ON PSEUDORANDOM BINARY LATTICES

by
P. Hubert, C. Mauduit
Institut de Mathématiques de Luminy
CNRS, UMR 6206
163, avenue de Luminy, Case 907
F–13288 Marseille Cedex 9, France

and
A. Sárközy
Eötvös Loránd University
Department of Algebra and Number Theory
H–1117 Budapest, Pázmány Péter sétány 1/C
Hungary

1 Introduction

Recently in a series of papers a new constructive approach has been developed to study pseudorandomness of binary sequences

\[ E_N = \{e_1, e_2, \ldots, e_N\} \in \{-1, +1\}^N. \]

In particular, in [3] Mauduit and Sárközy first introduced the following measures of pseudorandomness: the well-distribution measure of \( E_N \) is defined by

\[ W(E_N) = \max_{u,b,t} \left| \sum_{j=0}^{t-1} e_{u+jb} \right|. \]
where the maximum is taken over all \( a, b, t \in \mathbb{N} \) such that \( 1 \leq a \leq a + (t - 1)b \leq N \), and the correlation measure of order \( k \) of \( E_N \) is defined as
\[
C_k(E_N) = \max_{M, D} \left| \sum_{n=1}^{M} \epsilon_{n+D_1} \epsilon_{n+D_2} \cdots \epsilon_{n+D_k} \right|
\]
where the maximum is taken over all \( D = (d_1, \ldots, d_k) \) and \( M \) such that \( 0 \leq d_1 < \cdots < d_k \leq N - M \). (The combined well-distribution-correlation) pseudorandom measure of order \( k \) was also introduced:
\[
Q_k(E_N) = \max_{a, b, t, D} \left| \sum_{j=0}^{t} \epsilon_{a+jb+D_1} \epsilon_{a+jb+D_2} \cdots \epsilon_{a+jb+D_k} \right|
\]
where the maximum is defined for all \( a, b, t \) and \( D = (d_1, \ldots, d_k) \) such that all the subscripts \( a + jb + d_\ell \) belong to \( \{1, 2, \ldots, N\} \). However, later this measure was not used.) Then the sequence \( E_N \) is considered as a “good” pseudorandom sequence if both these measures \( W(E_N) \) and \( C_k(E_N) \) (at least for “small” \( k \)) are “small” in terms of \( N \) (in particular, both are \( o(N) \) as \( N \to \infty \)). Indeed, later Cassaigne, Mauduit and Sárközy [2] showed that this terminology is justified since for almost all \( E_N \in \{-1, +1\}^N \), both \( W(E_N) \) and \( C_k(E_N) \) are less than \( N^{1/2}(\log N)^c \). (See also [1].) It was also shown in [3] that the Legendre symbol forms a “good” pseudorandom sequence. Later several further sequences were tested for pseudorandomness, and further constructions were given for sequences with good pseudorandom properties. In some other papers the measures of pseudorandomness were studied.

In this paper our goal is to extend this theory to several dimensions. First in Section 2 we will formulate the problem and introduce the measures of pseudorandomness. In Section 3 we will study these measures in the “truly random” case. Finally, in Section 4 we will present a construction which is “good” in terms of these new measures of pseudorandomness.

## 2 Formulating the problem in several dimensions and introducing the new measures

Let \( I^n_N \) denote the set of the \( n \)-dimensional vectors all whose coordinates are selected from the set \( \{0, 1, \ldots, N - 1\} \):
\[
I^n_N = \{ \mathbf{x} = (x_1, \ldots, x_n) : x_1, \ldots, x_n \in \{0, 1, \ldots, N - 1\} \}.
\]
This set forms a (truncated) \( n \)-dimensional lattice thus we may call it \( n \)-dimensional \( N \)-lattice or briefly (if \( n \) is fixed) \( N \)-lattice. Then the binary sequences of form (1.1) can be considered as functions of type
\[
e_{\mathbf{x}} = \eta(\mathbf{x}) : I^n_N \to \{-1, +1\}.
\]
Thus clearly the natural $n$-dimensional extension of the problem of the pseudorandomness of binary sequences of form (1.1), i.e., of functions (2.1) is to study the pseudorandomness of functions of type

$$\eta(x): I^n_N \to \{-1, +1\}. \tag{2.2}$$

Such a function can be visualized as the lattice points of the $N$-lattice replaced by the two symbols $+$ and $-$, thus we may call them binary $N$-lattices or briefly binary lattices.

