On the correlation of subsequences

Katalin Gyarmati

Abstract

In 1997 Sárközy and Mauduit introduced the well-distribution measure (W) and the correlation measure of order ℓ (C_ℓ) of binary sequences as measures of their pseudorandomness. For a truly random binary sequence these measures are small ($\ll N^{1/2}(\log N)^c$ for a sequence of length N). Several constructions have been given for which these measures are small, namely they are $\ll N^{1/2}(\log N)^c$, so the sequence E_N has strong pseudorandom properties. But in certain applications, e.g. in cryptography, it is not enough to know that the sequence has strong pseudorandom properties, it is also important that the subsequences E_M (where E_M is of the form $\{e_x, e_{x+1}, ..., e_{x+M-1}\}$) also have strong pseudorandom properties for values M possibly small in terms of N. In this paper I will deal with this problem in case of values $M \gg N^{1/4+\varepsilon}$.

2010 AMS Mathematics Subject Classification: 11K45.

List of keywords and phrases: correlation, character sums.

Research partially supported by Hungarian National Foundation for Scientific Research, Grants No. K67676 and PD72264.

1 Introduction

C. Mauduit and A. Sárközy [12] introduced the following measures of pseudorandomness:

For a finite binary sequence $E_N = \{e_1, e_2, \dots, e_N\} \in \{-1, +1\}^N$ write

$$U(E_N, t, a, b) = \sum_{j=0}^{t-1} e_{a+jb} \tag{1}$$

and, for $D = (d_1, \dots, d_\ell)$ with non-negative integers $d_1 < \cdots < d_\ell$,

$$V(E_N, M, D) = \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \dots e_{n+d_\ell}. \tag{2}$$

Then the *well-distribution measure* of E_N is defined as

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

where the maximum is taken over all a, b, t such that $a, b, t \in \mathbb{N}$ and $1 \leq a \leq a + (t-1)b \leq N$. The *correlation measure of order* ℓ of E_N is defined as

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

where the maximum is taken over all $D = (d_1, d_2, \dots, d_\ell)$ and M such that $0 \leq d_1 < d_2 < \cdots < d_\ell < M + d_\ell \leq N$.

A sequence E_N is considered a "good" pseudorandom sequence if each of these measures $W(E_N)$, $C_\ell(E_N)$ (at least for small ℓ) is "small" in terms of N (in particular all are $o(N)$ as $N \longrightarrow \infty$). Indeed, it was proved in [4] that for a truly random sequence $E_N \subseteq \{-1, +1\}^N$ each of these measures is $\ll \sqrt{N \log N}$ and $\gg \sqrt{N}$. Later these bounds were sharpened by Alon, Kohayakawa, Mauduit, Moreira and Rödl [2].

Numerous binary sequences have been tested for pseudorandomness by several authors. In the best constructions we have $W(E_N) \ll \sqrt{N}(\log N)^{c_1}$ and $C_\ell(E_N) \ll \sqrt{N}(\log N)^{c_\ell}$ with positive constants c_1 and c_ℓ. From this it follows that

$$|U(E_N, t, a, b)| \ll N^{1/2}(\log N)^{c_1} \tag{3}$$

and

$$|V(E_N, M, D)| \ll N^{1/2}(\log N)^{c_\ell} \tag{4}$$

(for all t, a, b, M, D). For every M and t, we trivially have

$$\max_{E_N \in \{-1,+1\}^N} |U(E_N, t, a, b)| = t,$$

$$\max_{E_N \in \{-1,+1\}^N} |V(E_N, M, D)| = M.$$

If $|U(E_N, t, a, b)|$ is large compared with t or $|V(E_N, M, D)|$ is large compared with M, then it may occur that our sequence E_N has a "part" with weak pseudorandom properties. Indeed, if t or M is smaller than $\sqrt{N}$ then the estimates (3) and (4) are trivial. Thus it may occur that, say, we want to encrypt a message of estimated length slightly less than N, thus we use an N bit sequence possessing strong pseudorandom properties. However, it may turn out that the text to be encrypted is of length less than, say, $\sqrt{N}$. In this case we use only a short part (of length $\sqrt{N}$) of the sequence although we do not have any control over the pseudorandom properties of the short subsequences. In this paper we would like to present constructions with non-trivial estimates for $V(E_N, M, D)$ in case of small M's.

