+ \sum_{\substack{\mathbf{c}\in C\\ \mathbf{c}\neq\mathbf{0}}}\sum_{\mathbf{x}\in B\cap(B-\mathbf{c})}\sum_{\mathbf{m}\in A}\prod_{i=1}^{k}\eta(\mathbf{x}+\mathbf{d_i}+\mathbf{m})\eta(\mathbf{x}+\mathbf{c}+\mathbf{d_i}+\mathbf{m}).$$

Notice that the set A+B is also a box-lattice, denote it by $D \subseteq I_N^n$ and $B \cap (B - \mathbf{c})$ is a shifted version of a box lattice. The reason of this is that $B \cap (B - \mathbf{c})$ is non-empty only if $\mathbf{c}$ is a vector whose i-th coordinate is divisible by z_i, so $\mathbf{c}$ is of the form $\mathbf{c} = (c_1z_1, c_2z_2, \dots, c_nz_n)$. Define s_i by

$$s_i = \begin{cases} 0 & \text{if } c_i \geq 0 \\ -c_iz_i & \text{if } c_i < 0 \end{cases}$$

and let $\mathbf{s}(c)$ be the vector $\mathbf{s}(c) = (s_1, s_2, \dots, s_n)$. We define $B(c)$ as the following box lattice:

$$B(c) = \{\mathbf{x} = x_1\mathbf{u_1} + \dots + x_n\mathbf{u_n} : 0 \leq x_iz_i \leq t_i - c_iz_i - s_iz_i (< N)$$
$$\text{for } i = 1, \dots, n\}.$$

After introducing these notation it is not very difficult to see that $B \cap (B - \mathbf{c})$ is indeed a shifted box-lattice, namely

$$B \cap (B - \mathbf{c}) = \mathbf{s}(\mathbf{c}) + B(c).$$

Moreover $A + B(c)$ is also a box-lattice, denote it by $D(c)$. Using this new notation we get

$$
\begin{aligned}
S =& \sum_{z\in D}\left(\prod_{i=1}^{k}\eta(\mathbf{z}+\mathbf{d_i})\right)^2 + \\
&+\sum_{\substack{\mathbf{c}\in C\\ \mathbf{c}\neq \mathbf{0}}}\sum_{\mathbf{z}\in D(c)}\prod_{i=1}^{k}\eta(\mathbf{z}+\mathbf{s}(\mathbf{c})+\mathbf{d_i})\eta(\mathbf{z}+\mathbf{s}(\mathbf{c})+\mathbf{c}+\mathbf{d_i}) \\
\leq& N^n+\sum_{\substack{\mathbf{c}\in C\\ \mathbf{c}\neq \mathbf{0}}}\left|\sum_{\mathbf{z}\in D(c)}\prod_{i=1}^{k}\eta(\mathbf{z}+\mathbf{s}(\mathbf{c})+\mathbf{d_i})\eta(\mathbf{z}+\mathbf{s}(\mathbf{c})+\mathbf{c}+\mathbf{d_i})\right|.
\end{aligned}
$$

Next we estimate $\left|\sum_{\mathbf{z}\in D(c)}\prod_{i=1}^{k}\eta(\mathbf{z}+\mathbf{s}(\mathbf{c})+\mathbf{d_i})\eta(\mathbf{z}+\mathbf{s}(\mathbf{c})+\mathbf{c}+\mathbf{d_i})\right|$ by $Q_{2k}(\eta)$ if the vectors $\mathbf{d_1},\mathbf{d_2},\dots,\mathbf{d_k}$, $\mathbf{c}+\mathbf{d_1},\mathbf{c}+\mathbf{d_2},\dots,\mathbf{c}+\mathbf{d_k}$ are all different. In the other case, when there are i and j for which $\mathbf{c}+\mathbf{d_i}=\mathbf{d_j}$, we will use the trivial estimate N^n. For every fixed i and j at most one $\mathbf{c}$ exists with $\mathbf{c}+\mathbf{d_i}=\mathbf{d_j}$, so we will use the trivial estimate only at most $k(k-1)$ times. Thus

$$S\leq N^n+|C|Q_{2k}(\eta)+k(k-1)N^n.$$

Since $|C|\leq 2^nN^n$ and $k(k-1)+1\leq k^2$ we get

$$S\leq \left(2^n+k^2\right)Q_{2k}(\eta)N^n,$$

which was to be proved.