In order to introduce the measures of pseudorandomness of binary lattices one might like to adopt the one-dimensional definitions. However, there is a slight difficulty in doing this, namely, the $n$-dimensional $N$-lattice $I^n_N$ has a natural ordering in one dimension but not in higher dimensions. This fact explains that while the well-distribution measure can be generalized easily, it is not so in case of the correlation, so that instead of starting out from it, we will start out from the combined measure (1.3). We propose to use the following measures of pseudorandomness:

If $\eta = \eta(x)$ is an $n$-dimensional binary $N$-lattice of form (2.2), $k \in \mathbb{N}$, and $u_i (i = 1, 2, \ldots, n)$ denotes the $n$-dimensional unit vector whose $i$-th coordinate is 1 and the other coordinates are 0, then write

$$C_k(\eta) = \max_{B, d_1, \ldots, d_k, T} \left| \sum_{j_1=0}^{t_1} \cdots \sum_{j_n=0}^{t_n} \eta(j_1b_1u_1 + \cdots + j_n b_n u_n + d_1) \right| \cdots \left| \eta(j_1b_1u_1 + \cdots + j_n b_n u_n + d_k) \right| \tag{2.3}$$

where the maximum is taken over all $n$-dimensional vectors $B = (b_1, \ldots, b_n)$, $d_1, \ldots, d_k$, $T = (t_1, \ldots, t_n)$ such that their coordinates are non-negative integers, $b_1, \ldots, b_n$ are non-zero, $d_1, \ldots, d_k$ are distinct, and all the points $j_1b_1u_1 + \cdots + j_n b_n u_n + d_i$ occurring in the multiple sum belong to the $n$-dimensional $N$-lattice $I^n_N$. We will call $C_k(\eta)$ the pseudorandom (briefly PR) measure of order $k$ of $\eta$.

Note that in the one-dimensional special case $C_1(\eta)$ is the same as the well-distribution measure (1.2), and for every $k \in \mathbb{N}$, $C_k(\eta)$ is the combined measure (1.3). Then a binary $N$-lattice $\eta$ is considered as a “good” pseudorandom binary lattice if the PR measure of order $k$ of $\eta$ is “small” in terms of $N$ (in particular, $C_k(\eta) = o(N^n)$ as $N \to \infty$) for small $k$. This terminology will be justified by Theorem 1 in the next section.

3 The pseudorandom measures for truly random binary lattices

In this section we will estimate $C_k(\eta)$ for a truly random binary lattice. More precisely, assume that $N \in \mathbb{N}$, $n \in \mathbb{N}$, write $Z = |I^n_N| = N^n$, denote the elements of $I^n_N$ by $x_1, x_2, \ldots, x_Z$, and then choose each of the binary lattices $\eta$ of form
(2.2) with the same probability $2^{-Z}$, i.e., define $\eta$ so that $\eta(x_1), \eta(x_2), \ldots, \eta(x_Z)$ are independent random variables with

$$ P(\eta(x_i) = +1) = P(\eta(x_i) = -1) = \frac{1}{2}. $$

We will prove:

**Theorem 1.** If $k \in \mathbb{N}$ and $\varepsilon > 0$, then there are numbers $N_0 = N_0(k, \varepsilon)$ and $\delta = \delta(k, \varepsilon) > 0$ such that for $N > N_0$ we have

$$ P(C_k(\eta) > \delta N^{n/2}) > 1 - \varepsilon \quad \text{and} \quad P(C_k(\eta) > (KN^n \log N^n)^{1/2}) < \varepsilon, $$

where $K = 81k$.