Theorem 1 *For every N there is a binary sequence $E_N \in \{-1,+1\}^N$ such that if $D = (d_1, d_2, \ldots, d_\ell)$ and $M \le N^{1/2}$ are such that $0 \le d_1 < d_2 < \cdots < d_\ell < M + d_\ell \le N$, then we have*

$$|V(E_N, M, D)| \ll \ell^2 N^{1/4} \log N. \tag{5}$$

From this follows that for $1 \le M \le N$ we have

$$|V(E_N, M, D)| \ll \ell^2 \left\lceil \frac{M}{N^{1/2}} \right\rceil N^{1/4} \log N.$$

Corollary 1 *For the binary sequence $E_N \in \{-1,+1\}^N$ constructed in the proof of Theorem 1 we have*

$$C_\ell(E_M) \ll \ell^2 \left\lceil \frac{M}{N^{1/2}} \right\rceil N^{1/4} \log N \tag{6}$$

for every $M \le N$ and $E_M \subseteq E_N$ (so E_M is of the form $\{e_x, e_{x+1}, \ldots, e_M\}$).

It is an interesting question whether similar results hold for $U(E_N, t, a, b)$?

Theorem 1 is not optimal in the sense that it follows from (6) for the sequence E_N which satisfies the conditions of Theorem 1 that

$$C_\ell(E_N) \ll \ell^2 N^{3/4} \log N,$$

while in the best constructions we have $C_\ell(E_N) \ll N^{1/2} (\log N)^{c_\ell}$. Next we will show the existence of such a sequence.

Theorem 2 *For every N there is a binary sequence $E_N \in \{-1,+1\}^N$ such that if $D = (d_1, d_2, \ldots, d_\ell)$ and $M \le N^{1/2}$ satisfy $0 \le d_1 < d_2 < \cdots < d_\ell < M + d_\ell \le N$, then we have*

$$|V(E_N, M, D)| \ll \ell^2 N^{1/4} \log N. \tag{7}$$

Moreover

$$C_\ell(E_N) \ll \ell^2 N^{1/2} (\log N)^2 \tag{8}$$

and

$$W(E_N) \ll N^{3/4} \log N \tag{9}$$

holds.

From (7) *follows that for* $1 \le M \le N$ *we have*

$$|V(E_N, M, D)| \ll \ell^2 \left\lceil \frac{M}{N^{1/2}} \right\rceil N^{1/4} \log N.$$

Corollary 2 *For the binary sequence* $E_N \in \{-1, +1\}$ *constructed in the proof of Theorem 2 we have*

$$C_\ell(E_M) \ll \ell^2 \left\lceil \frac{M}{N^{1/2}} \right\rceil N^{1/4} \log N$$

for every $M \le N$ *and* $E_M \subseteq E_N$ *(where* E_M *is of the form* $\{e_x, e_{x+1}, \dots, e_{x+M-1}\}$*). Moreover*

$$C_\ell(E_N) \ll \ell^2 N^{1/2} (\log N)^2$$

and

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

holds.

The proofs of Theorem 1 and 2 are constructive. The construction in Theorem 2 uses two-dimensional binary lattices. The multidimensional theory of pseudorandomness was developed by Hubert, Mauduit and Sárközy [9]. They introduced the following definitions:

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

$$I_N^n = \{\mathbf{x} = (x_1, x_2, \dots, x_n) : \ x_i \in \{0, 1, \dots, N-1\}\}.$$

This set is called an *n-dimensional N-lattice* or briefly an *N-lattice*. In [8] 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 vectors, where 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 $(0, \dots, 0, z_i, 0, \dots, 0)$. 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

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

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

In [9] the definition of binary sequences was extended to more dimensions by considering functions of type

$$e_{\mathbf{x}} = \eta(\mathbf{x}) : \ I_N^n \to \{-1, +1\}. \tag{10}$$

If $\mathbf{x} = (x_1, \dots, x_n)$ so that $\eta(\mathbf{x}) = \eta((x_1, \dots, x_n))$ then we will slightly simplify the notation 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. Binary 2 or 3 dimensional pseudorandom lattices can be used in encryption of digital images.