3 Proof of Theorem 2

In order to prove Theorem 2 we will present a construction for which

$$N^{cn}\gg Q_k(\eta)\gg\sqrt{N^nC_{2k}(\eta)}\gg N^{cn}$$

holds. In our construction N will always be a prime, thus we change our notation, and we write p in place of N (primes usually are denoted by p). The construction will be based on finite fields and their generators. Namely, let $\mathbb{F}_{p^n}$ be a finite field with p^n elements, and let g be a generator element of $\mathbb{F}^*_{p^n}(=\mathbb{F}_{p^n}\setminus\{0\})$. Moreover, for $a\in\mathbb{F}^*_{p^n}$ define ind $a\in\mathbb{N}$ by

$$g^{\text{ind }a}=a \qquad \text{and} \qquad 0\le \text{ind } a<p^n-1.$$

Next $v_1,v_2,\dots,v_n$ will denote a fixed basis of the vector space $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. We define the binary lattice $\eta:\ I_p^n\to\{-1,+1\}$ by

$$\eta(x_1,x_2,\dots,x_n)=\begin{cases}1 & \text{if } 0\le \text{ind }(x_1v_1+x_2v_2+\dots+x_nv_n)\le L-1\\ -1 & \text{if } L\le\text{ind }(x_1v_1+x_2v_2+\dots+x_nv_n)<p^n-1\\ & \quad\text{or } (x_1,x_2,\dots,x_n)=(0,0,\dots,0),\end{cases} \tag{3.1}$$

where L is a positive integer with $1\le L\le p^n-1$ which will be defined later. We claim that for L optimally chosen we have

$$p^{cn}\gg Q_k(\eta)\gg\sqrt{p^nC_{2k}(\eta)}\gg p^{cn},$$

which proves the theorem. In order to estimate $Q_k(\eta)$ and $C_{2k}(\eta)$ we need the following lemma:

Lemma 3. *Consider the binary lattice η defined by* (3.1) *where L is a positive integer with $1\le L\le p^n-1$. Define H by $H\overset{def}{=}L-\frac{p^n-1}{2}$. let B be a box N-lattice (with $N=p$) and $\mathbf{d_1},\mathbf{d_2},\dots,\mathbf{d}_\ell\in I_N^n$ distinct vectors with $B+\mathbf{d_1},B+\mathbf{d_2},\dots,B+\mathbf{d}_\ell\subseteq I_N^n$. Then*

$$\left|\sum_{\mathbf{x}\in B}\eta(\mathbf{x}+\mathbf{d}_1)\eta(\mathbf{x}+\mathbf{d}_2)\cdots\eta(\mathbf{x}+\mathbf{d}_\ell)\right| \tag{3.2}$$
$$=\frac{2^\ell}{(p^n-1)^\ell}H^\ell\,|B|+O\left(\ell(4n)^\ell\sqrt{p^n}(1+\log p)^{n+\ell}\right).$$

In order to handle the sum in (3.2) we will use multiplicative characters over $\mathbb{F}_{p^n}$. First, we express $\eta(\mathbf{x})$ by character sums. We will apply the formula

$$\frac{1}{p^n-1}\sum_\chi\overline{\chi}(a)\chi(b)=\begin{cases}1 & \text{if } a=b\ne 0\\ 0 & \text{if } a\ne b \text{ or } a=b=0\end{cases},$$

where the sum runs over all multiplicative characters χ over $\mathbb{F}_{p^n}$ (and throughout this paper we use the convention $\chi(0) = 0$). By this formula for $\mathbf{x}(= (x_1, x_2, \ldots, x_n)) \neq \mathbf{0}$ we have

$$\begin{aligned}\eta(\mathbf{x}) &= 2 \sum_{\substack{0\le j\le L-1\\ j=\text{ind }(x_1v_1+\cdots+x_nv_n)}} 1 - 1 = \\ &= \frac{2}{p^n-1}\sum_{0\le j\le L-1}\sum_{\chi}\overline{\chi}(x_1v_1+\cdots+x_nv_n)\chi(g^j) - 1 \\ &= \frac{2}{p^n-1}\sum_{0\le j\le L-1}\sum_{\chi\neq\chi_0}\overline{\chi}(x_1v_1+\cdots+x_nv_n)\chi(g^j) + \frac{2H}{p^n-1}\end{aligned}$$