**Proof of Theorem 1.** If $k = 1$, then (3.2) follows from

$$ P(C_k(\eta) > \delta N^{n/2}) > P \left( \left| \sum_{j_1=0}^{N-1} \cdots \sum_{j_n=0}^{N-1} \eta(j_1 u_1 + \cdots + j_n u_n) \right| > \delta N^{n/2} \right) $$

$$ = P \left( \left| \sum_{i=1}^{N^n} \eta(x_i) \right| > \delta N^{n/2} \right), $$

(3.1) and the central limit theorem.

If $k \geq 2$, then consider the $n$-fold sum in the definition of $C_k(\eta)$ in (2.3) with $t_1 = \lceil \frac{N}{2k} \rceil - 1$, $t_2 = \cdots = t_n = N - 1$, $b_1 = k$, $b_2 = \cdots = b_n = 1$, $d_i = (i-1)u_1$ for $i = 1, 2, \ldots, k - 1$ and $d_k = \lceil N/2 \rceil u_1$. Then clearly, for $0 \leq j_1 \leq t_1, \ldots, 0 \leq j_n \leq t_n$, $1 \leq i \leq k$ we have

$$ j_1 b_1 u_1 + \cdots + j_n b_n u_n + d_i \in I_N^k $$

thus, indeed, this sum

$$ S = \sum_{j_1=0}^{t_1} \cdots \sum_{j_n=0}^{t_n} \eta(j_1 b_1 u_1 + \cdots + j_n b_n u_n + d_i) \cdots $$

$$ \cdots \eta(j_1 b_1 u_1 + \cdots + j_n b_n u_n + d_k) $$

is considered in the maximum in (2.3). Moreover, it is easy to see that for distinct $(n+1)$-tuples $(j_1, \ldots, j_n, i)$ we obtain different vectors $j_1 b_1 u_1 + \cdots + j_n b_n u_n + d_i$, thus all the factors $\eta(\ldots)$ in this sum are independent random variables of type (3.1). Now fixing the values of the first $k-1$ random variables $\eta$ in each term in $S$ and denoting the vectors $j_1 b_1 u_1 + \cdots + j_n b_n u_n + d_k$ in $S$ by $v_1, \ldots, v_{(t_1+1)\cdots(t_n+1)}$, we get a sum of form

$$ S' = \sum_{1 \leq i \leq (t_1+1)\cdots(t_n+1)} c_i \eta(v_i) $$

4
where \( e_\ell \in \{-1, +1\} \) for each \( \ell \). Writing \( \xi_\ell = e_\ell \eta(\nu_\ell) \), this becomes

\[
S' = \sum_{1 \leq \ell \leq \lfloor N/2k \rfloor N^{n-1}} \xi_\ell
\]

where the \( \xi_\ell \)'s are independent random variables which are also of distribution

\[
P(\xi_\ell = +1) = P(\xi_\ell = -1) = \frac{1}{2}.
\]

By the central limit theorem, there are \( N_0 = N_0(k, \varepsilon) \) and \( \delta = \delta(k, \varepsilon) > 0 \) such that

\[
P(|S'| > \delta N^{n/2}) = P\left( \left| \sum_{1 \leq \ell \leq \lfloor N/2k \rfloor N^{n-1}} \xi_\ell \right| > \delta N^{1/2} \right) > 1 - \varepsilon.
\]

This is so under the condition that certain random variables \( \eta(\ldots) \) in \( S \) are fixed as described above, and this holds uniformly for any fixed \( \eta(\ldots) \) values which implies (3.2).