Hubert, Mauduit and Sárközy [9] introduced the following measure of pseudorandomness of binary lattices (here we will present the definition in the same slightly modified but equivalent form as in [8]):

Definition 1 *Let*

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

be a binary lattice. Define the pseudorandom measure of order ℓ of η *by*

$$Q_\ell(\eta) = \max_{B, \mathbf{d_1}, \ldots, \mathbf{d}_\ell} \left| \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d_1}) \ldots \eta(\mathbf{x} + \mathbf{d}_\ell) \right|, \tag{11}$$

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

Then η is said to have strong pseudorandom properties, or briefly, it is considered a "good" pseudorandom lattice if for fixed n and ℓ and "large" N the measure $Q_\ell(\eta)$ is "small" (much smaller, then the trivial upper bound N^n). This terminology is justified by the fact that, as was proved in [9], for a truly random binary lattice defined on I_N^n and for fixed ℓ the measure $Q_\ell(\eta)$ is "small"; in particular, it is less than $N^{n/2}$ multiplied by a logarithmic factor. Later Gyarmati, Mauduit and Sárközy [6] introduced a new measure of pseudorandom binary lattices: The *correlation measure of order* ℓ of the lattice $\eta : I_N^n \to \{-1, +1\}$ is defined by

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

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

$$B' = \{\mathbf{x} = (x_1, x_2, \ldots, x_n) : \ 0 \le x_1 \le t_1 (< N), \ldots, \ 0 \le x_n \le t_n (< N)\}$$

such that $B' + \mathbf{d_1}, \ldots, B' + \mathbf{d}_\ell \subseteq I_N^n$. Note that it follows trivially from the definition that for all binary lattice η and all integer ℓ we have

$$C_\ell(\eta) \le Q_\ell(\eta) \tag{12}$$

(but Q_ℓ is usually much greater than C_ℓ).

In [7] we reduced the two dimensional case to the one dimensional one by the following way: To any 2-dimensional binary N-lattice

$$\eta(\underline{x}): \ I_N^2 \to \{-1,+1\} \tag{13}$$

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 (13) then we continue the binary sequence by taking the second row of the lattice, then the third row follows, etc.; in general, we set

$$e_{iN+j} = \eta((j-1,i)) \text{ for } i = 0,1,\dots,N-1, \ j = 1,2,\dots,N. \tag{14}$$

In [7] we asked if it is true that if $E_{N^2}(\eta)$ is a "good" pseudorandom binary *sequence* then η is a "good" pseudorandom 2-dimensional lattice? The answer to this question is negative; we 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. Here we study the opposite. We will prove that if the lattice η has small correlation measure, then the corresponding $E_N^2(\eta)$ sequence has small correlation measures as well.

Theorem 3 *Let η be an arbitrary binary lattice. Then*

$$C_\ell(E_{N^2}(\eta)) \le (\ell+2)C_\ell(\eta).$$

By $C_\ell(\eta) \le Q_\ell(\eta)$ it follows that

Corollary 3 *Let η be an arbitrary binary lattice. Then*

$$C_\ell(E_{N^2}(\eta)) \le (\ell+2)Q_\ell(\eta).$$

In the proof of Theorem 2 we will use Theorem 3. But Theorem 3 is of independent interest: by using Theorem 3 we can construct pseudorandom binary sequences by using pseudorandom binary lattices.