We will estimate the left hand side of (3.2). Write $\mathbf{d_i} = (d_i^{(1)}, d_i^{(2)}, \ldots, d_i^{(n)})$. Then for $\mathbf{x} \neq \mathbf{0}$ we have

$$\begin{aligned}&\eta(\mathbf{x}+\mathbf{d}_1)\eta(\mathbf{x}+\mathbf{d}_2)\cdots\eta(\mathbf{x}+\mathbf{d}_\ell) = \frac{2^\ell}{(p^n-1)^\ell}\cdot \\ &\cdot\prod_{i=1}^{\ell}\left(\sum_{j=0}^{L-1}\sum_{\chi\neq\chi_0}\overline{\chi}\left(\left(x_1+d_i^{(1)}\right)v_1+\cdots+\left(x_n+d_i^{(n)}\right)v_n\right)\chi(g^j)+H\right) \\ &= \frac{2^\ell}{(p^n-1)^\ell}\sum_{\{i_1,i_2\ldots,i_t\}\subset\{1,2,\ldots,\ell\}} H^{\ell-t}\sum_{\chi_{i_1}\neq\chi_0}\cdots\sum_{\chi_{i_t}\neq\chi_0} \\ &\overline{\chi_{i_1}}\left(\left(x_1+d_{i_1}^{(1)}\right)v_1+\cdots+\left(x_n+d_{i_1}^{(n)}\right)v_n\right)\cdots \\ &\overline{\chi_{i_t}}\left(\left(x_1+d_{i_t}^{(1)}\right)v_1+\cdots+\left(x_n+d_{i_t}^{(n)}\right)v_n\right)\times\prod_{j=1}^{t}\left(\sum_{r=0}^{L-1}\chi_{i_j}\left(g^r\right)\right).\end{aligned}$$

Here in the first sum of the right-hand side of the inequality we separate the term $t=0$:

$$\eta(\mathbf{x}+\mathbf{d}_1)\eta(\mathbf{x}+\mathbf{d}_2)\cdots\eta(\mathbf{x}+\mathbf{d}_\ell)=\frac{2^\ell}{(p^n-1)^\ell}H^\ell+$$
$$+\frac{2^\ell}{(p^n-1)^\ell}\sum_{\substack{\{i_1,i_2\dots,i_t\}\subset\{1,2,\dots,\ell\}\\ 1\le t\le \ell}}H^{\ell-t}\sum_{\chi_{i_1}\ne\chi_0}\cdots\sum_{\chi_{i_t}\ne\chi_0}$$
$$\overline{\chi_{i_1}}\left(\left(x_1+d_{i_1}^{(1)}\right)v_1+\dots+\left(x_n+d_{i_1}^{(n)}\right)v_n\right)\cdots$$
$$\overline{\chi_{i_t}}\left(\left(x_1+d_{i_t}^{(1)}\right)v_1+\dots+\left(x_n+d_{i_t}^{(n)}\right)v_n\right)\times\prod_{j=1}^{t}\left(\sum_{r=0}^{L-1}\chi_{i_j}\left(g^r\right)\right).$$

Next we consider the sum of those terms where $\mathbf{x}\in B$:

$$\sum_{\mathbf{x}\in B}\eta(\mathbf{x}+\mathbf{d}_1)\eta(\mathbf{x}+\mathbf{d}_2)\cdots\eta(\mathbf{x}+\mathbf{d}_\ell)=$$
$$=\frac{2^\ell}{(p^n-1)^\ell}H^\ell\,|B|+\frac{2^\ell}{(p^n-1)^\ell}\sum_{\substack{\{i_1,i_2\dots,i_t\}\subset\{1,2,\dots,\ell\}\\ 1\le t\le \ell}}H^{\ell-t}\sum_{\chi_{i_1}\ne\chi_0}\cdots\sum_{\chi_{i_t}\ne\chi_0}$$
$$\left(\sum_{\mathbf{x}\in B}\overline{\chi_{i_1}}\left(\left(x_1+d_{i}^{(1)}\right)v_1+\dots+\left(x_n+d_{i}^{(n)}\right)v_n\right)\cdots\right.$$
$$\left.\overline{\chi_{i_t}}\left(\left(x_1+d_{i}^{(1)}\right)v_1+\dots+\left(x_n+d_{i}^{(n)}\right)v_n\right)\right)\times\prod_{j=1}^{t}\left(\sum_{r=0}^{L-1}\chi_{i_j}\left(g^r\right)\right).$$