In order to prove (3.3), we will need the following lemma:

**Lemma 1.** Let \( r, k, M, Z \in \mathbb{N} \). Assume that \( E_Z = \{e_1, e_2, \ldots, e_Z\} \) is a set of independent random variables of type (3.1), i.e.,

\[
P(e_i = +1) = P(e_i = -1) = \frac{1}{2}.
\]

Assume also that \( y_1, y_2, \ldots, y_M \) are random variables of form

\[
y_\ell = e_{i(\ell, 1)} e_{i(\ell, 2)} \cdots e_{i(\ell, k)} \quad \text{for } \ell = 1, 2, \ldots, M
\]

where

\[
i(\ell, j) \in \{1, 2, \ldots, Z\} \quad \text{for } 1 \leq \ell \leq M, \quad 1 \leq j \leq k,
\]

\[
i(\ell, j_1) \neq i(\ell, j_2) \quad \text{for } 1 \leq \ell \leq M, \quad 1 \leq j_1 < j_2 \leq k
\]

and

\[
i(\ell, 1) \neq i(\ell + j, m) \quad \text{for } 1 \leq \ell \leq M, \quad 1 \leq j \leq M - \ell, \quad 1 \leq m \leq k
\]

Then we have

\[
E\left( \left( \sum_{n=1}^{M} y_n \right)^{2r} \right) \leq 2^{1-M} \sum_{h=0}^{[M/2]} \binom{M}{h} (M - 2h)^{2r}.
\]

(\( E(\xi) \) denotes the expectation of the random variable \( \xi \).)
Proof of Lemma 1. Both the proof of the lemma and the completion of the proof of (3.3) are similar to the proof of the upper bound in Theorem 2 in [2], thus we will omit some details. However, there is a significant difference: while in the one-dimensional case we may use the natural ordering of the positive integers, here in the several dimensional case there is no natural ordering, thus we have to introduce and use an artificial one which leads to certain complications (in particular, this fact explains the role of condition (3.8) in the lemma).

By the multinomial theorem we have

\[
E \left( \sum_{n=1}^{M} y_n \right)^{2r} = E \left( \sum_{t=1}^{2r} \sum_{i_1 < \cdots < i_t \leq M} \sum_{j_1 + \cdots + j_t = 2r} \frac{(2r)!}{j_1! \cdots j_t!} y_{i_1}^{j_1} \cdots y_{i_t}^{j_t} \right) 
\]

\[
= \sum_{t=1}^{2r} \sum_{i_1 < \cdots < i_t \leq M} \sum_{j_1 + \cdots + j_t = 2r} \frac{(2r)!}{j_1! \cdots j_t!} E(y_{i_1}^{j_1} \cdots y_{i_t}^{j_t}). 
\]

Observe that for each \( i \) we have \( y_i \in \{-1, +1\} \), thus the value of \( y_i^j \) depends only on the parity of \( j \): \( y_i^j = 1 \) if \( j \) is even and \( y_i^j = y_i \) if \( j \) is odd. Let \( \sum_1 \) denote the contribution of those terms for which at least one of \( j_1, \ldots, j_t \) is odd, and let \( \sum_2 \) denote the contribution of the terms such that each of \( j_1, \ldots, j_t \) is even so that

\[
(3.10) \quad E \left( \sum_{n=1}^{M} y_n \right)^{2r} = \sum_1 + \sum_2. 
\]

In \( \sum_1 \) in each term the last factor can be replaced by a factor of form

\[ E(y_{s_1} \cdots y_{s_u}) \text{ with } s_1 < \cdots < s_u. \]

By (3.5) here we may replace each \( y_{s_h} \) by \( e_{i(s_h,1)}e_{i(s_h,2)} \cdots e_{i(s_h,k)} \). Then by conditions (3.7) and (3.8), \( e_{i(s_h,1)} \) occurs only once. Thus \( y_{s_1} \cdots y_{s_u} \) can be rewritten as

\[ y_{s_1} \cdots y_{s_u} = e_{i(s_1,1)}e_{v_1} \cdots e_{v_p} \text{ with } i(s_1,1) \neq v_j \text{ for } 1 \leq j \leq p. \]