We remark that one may obtain similar results for shorter intervals in Theorem 2: If t is an integer then for $M \leq N^{1/t}$ we have $|V(E_N, M, D)| \ll N^{1/(2t)} \log N$ in place of (7) while $C_\ell(E_N) \ll N^{1/2}(\log N)^{c_\ell}$ and $W(E_N) \ll N^{3/4}(\log N)^{c_1}$ also holds. However the proof of this result would be lengthy (we would need more sophisticated sums as the ones in Lemma 4 and the relation between the pseudorandom measures of the binary lattices and the associated binary sequences is more complicated) thus we ommit here the details, but one might return to this problem in a continuation of the present paper.

Throughout the paper $[a, b]$ will denote the set $\{a, a+1, \dots, b\}$.

2 Proofs

Proof of Theorem 1

For $N = 2$ the theorem is trivial. For $N \geq 3$ by Chebysev's theorem there exists an odd prime p such that

$$N^{1/2} < p < 2N^{1/2}. \tag{15}$$

For an irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree $k \geq 2$, we define a binary sequence $E_p(f) = \{e_1, e_2, \dots, e_p\}$ by the following way:

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

(We remark that since f is irreducible, for an integer n, $f(n)$ is never divisible by p thus $\left(\frac{f(n)}{p}\right)$ always assumes ± 1.) Next we will construct a pseudorandom binary sequence for which (5) holds. Let $f_1(x), f_2(x), \dots, f_p(x)$ be different irreducible polynomials of degree $k \geq 2$ and for $1 \leq i \leq p$ let $f_i(x)$ be of the form

$$f_i(x) = x^k + a_{i,k-2}x^{k-2} + a_{i,k-3}x^{k-3} + \dots + a_{i,0} \tag{16}$$

with $a_{i,j} \in \mathbb{F}_p$. (so the coefficient of x^{k-1} is 0 in $f_i(x)$). We remark that the number of monic irreducible polynomials of degree $k < p$ over the finite field $\mathbb{F}_q$ is

$$L_q(k) = \frac{1}{k} \sum_{d|k} \mu\left(\frac{k}{d}\right) q^d$$

see [5, pp. 602-629]. For $k \geq 4$

$$L_q(k) \geq \frac{1}{k}q^k - \frac{1}{k}\sum_{d=1}^{[k/2]} q^d \geq \frac{1}{k}q^k - \frac{1}{k}q\frac{q^{k/2}-1}{q-1} \geq \frac{1}{k}\left(q^k - q^{(k+2)/2}\right) \geq \frac{1}{2k}q^k.$$

For every $j \in \mathbb{F}_q$ consider $f(x+j)$. Between these q different irreducible polynomials there is exactly one which is of the form

$$f(x+j) = x^k + a_{k-2}x^{k-2} + \dots + a_0$$

(so the coefficient of x^{k-1} is 0 in $f(x+j)$). Thus for $k \geq 4$ and $p \geq 3$ the number of irreducible polynomials which are of the form $x^k + a_{k-2}x^{k-2} + \dots + a_0$ is

$$N_q(k) \stackrel{\text{def}}{=} \frac{1}{q}L_q(k) \geq \frac{1}{2k}q^{k-1}. \tag{17}$$

For $k \geq 4$, $p \geq 3$ we have $N_p(k) \geq p$, thus there exist p different irreducible polynomials $f_1(x), f_2(x), \dots, f_p(x)$ which are of the form (16). Let

$$E_{p^2} \stackrel{\text{def}}{=} \{E_p(f_1), E_p(f_2), \dots, E_p(f_p)\} \tag{18}$$

where E_{p^2} is a binary sequence of length p^2 obtained by writing the elements of $E_p(f_1), E_p(f_2), \dots, E_p(f_p)$ successively. Let $E_{p^2} = \{e_1, e_2, \dots, e_{p^2}\}$ and since by (15) we have

$$N < p^2 < 4N,$$

we may define E_N by the sequence of the first N elements of E_{p^2}:

$$E_N = \{e_1, e_2, \dots, e_N\}.$$

If $M < p$, $D = (d_1, \dots, d_\ell)$

$$\begin{aligned} &V(E_N, M, D) = V(E_{p^2}, M, D) \\ &= e_{1+d_1}e_{1+d_2}\dots e_{1+d_\ell} + e_{2+d_1}e_{2+d_2}\dots e_{2+d_\ell} + \dots + e_{M+d_1}e_{M+d_2}\dots e_{M+d_\ell}. \end{aligned}$$