Using the triangle inequality we get that there exists a $-1\le\varepsilon\le 1$ such that

$$\sum_{\mathbf{x}\in B}\eta(\mathbf{x}+\mathbf{d}_1)\eta(\mathbf{x}+\mathbf{d}_2)\cdots\eta(\mathbf{x}+\mathbf{d}_\ell)=$$
$$=\frac{2^\ell}{(p^n-1)^\ell}H^\ell\,|B|+\varepsilon\frac{2^\ell}{(p^n-1)^\ell}\sum_{\substack{\{i_1,i_2\dots,i_t\}\subset\{1,2,\dots,\ell\}\\ 1\le t\le \ell}}H^{\ell-t}\sum_{\chi_{i_1}\ne\chi_0}\cdots\sum_{\chi_{i_t}\ne\chi_0}$$
$$\left|\sum_{\mathbf{x}\in B}\overline{\chi_{i_1}}\left(\left(x_1+d_{i_1}^{(1)}\right)v_1+\dots+\left(x_n+d_{i_1}^{(n)}\right)v_n\right)\cdots\right.$$
$$\left.\overline{\chi_{i_t}}\left(\left(x_1+d_{i_t}^{(1)}\right)v_1+\dots+\left(x_n+d_{i_t}^{(n)}\right)v_n\right)\right|\times\left|\prod_{j=1}^{t}\left(\sum_{r=0}^{L-1}\chi_{i_j}\left(g^r\right)\right)\right|. \quad (3.3)$$

The characters over $\mathbb{F}_q$ form a cyclic group, whose generator element will be denoted by χ_1. Fix $i_1, i_2, \ldots, i_t$ and consider the sum

$$\left| \sum_{\mathbf{x}\in B} \overline{\chi_{i_1}} \left(\left(x_1 + d_{i_1}^{(1)} \right) v_1 + \cdots + \left(x_n + d_{i_1}^{(n)} \right) v_n \right) \cdots \right.$$
$$\left. \overline{\chi_{i_t}} \left(\left(x_1 + d_{i_t}^{(1)} \right) v_1 + \cdots + \left(x_n + d_{i_t}^{(n)} \right) v_n \right) \right|$$

in (3.3). Here χ_{i_j} is of the form $\chi_{i_j} = \chi_1^{\alpha_j}$ where $(q-1) \nmid \alpha_j$. Moreover write

$$\begin{aligned} g(x_1v_1 + \cdots + x_nv_n) \stackrel{\text{def}}{=} & \left(x_1v_1 + \cdots + x_nv_n + d_{i_1}^{(1)} v_1 + \ldots d_{i_1}^{(n)} \right) v_n \\ & \cdot \left(x_1v_1 + \cdots + x_nv_n + d_{i_2}^{(1)} v_1 + \ldots d_{i_2}^{(n)} v_n \right) \\ & \vdots \\ & \cdot \left(x_1v_1 + \cdots + x_nv_n + d_{i_t}^{(1)} v_1 + \ldots d_{i_t}^{(n)} v_n \right) \end{aligned} \tag{3.4}$$

Then

$$\begin{aligned} & \overline{\chi_{i_1}} \left(\left(x_1 + d_{i_1}^{(1)} \right) v_1 + \cdots + \left(x_n + d_{i_1}^{(n)} \right) v_n \right) \cdots \\ & \overline{\chi_{i_t}} \left(\left(x_1 + d_{i_t}^{(1)} \right) v_1 + \cdots + \left(x_n + d_{i_t}^{(n)} \right) v_n \right) \\ & = \overline{\chi_1} \Bigg(\left(\left(x_1 + d_{i_1}^{(1)} \right) v_1 + \cdots + \left(x_n + d_{i_1}^{(n)} \right) v_n \right)^{\alpha_1} \cdots \\ & \left(\left(x_1 + d_{i_t}^{(1)} \right) v_1 + \cdots + \left(x_n + d_{i_t}^{(n)} \right) v_n \right)^{\alpha_t} \Bigg) \\ & = \overline{\chi_1} \Bigg(\left(x_1v_1 + \cdots + x_nv_n + v_1 d_{i_1}^{(1)} + \ldots v_n d_{i_1}^{(n)} \right)^{\alpha_1} \cdots \\ & \left(x_1v_1 + \cdots + x_nv_n + v_1 d_{i_t}^{(1)} + \ldots v_n d_{i_t}^{(n)} \right)^{\alpha_t} \Bigg) \\ & = \overline{\chi_1} \left(g(x_1v_x + \cdots + x_nv_n) \right). \end{aligned}$$