\( e_1, e_2, \ldots, e_Z \) are independent random variables with expectation 0 (by (3.4)), thus we have

\[ E(y_{s_1} \cdots y_{s_u}) = E(e_{i(s_1,1)})E(e_{v_1}) \cdots E(e_{v_p}) = 0. \]

It follows that

\[
(3.11) \quad \sum_1 = 0.
\]

In \( \sum_2 \) we may replace each \( j_i \) by \( 2q_i \):

\[
\sum_2 = \sum_{t=1}^{2r} \sum_{1 \leq i_1 < \cdots < i_t \leq M} \sum_{q_1 + \cdots + q_t = r} \frac{(2r)!}{(2q_1)! \cdots (2q_t)!} E(y_{i_1}^{2q_1} \cdots y_{i_t}^{2q_t}) = 
\]

6
\[= \sum_{t=1}^{2r} \sum_{i_1 \leq \cdots \leq i_t \leq M} \sum_{q_1 + \cdots + q_t = r} \frac{(2r)!}{(2q_1)! \cdots (2q_t)!} \mathbb{E}(1) = \]

\[= \sum_{t=1}^{2r} \sum_{i_1 \leq \cdots \leq i_t \leq M} \sum_{q_1 + \cdots + q_t = r} \frac{(2r)!}{(2q_1)! \cdots (2q_t)!}. \]

This triple sum was computed in [2, p. 104], and we obtained

(3.12) \[\sum_{t=2}^{2r} 2^{1-M} \sum_{h=0}^{[M/2]} \binom{M}{h} (M - 2h)^{2r}.\]

(3.9) follows from (3.10), (3.11) and (3.12), and this completes the proof of Lemma 1.

We will complete the proof of (3.3) by using the moment method. Write \(D = (d_1, \ldots, d_k), \ B = (b_1, \ldots, b_n), \ T = (t_1, \ldots, t_n),\)

(3.13) \[V(\eta, B, D, T) = \sum_{j_1=0}^{t_1} \cdots \sum_{j_n=0}^{t_n} \eta(j_1 b_1 u_1 + \cdots + j_n b_n u_n + d_1) \cdots \]

\[\cdots \eta(j_1 b_1 u_1 + \cdots + j_n b_n u_n + d_k)\]

and

\[S(r) = \mathbb{E} \left( \sum_{B} \sum_{D} \sum_{T} (V(\eta, B, D, T))^{2r} \right) = \]

\[\sum_{B} \sum_{D} \sum_{T} \mathbb{E} \left( (V(\eta, B, D, T))^{2r} \right)\]

where \(r = r(k, Z) \in \mathbb{N}\) will be fixed later and the triple sum is taken over all \(B, D, T\) considered in (2.3).

For a fixed sum \(V(\eta, B, D, T)\) denote the number of its terms by \(M\), i.e., let

\[M = t_1 t_2 \cdots t_n,\]

and split \(S(r)\) in two parts: let \(S_1(r)\) denote the contribution of the terms with \(M \leq Z^{1/4}\) and let \(S_2(r)\) be the contribution of the terms with

(3.14) \[Z^{1/4} < M \leq Z\]

so that

(3.15) \[S(r) = S_1(r) + S_2(r).\]

First we will estimate \(S_1(r)\). Clearly we have

\[|V(\eta, B, D, T)| \leq \sum_{j_1=0}^{t_1} \cdots \sum_{j_n=0}^{t_n} 1 = M\]
whence
\[ S_1(r) \leq \sum_B \sum_D \sum_T M^{2r} = M^{2r} \sum_B \sum_D \sum_T 1. \]
Here \( B = (b_1, \ldots, b_n) \) can be chosen in at most \( N^n = Z \) ways, \( D = (d_1, \ldots, d_k) \) in \( |I_N|^k = Z^k \) ways and \( T = (t_1, \ldots, t_n) \) in \( N^n = Z \) ways so that, by the definition of \( S_1(r) \),
\[(3.16) \quad S_1(r) \leq M^{2r} \cdot Z \cdot Z^k \cdot Z \leq Z^{r/2+k+2}.\]