Next we will prove that for each $1 \le i \le \ell$ and $1 \le n < M$, there exist integers a_i, b_i and intervals $I_i = \{1, 2, \dots, b_i\}$ and $J_i = \{b_i+1, b_i+2, \dots, M\}$ such that

$$e_{n+d_i} = \begin{cases} \left(\frac{f_{a_i}(n+d_i)}{p}\right) & \text{if } n \in I_i, \\ \left(\frac{f_{a_i+1}(n+d_i)}{p}\right) & \text{if } n \in J_i, \end{cases} \tag{19}$$

(if $b_i = M$ then $J_i = \emptyset$). Indeed, let $m_p(x)$ denote the least nonnegative integer with

$$x \equiv m_p(x) \pmod p,$$

so $0 \le m_p(x) \le p-1$. Then

$$n + d_i = \left[\frac{n+d_i-1}{p}\right]p + m_p(n+d_i-1) + 1.$$

Thus

$$e_{n+d_i} = f_{\left[\frac{n+d_i-1}{p}\right]+1}(m_p(n+d_i-1)+1) = f_{\left[\frac{n+d_i-1}{p}\right]+1}(n+d_i). \tag{20}$$

In (19) $0 \leq n \leq M < p$. Let $d_i = q_i p + s_i$ where $0 \leq s_i \leq p-1$. Then

$$\left[\frac{n+d_i-1}{p}\right] = \left[\frac{q_i p + s_i + n - 1}{p}\right] = q_i + \left[\frac{s_i+n-1}{p}\right]$$
$$= \begin{cases} q_i & \text{if } n \leq p - s_i, \\ q_i + 1 & \text{if } n > p - s_i, \end{cases} \tag{21}$$

which proves (19) with $a_i = q_i + 1$ and $b_i = \max\{p - s_i, M\}$, so $I_i = [1, b_i]$, $J_i = [b_i+1, M]$ (if $b_i = M$ then $J_i = \emptyset$). Then $\{1, b_1+1, b_2+1, \ldots, b_\ell+1, M+1\}$ is a multiset which contains integers $1 = c_1 < c_2 < \cdots < c_m = M+1$ where

$$m \leq \ell + 2. \tag{22}$$

Then $[0, M] = \cup_{j=1}^{m-1} [c_j, c_{j+1} - 1]$. By the definition of the c_j's, $c_j < b_i + 1 < c_{j+1}$ is not possible, thus $c_{j+1} - 1 \leq b_i$ or $b_i \leq c_j - 1$, so $[c_j, c_{j+1} - 1] \subseteq [0, b_i]$ or $[c_j, c_{j+1} - 1] \subseteq [b_i + 1, M]$. Hence

$$V(E_N, M, D) = \sum_{n=1}^{M} e_{n+d_1} \ldots e_{n+d_\ell} = \sum_{j=1}^{m-1} \sum_{n \in [c_j, c_{j+1}-1]} e_{n+d_1} \ldots e_{n+d_\ell}. \tag{23}$$

Now each interval $[c_j, c_{j+1} - 1]$ is either $\subseteq I_i$ or $\subseteq J_i$ for every $1 \leq i \leq \ell$. Thus for every $d_1, d_2, \ldots, d_\ell$ and for every interval $[c_j, c_{j+1} - 1]$ there exists fixed numbers $h_1, h_2, \ldots, h_\ell$ (depending only on $d_1, d_2, \ldots, d_\ell$ and j) such that for $n \in [c_j, c_{j+1} - 1]$

$$e_{n+d_1} e_{n+d_2} \ldots e_{n+d_\ell} = \left(\frac{f_{h_1}(n+d_1)}{p}\right)\left(\frac{f_{h_2}(n+d_2)}{p}\right) \cdots \left(\frac{f_{h_\ell}(n+d_\ell)}{p}\right)$$
$$= \left(\frac{f_{h_1}(n+d_1) f_{h_2}(n+d_2) \ldots f_{h_\ell}(n+d_\ell)}{p}\right)$$