By this we get

$$\left| \sum_{\mathbf{x} \in B} \overline{\chi_{i_1}} \left(\left(x_1 + d_{i_1}^{(1)} \right) v_1 + \cdots + \left(x_n + d_{i_1}^{(n)} \right) v_n \right) \cdots \right.$$

$$\left. \overline{\chi_{i_t}} \left(\left(x_1 + d_{i_t}^{(1)} \right) v_1 + \cdots + \left(x_n + d_{i_t}^{(n)} \right) v_n \right) \right|$$

$$= \left| \sum_{\mathbf{x} \in B} \overline{\chi_1} \left(g(x_1 v_1 + \cdots + x_n v_n) \right) \right|. \tag{3.5}$$

Winterhof proved in [13] the following lemma:

Lemma 4. *Suppose that χ is a non-trivial multiplicative character of order d over the finite field $\mathbb{F}_q$, and $f(x)$ is a polynomial which is not of the form $ch(x)^d$, with $h(x) \in \mathbb{F}_q[x]$ and $f(x)$ has m distinct zeros in its splitting field $\mathbb{F}_q$. Then for $1 \le k_i \le p$; $i = 1, \dots, n$ let*

$$B = B(k_1, k_2, \dots, k_n) = \{x_1 v_1 + \cdots + x_n v_n : \ 0 \le x_i < k_i, \ i = 1, 2, \dots, n\}.$$

Then for any $1 \le k_i \le p$; $i = 1, 2, \dots, n$ we have

$$\left| \sum_{z \in B} \chi(f(z)) \right| < m q^{1/2} (1 + \log p)^n.$$

Next we will use Lemma 4 for the character χ_1 and the polynomial $g(x_1 v_1 + \cdots + x_n v_n)$. Here the order of the character χ_1 is $p^n - 1$ (> 1) and the polynomial $g(x_1 v_1 + \cdots + x_n v_n)$ defined in (3.4) has no multiple roots since the vectors $\mathbf{d_{i_1}}, \mathbf{d_{i_2}}, \dots, \mathbf{d_{i_t}}$ are different, thus it is not of the form

$ch(x)^d$ for any $d > 1$. Thus by Lemma 4 and (3.5) we get

$$\left|\sum_{\mathbf{x}\in B}\overline{\chi_{i_1}}\left(\left(x_1+d_{i_1}^{(1)}\right)v_1+\cdots+\left(x_n+d_{i_1}^{(n)}\right)v_n\right)\cdots\right.$$
$$\left.\overline{\chi_{i_t}}\left(\left(x_1+d_{i_t}^{(1)}\right)v_1+\cdots+\left(x_n+d_{i_t}^{(n)}\right)v_n\right)\right|$$
$$=\left|\sum_{\mathbf{x}\in B}\overline{\chi_1}\left(g(x_1v_1+\cdots+x_nv_n)\right)\right|$$
$$\leq t\sqrt{p^n}(1+\log p)^n$$
$$\leq \ell\sqrt{p^n}(1+\log p)^n.$$

Thus

$$\sum_{\mathbf{x}\in B}\eta(\mathbf{x}+\mathbf{d}_1)\eta(\mathbf{x}+\mathbf{d}_2)\cdots\eta(\mathbf{x}+\mathbf{d}_\ell)=$$
$$=\frac{2^\ell}{(p^n-1)^\ell}H^\ell|B|+O\left(\frac{2^\ell}{(p^n-1)^\ell}\sum_{\substack{\{i_1,i_2\dots,i_t\}\subset\{1,2,\dots,\ell\}\\ 1\leq t\leq \ell}}H^{\ell-t}\sum_{\chi_{i_1}\neq\chi_0}\cdots\sum_{\chi_{i_t}\neq\chi_0}\right.$$
$$\left.\ell\sqrt{p^n}(1+\log p)^n\times\left|\prod_{j=1}^{t}\left(\sum_{r=0}^{L-1}\chi_{i_j}(g^r)\right)\right|\right).$$