In order to estimate \( S_2(r) \) we will use Lemma 1. \( S_2(r) \) is a triple sum (over \( B, D, T \)) whose general term is
\[(3.17) \quad E \left( (V(\eta, B, d, T))^{2r} \right) = E \left( \left( \sum_{j_1=0}^{t_1} \cdots \sum_{j_n=0}^{t_n} \eta(j_1b_1u_1 + \cdots + j_nb_nu_n + d_1) \cdots \eta(j_1b_1u_1 + \cdots + j_nb_nu_n + d_k) \right)^{2r} \right) \]
with \( M = t_1t_2\ldots t_n \) satisfying (3.14). This expression is of the type considered in (3.9) in Lemma 1, but to ensure that (3.8) in the lemma holds first we have to change the order of the terms in this \( n \)-fold sum. We will introduce and use an ordering of \( I_N \). Indeed, we will use the ordering of \( I_N \) which is sometimes called “the graduated lexicographic ordering” and is defined in the following way: if \((a_1, \ldots, a_n), (b_1, \ldots, b_n) \in I_N\) then we say that \((a_1, \ldots, a_n) < (b_1, \ldots, b_n)\) if and only if either \(a_1 + \cdots + a_n < b_1 + b_2 + \cdots + b_n\) or \(a_1 + \cdots + a_n = b_1 + \cdots + b_n\) and \((a_1, \ldots, a_n)\) is less than \((b_1, \ldots, b_n)\) in terms of the lexicographic order.

This “graduated lexicographic ordering” possesses the following fundamental property:
\[(3.18) \quad \text{if } (a_1, \ldots, a_n) < (b_1, \ldots, b_n), \text{ then } (a_1 + c_1, \ldots, a_n + c_n) < (b_1 + c_1, \ldots, b_n + c_n) \text{ for all } (c_1, \ldots, c_n) \in I_N.\]

Now we reorder the vectors \( j_1b_1u_1 + \cdots + j_nb_nu_n \) (with \(1 \leq j_1 \leq t_1, \ldots, 1 \leq j_n \leq t_n\)) so that they should follow each other in increasing order in terms of the “graduated lexicographic ordering”; denote them by
\[(3.19) \quad v_1 < \cdots < v_M.\]

Moreover, the vectors \( d_1, \ldots, d_k \) play a symmetric role thus we may assume without the loss of generality that
\[(3.20) \quad d_1 < \cdots < d_k.\]

Then (3.17) can be rewritten as
\[ E \left( (V(\eta, B, d, T))^{2r} \right) = E \left( \left( \sum_{i=1}^{M} \eta(v_i + d_1) \cdots \eta(v_i + d_k) \right)^{2r} \right). \]
Now we use Lemma 1 with $E_Z = \{e_1, \ldots, e_Z\} = \{\eta(x_1), \ldots, \eta(x_Z)\}$, $y_\ell = \eta(v_\ell + d_1) \ldots \eta(v_\ell + d_k)$ (for $\ell = 1, \ldots, M$), $e_{(\ell, j)} = \eta(v_\ell + d_j)$ (for $1 \leq \ell \leq M$, $1 \leq j \leq k$). Then (3.4), (3.5) and (3.6) in Lemma 1 hold trivially, (3.7) and (3.8) hold by (3.18), (3.19) and (3.20), thus the lemma can be applied. We obtain

\[(3.21) \quad E((V(\eta, B, d, T))^{2r}) \leq 2^{1-M} \sum_{h=0}^{[M/2]} \binom{M}{h} (M - 2h)^{2r}.\]

Now we fix the value of $r$: let $r = [2k \log Z]$.