Next we estimate

$$\sum_{n\in[c_j,c_{j+1}-1]} e_{n+d_1}e_{n+d_2}\dots e_{n+d_\ell}$$
$$=\sum_{n\in[c_j,c_{j+1}-1]} \left(\frac{f_{h_1}(n+d_1)f_{h_2}(n+d_2)\dots f_{h_\ell}(n+d_\ell)}{p}\right).$$

Here $f_{h_1}(x+d_1),\dots,f_{h_\ell}(x+d_\ell)$ are different polynomials. Indeed if

$$f_{h_r}(x+d_r)=f_{h_t}(x+d_t),$$

then substituting $x+d_r$ by x we get

$$f_{h_r}(x)=f_{h_t}(x+d_t-d_r). \tag{24}$$

It is easy to see that there is exactly one among the polynomials $f_{h_t}(x), f_{h_t}(x+1),\dots,f_{h_t}(x+p-1)$ for which the coefficient of x^{k-1} is 0, and this one is $f_{h_t}(x)$. From this and (24) follows that

$$d_r\equiv d_t \pmod p. \tag{25}$$

Thus from (24) we get

$$f_{h_r}(x)=f_{h_t}(x).$$

Since the polynomials $f_1,f_2,\dots,f_\ell$ are different, from this

$$h_r=h_t \tag{26}$$

follows. Now we compute the value $h_r=h_t$. By (20) for $n\in[c_j,c_{j+1}-1]$ $e_{n+d_r}=f_{h_r}(n+d_r)$, $e_{n+d_t}=f_{h_t}(n+d_t)$ where

$$h_r=\left[\frac{n+d_r-1}{p}\right]+1,$$
$$h_t=\left[\frac{n+d_t-1}{p}\right]+1. \tag{27}$$

By (26) and (27)

$$\left[\frac{n+d_r-1}{p}\right]=\left[\frac{n+d_t-1}{p}\right]. \tag{28}$$

Now

$$n+d_r=q_rp+s_r,\ n+d_t=q_tp+s_t \tag{29}$$

where $0\le s_r, s_t\le p-1$. By (25)

$$s_r=s_t. \tag{30}$$

Now

$$\left[\frac{n+d_r-1}{p}\right]+1=\left[\frac{q_rp+s_r-1}{p}\right]+1=q_r+1+\left[\frac{s_r-1}{p}\right].$$

Similarly

$$\left[\frac{n+d_t-1}{p}\right]=q_t+1+\left[\frac{s_t-1}{p}\right].$$

By this, (28) and (30) we have

$$q_r=q_t.$$

By this, (29) and (30)

$$d_r=d_t,$$

which is a contradiction. So indeed, the irreducible polynomials $f_{h_1}(x+d_1),\dots,f_{h_\ell}(x+d_\ell)$ are different. Thus the product $f_{h_1}(x+d_1)f_{h_2}(x+d_2)\dots f_{h_\ell}(x+d_\ell)$ is not of the form $cg^2(x)$. We will use the following lemma:

Lemma 1 *Suppose that p is a prime, χ is a non-principal character modulo p of order d, $f\in\mathbb{F}_p[x]$ has s distinct roots in $\overline{\mathbb{F}}_p$, and it is not a constant* *multiple of the d-th power of a polynomial over* $\mathbb{F}_p$*. Let* y *be a real number with* $0 < y \le p$*. Then for any* $x \in \mathbb{R}$*:*

$$\left| \sum_{x < n \le x+y} \chi(f(n)) \right| < p^{1/2} \log p. \tag{31}$$

Poof of Lemma 1

This lemma is the one-dimensional case of Lemma 10 due to Winterhof [17], who derived it from Weil theorem [16]. We mention that a slightly weaker version of the lemma can be found in Lemma 1 in [1] where $9sp^{1/2}\log p$ is proved in place of the right hand side of (31). (In the case $f(x) = x$ the best constant factor is achieved by Bourgain, Cochrane, Paulhus and C. Pinner in [3], and their method also works for higher degree polynomials.)