Here g is a generator of $\mathbb{F}_{p^n}^*$, thus if $\chi_{i_j}(g)=1$, then for every $a\in\mathbb{F}_{p^n}^*$ we have $\chi_{i_j}(a)=1$, which means that χ_{i_j} is the principal character. But this contradicts to $\chi_{i_j}\neq\chi_0$ so we get $\chi_{i_j}(g)\neq 1$. Then $\left|\sum_{r=0}^{L-1}\chi_{i_j}(g^r)\right| = \frac{\left|1-\chi_{i_j}(g)^L\right|}{\left|1-\chi_{i_j}(g)\right|}\leq\frac{2}{\left|1-\chi_{i_j}(g)\right|}$ so

$$\sum_{\mathbf{x}\in B}\eta(\mathbf{x}+\mathbf{d}_1)\eta(\mathbf{x}+\mathbf{d}_2)\cdots\eta(\mathbf{x}+\mathbf{d}_\ell)=\frac{2^\ell}{(p^n-1)^\ell}H^\ell|B|+$$
$$+O\left(\frac{\ell 2^\ell\sqrt{p^n}(1+\log p)^n}{(p^n-1)^\ell}\sum_{\substack{\{i_1,\dots,i_t\}\subset\{1,2,\dots,\ell\}\\ 1\leq t\leq\ell}}H^{\ell-t}\sum_{\chi_{i_1}\neq\chi_0}\cdots\sum_{\chi_{i_t}\neq\chi_0}\right.$$
$$\left.\prod_{j=1}^{t}\frac{2}{\left|1-\chi_{i_j}(g)\right|}\right).$$

Thus

$$\sum_{\mathbf{x}\in B}\eta(\mathbf{x}+\mathbf{d}_1)\eta(\mathbf{x}+\mathbf{d}_2)\cdots\eta(\mathbf{x}+\mathbf{d}_\ell)=$$

$$=\frac{2^\ell}{(p^n-1)^\ell}H^\ell\,|B|+O\left(\frac{\ell 2^\ell\sqrt{p^n}(1+\log p)^n}{(p^n-1)^\ell}\left(H+\sum_{\chi\neq\chi_0}\frac{2}{|1-\chi(g)|}\right)^\ell\right).$$

Now χ_1 is a generator of the group of characters over $\mathbb{F}_q$. More precisely, since g is a generator element of $\mathbb{F}^*_{p^n}$, we may define χ_1 by $\chi_1(g)=e^{2\pi i/(p^n-1)}$ (and $\chi(0)=0$). Then

$$\begin{aligned}\sum_{\chi\neq\chi_0}\frac{1}{|1-\chi(g)|}&=\sum_{j=1}^{p^n-2}\frac{1}{|1-\chi^j(g)|}=\sum_{j=1}^{p^n-2}\frac{1}{|1-e^{2\pi ij/(p^n-1)}|}\\&\leq\frac{1}{4}\sum_{j=1}^{p^n-2}\frac{1}{||j/(p^n-1)||}\leq\frac{1}{2}\sum_{j=1}^{(p^n-1)/2}\frac{1}{||j/(p^n-1)||}\\&=\frac{1}{2}\sum_{j=1}^{(p^n-1)/2}\frac{p^n-1}{j}<\frac{1}{2}(p^n-1)(1+\log(p^n/2))\\&<n(p^n-1)\log p^n.\end{aligned}$$

Thus

$$\sum_{\mathbf{x}\in B}\eta(\mathbf{x}+\mathbf{d}_1)\eta(\mathbf{x}+\mathbf{d}_2)\cdots\eta(\mathbf{x}+\mathbf{d}_\ell)=$$

$$=\frac{2^\ell}{(p^n-1)^\ell}H^\ell\,|B|+O\left(\frac{\ell 2^\ell\sqrt{p^n}(1+\log p)^n}{(p^n-1)^\ell}\left(H+n(p^n-1)\log p\right)^\ell\right).$$