Then as in [2, pp. 104–105], it follows from (3.21) that

$E((V(\eta, B, d, T))^{2r}) < 4M(4rM)^r$ for $Z^{1/4} < M \leq Z$

whence

\[(3.22) \quad S_2(r) < \sum_B \sum_D \sum_T 4M(4rM)^r \leq \sum_B \sum_D \sum_T 4Z(4rZ)^r = 4Z(4rZ)^r \sum_B \sum_D \sum_T 1.

Here $B = (b_1, \ldots, b_n)$ can be chosen in at most $N^n = Z$ ways, $D = (d_1, \ldots, d_k)$ in $(N^n)^k = Z^k$ ways, $T = (t_1, \ldots, t_n)$ in $N^n = Z$ ways, thus we get from (3.22) that

\[(3.23) \quad S_2(r) < 4Z^{k+3}(4rZ)^r.

It follows from (3.15), (3.16) and (3.23) that

\[(3.24) \quad S(r) < Z^{r/2+k+2} + 4Z^{k+3}(4rZ)^r < 5Z^{k+3}(4rZ)^r.

On the other hand, writing $X = 9(kZ \log Z)^{1/2} = (81kN^n \log N^n)^{1/2}$, clearly we have

\[(3.25) \quad S(r) = E\left(\sum_B \sum_D \sum_T (V(\eta, B, D, T))^{2r}\right) \geq \sum_B \sum_D \sum_T (\max_{B,D,T} |V(\eta, B, D, T)|)^{2r} \geq \sum_B \sum_D \sum_T (C_k(\eta))^{2r} \geq P(C_k(\eta) > X)X^{2r}.

It follows from (3.24) and (3.25) that

$P(C_k(\eta) > X) < 5Z^{k+3}(4rZX^{-2})^r = 5Z^{k+3}(4[2k \log Z]X^{-2})^r \leq 5Z^{k+3}\left(\frac{8}{81}\right)^r = 5 \exp\left((k + 3) \log Z - [2k \log Z] \log \frac{81}{8}\right).

If $N$ and thus also $Z$ is large enough in terms of $\varepsilon$, then this upper bound is less than $\varepsilon$, and this completes the proof of Theorem 1. \[\square\]
4 A construction

In this section we will present a construction where good upper bounds can be given for the pseudorandom measures introduced in Section 2. We will use the following notations: We write $e(\alpha) = e^{2\pi i \alpha}$, $p$ will denote an odd prime, $n \in \mathbb{N}$, $q = p^n$, and the quadratic character of $\mathbb{F}_q$ will be denoted by $\gamma$. Consider the linear vector space formed by the elements of $\mathbb{F}_q$ over $\mathbb{F}_p$, and let $v_1, v_2, \ldots, v_n$ be a basis of this vector space, i.e., assume that $v_1, v_2, \ldots, v_n$ are $n$ linearly independent elements of $\mathbb{F}_q$ over $\mathbb{F}_p$. Then define the mapping $\eta(x)$ of type $\eta(x) : I^n \rightarrow \{-1, +1\}$ by

\[
\eta(x) = \eta((x_1, x_2, \ldots, x_n)) = \begin{cases} 
\gamma(x_1v_1 + x_2v_2 + \cdots + x_nv_n) & \text{for } (x_1, x_2, \ldots, x_n) \neq (0, 0, \ldots, 0) \\
1 & \text{for } (x_1, x_2, \ldots, x_n) = (0, 0, \ldots, 0)
\end{cases}
\]

for any $x_1, x_2, \ldots, x_n \in \mathbb{F}_p$.

**Theorem 2.** If $p$ is a prime, $n \in \mathbb{N}$, $k \in \mathbb{N}$ and the $n$-dimensional binary $p$-lattice is defined by (4.1), then we have

\[
C_k(\eta) < kq^{1/2}(1 + \log p)^n.
\]

(Note that by Theorem 1, for fixed $n$ this upper bound is greater than the value of $C_k(\eta)$ for a truly random $\eta$ by at most a logarithm power.)