Since later in the proof we will also use Weil's theorem, we state it here as a lemma (see in [11] and [16]):

Lemma 2 *Suppose that* p *is a prime,* χ *is a non-principal character modulo* p *of order* d*,* $f \in \mathbb{F}_p[x]$ *has* s *distinct roots in* $\overline{\mathbb{F}}_p$*, and it is not a constant multiple of the d-th power of a polynomial over* $\mathbb{F}_p$*. Then:*

$$\left| \sum_{n \in \mathbb{F}_p} \chi(f(n)) \right| < sp^{1/2}.$$

By Lemma 1 we get

$$\begin{aligned} &\sum_{n \in [c_j, c_{j+1}-1]} e_{n+d_1} e_{n+d_2} \dots e_{n+d_\ell} \\ &= \sum_{n \in [c_j, c_{j+1}-1]} \left(\frac{f_{h_1}(n+d_1) f_{h_2}(n+d_2) \dots f_{h_\ell}(n+d_\ell)}{p} \right). \\ &\le 9\ell k p^{1/2} \log p. \end{aligned}$$

By (22) and (23) we get

$$|V(E_N, M, D)| \ll \ell^2 k p^{1/2} \log p \ll \ell^2 k N^{1/4} \log N. \qquad (32)$$

Since k, the degree of the polynomials $f_1(x), f_2(x), \dots, f_p(x)$ can be chosen as $k = 4$, from (32) we get (5), which was to be proved.

Proof of Theorem 2 First we will need some technical preparation in order to be able to estimate character sums of the type which appear later in the proof of our theorem. First Katz [10] and Perelmuter-Shparlinski [14] studied character sums over subfields of a finite field. Their result was generalized by Wan [15] who proved the following very general theorem:

Lemma 3 *Let the $f_i(T)$ with $1 \le i \le n$ be pairwise coprime polynomials. Let D be the degree of the largest squarefree divisor of $\prod_{i=1}^n f_i(T)$. Let χ_i be a multiplicative character of the field $\mathbb{F}_{q^m}$ for $1 \le i \le n$. Suppose that for some $1 \le i \le n$, there is a root ξ_i of multiplicity m_i of $f_i(T)$ such that the character χ^{m_i} is non-trivial on the set $Norm_{\mathbb{F}_{q^m}[\xi_i]/\mathbb{F}_{q^m}}(\mathbb{F}_q[\xi])$. Then we have*

$$\left| \sum_{a \in \mathbb{F}_q} \chi_1(f_1(a)) \dots \chi_n(f_n(a)) \right| \le (mD - 1) q^{1/2}.$$

Part a) of the following lemma is a consequence of Lemma 3, while the estimate in part b) - the incomplete case - is new and I will derive it directly from Weil's theorem. (At the same time I will also give an alternative proof for part a), since in order to do so I just need to add one more sentence to the proof of part b).)

Lemma 4 *Let p be an odd prime, $q = p^2$ and denote the quadratic character of $\mathbb{F}_q$ by γ. Clearly $\mathbb{F}_p \subseteq \mathbb{F}_q$. Let $I = [a, a+1, a+2, \dots, b] \subseteq \mathbb{F}_p$ and*