Now we fix the value of L as $L=\frac{p^n-1}{2}+\left[p^{1-(1-c)/n}\right]$ so that $H=\left[p^{1-(1-c)/n}\right]$. Then $H<n(p^n-1)\log p$, thus

$$\begin{aligned}&\sum_{\mathbf{x}\in B}\eta(\mathbf{x}+\mathbf{d}_1)\eta(\mathbf{x}+\mathbf{d}_2)\cdots\eta(\mathbf{x}+\mathbf{d}_\ell)=\\&=\frac{2^\ell}{(p^n-1)^\ell}H^\ell\,|B|+O\left(\frac{\ell 2^\ell\sqrt{p^n}(1+\log p)^n}{(p^n-1)^\ell}\left(2n(p^n-1)\log p\right)^\ell\right)\\&=\frac{2^\ell}{(p^n-1)^\ell}H^\ell\,|B|+O\left(\ell(4n)^\ell\sqrt{p^n}\,(1+\log p)^{n+\ell}\right).\end{aligned}$$

The maximum value of $|B|$ is $p^n - 1$, thus

$$Q_k(\eta) = \frac{2^k}{(p^n-1)^{k-1}} H^k + O\left(k \cdot (4n)^k \sqrt{p^n}\,(1+\log p)^{n+k}\right)$$
$$C_{2k}(\eta) = \frac{2^{2k}}{(p^n-1)^{2k-1}} H^{2k} + O\left(2k \cdot (4n)^{2k} \sqrt{p^n}\,(1+\log p)^{n+2k}\right).$$

Using $\frac{H^k}{(p^n-1)^k} > O\left(k \cdot (4n)^k \sqrt{p^n}(1+\log p)^{n+k}\right)$
and $\frac{H^{2k}}{(p^n-1)^{2k}} > O\left(2k \cdot (4n)^{2k} \sqrt{p^n}(1+\log p)^{n+2k}\right)$ if $c > 3/4$ and p is large enough, we get

$$Q_k(\eta) \leq \frac{2^k+1}{(p^n-1)^{k-1}} H^k$$
$$C_{2k}(\eta) \geq \frac{2^{2k}-1}{(p^n-1)^{2k-1}} H^{2k}.$$

By $H = [p^{n(1-(1-c)/k)}]$, it follows from these inequalities that

$$p^{cn} \gg Q_k(\eta) \gg \sqrt{p^n C_{2k}(\eta)} \gg p^{cn},$$

which was to be proved.

References

[1] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, *Measures of pseudorandomness for finite sequences: minimal values*, Combin., Probab. Comput. 15 (2005), 1-29.

[2] J. Cassaigne, C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences VII: The measures of pseudorandomness*, Acta Arith. 103 (2002), 97-118.

[3] K. Gyarmati, *An inequality between the measures of pseudorandomness*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 46 (2003), 157-166.

[4] K. Gyarmati, *Measures of pseudorandomness*, P. Charpin, A. Pott, A. Winterhof (eds.), Radon Series in Computational and Applied Mathematics, de Gruyter (2013), 43-64.

[5] K. Gyarmati, C. Mauduit, A. Sárközy, *Measures of pseudorandomness of finite binary lattices*, III (Q_k, correlation, normality, minimal values.), Unif. Distrib. Theory 5 (2010), 183-207.

[6] K. Gyarmati, A. Sárközy and C. Stewart, *On Legendre symbol lattices*, Unif. Distri. Theory 4 (2009), no. 1, 81-95.

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

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

[9] C. Mauduit and A. Sárközy, *On the measures of pseudorandomness of binary sequences*, Discrete Math. 271 (2003), 195-207.

[10] A. Sárközy, *On pseudorandomness of families of binary sequences*, Discrete Applied Math. 216 (2017), 670-676.

[11] R. Sebők, *On a connection between pseudorandom measures*, Unif. Distrib. Theory 10 (2015), 107-113.

[12] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Act. Sci. Ind. 1041, Hermann, Paris, (1948).

[13] A. Winterhof, *Some estimates for character sums and applications*, Des. Codes and Cryptogr. 22, (2001). 123-131.