**Proof of Theorem 2.** We will need the following result of Winterhof:

**Lemma 2.** If $P, n, q, v_1, v_2, \ldots, v_n$ are defined as above, $\chi$ is a multiplicative character of $\mathbb{F}_q$ of order $d > 1$, $\mathbb{F}_q[x]$ is a nonconstant polynomial which is not a $d$-th power and which has $m$ distinct zeros in its splitting field over $\mathbb{F}_q$, and $k_1, \ldots, k_n$ are positive integers with $k_1 \leq p, \ldots, k_n \leq p$, then, writing $B = \left\{ \sum_{i=1}^{n} j_i v_i : 0 \leq j_i < k_i \right\}$, we have

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

**Proof of Lemma 2.** This is a part of Theorem 2 in [5] (where its proof was based on A. Weil’s theorem [4]).

Now consider a multiple sum of the type occurring in (2.3) with $d_i = (d_{1i}, \ldots, d_{ni})$ (for $i = 1, \ldots, k$):

\[
S = \sum_{j_1=0}^{t_1} \cdots \sum_{j_n=0}^{t_n} \eta(j_1b_1u_1 + \cdots + j_nb_nu_n + d_1)
\]
\[ \ldots \eta(j_1 b_1 u_1 + \cdots + j_n b_n u_n + d_k) = \]
\[ \sum_{j_1 = 0}^{t_1} \cdots \sum_{j_n = 0}^{t_n} \eta((j_1 b_1 + d^{(1)}_1, \ldots, j_n b_n + d^{(1)}_n)) \]
\[ \ldots \eta((j_1 b_1 + d^{(k)}_1, \ldots, j_n b_n + d^{(k)}_n)) \]

whence, by (4.1) and the multiplicativity of \( \gamma \),
\[
(4.3) \quad S = \sum_{j_1 = 0}^{t_1} \cdots \sum_{j_n = 0}^{t_n} \gamma((j_1 b_1 v_1 + \cdots + j_n b_n v_n) + (d^{(1)}_1 v_1 + \cdots + d^{(1)}_n v_n)) \\
\ldots \gamma((j_1 b_1 v_1 + \cdots + j_n b_n v_n) + (d^{(k)}_1 v_1 + \cdots + d^{(k)}_n v_n)) \\
= \sum_{Z \in B'} \gamma((z + z_1) \cdots (z + z_k)) = \sum_{Z \in B'} \gamma(f(z))
\]

with
\[
(4.4) \quad B' = \left\{ \sum_{i=1}^{n} j_i (b_i v_i) : 0 \leq j_i < t_i + 1 \right\},
\]
\[
(4.5) \quad z_i = d^{(i)}_1 v_1 + \cdots + d^{(i)}_n v_n \quad \text{(for } i = 1, \ldots, k) \]

and
\[
(4.6) \quad f(z) = (z + z_1) \cdots (z + z_k).
\]

Note that since \( v_1, \ldots, v_n \) are linearly independent over \( \mathbb{F}_p \) and \( b_1, \ldots, b_n \) are non-zero, thus \( b_1 v_1, \ldots, b_n v_n \) are also linearly independent over \( \mathbb{F}_p \), so that the box \( B' \) in (4.4) is of the same type as the box \( B \) in Lemma 2. Since the vectors \( d_1, \ldots, d_k \) are distinct, thus the numbers \( z_1, \ldots, z_k \) in (4.5) are also distinct. It follows that the polynomial \( f(z) \) in (4.6) has \( k \) distinct zeros so that it is certainly not a square (the order of the character \( \gamma \) is \( d = 2 \)) so that Lemma 2 can be applied to estimate the sum \( S \) in (4.3). Applying the lemma we obtain
\[ |S| < kq^{1/2}(1 + \log p)^n \]
whence (4.2) follows.

\[
\square
\]

References