$f(x) \in \mathbb{F}_q[x]$ be a polynomial which is not of the form $cg(x)h^2(x)$ with $c \in \mathbb{F}_q$, $g(x) \in \mathbb{F}_p[x]$ and $h(x) \in \mathbb{F}_q[x]$. Suppose that $f(x)$ has m distinct zeros in its splitting field over $\mathbb{F}_p$. Then

$$a)\quad \left|\sum_{x\in\mathbb{F}_p} \gamma(f(x))\right| \leq 2mp^{1/2}, \tag{33}$$

$$b)\quad \left|\sum_{x\in I} \gamma(f(x))\right| \leq 2mp^{1/2}(1+\log p). \tag{34}$$

Proof of Lemma 4 Let $n \in \mathbb{F}_p$ be a quadratic non-residue modulo p, so

$$\left(\frac{n}{p}\right) = -1. \tag{35}$$

The polynomial $x^2 - n \in \mathbb{F}_q[x] = \mathbb{F}_{p^2}[x]$ is reducible in $\mathbb{F}_q[x]$, let $\theta \in \mathbb{F}_q$ be an element for which

$$\theta^2 = n \tag{36}$$

in $\mathbb{F}_q$. Since n is quadratic non-residue modulo p, $\theta \notin \mathbb{F}_p$. Then $\{1, \theta\}$ is a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$, so every element of $\mathbb{F}_q$ can be written uniquely in the form $x + \theta y$ with $x, y \in \mathbb{F}_p$. Then define the conjugate of $x + \theta y$ by

$$\overline{x+\theta y} \stackrel{\text{def}}{=} x - \theta y.$$

Then for $a, b \in \mathbb{F}_q$ we have

$$\overline{ab} = \overline{a}\cdot\overline{b},$$

$$\overline{a+b} = \overline{a} + \overline{b},$$

and

$$a\overline{a} \in \mathbb{F}_p. \tag{37}$$

It is easy to check that

$$\overline{x+\theta y} = (x+\theta y)^p, \tag{38}$$

since by using the Euler lemma for $x, y \in \mathbb{F}_p$ we have

$$\begin{aligned}(x+\theta y)^p &= x^p + \theta^p y^p = x^p + \left(\theta^2\right)^{p-1/2} \theta y^p = x + \left(\theta^2\right)^{p-1/2} \theta y \\ &= x + n^{(p-1)/2} \theta y = x + \left(\frac{n}{p}\right) \theta y = x - \theta y.\end{aligned}$$

Thus the conjugation is an automorphism of $\mathbb{F}_q$ which can be extended to an automorphism of $\overline{\mathbb{F}}_q$ by

$$\begin{aligned}\overline{\mathbb{F}}_q &\to \overline{\mathbb{F}}_q, \\ \varepsilon &\to \varepsilon^p.\end{aligned}$$

This is the Froebenius automorphism.

Lemma 5 *For* $x, y \in \mathbb{F}_p$

$$\gamma(x+\theta y) = \left(\frac{(x+\theta y)\overline{(x+\theta y)}}{p}\right) = \left(\frac{x^2 - ny^2}{p}\right).$$

Proof of Lemma 5 Using (38) and the Euler lemma we get

$$\begin{aligned}\gamma(x+\theta y) &= (x+\theta y)^{(q-1)/2} = (x+\theta y)^{\left(p^2-1\right)/2} \\ &= (x+\theta y)^{\left(p^2-p\right)/2} (x+\theta y)^{(p-1)/2} \\ &= \left((x+\theta y)^p\right)^{(p-1)/2} (x+\theta y)^{(p-1)/2} \\ &= \left(\overline{x+\theta y}\right)^{(p-1)/2} (x+\theta y)^{(p-1)/2} \\ &= (x-\theta y)^{(p-1)/2} (x+\theta y)^{(p-1)/2} \\ &= \left(x^2 - \theta^2 y^2\right)^{(p-1)/2} \\ &= \left(x^2 - ny^2\right)^{(p-1)/2},\end{aligned}$$

which proves Lemma 5.

By Lemma 5

$$\sum_{x\in I}\gamma(f(x))=\sum_{x\in I}\left(\frac{f(x)\overline{f(x)}}{p}\right).$$

Since $I\subseteq\mathbb{F}_p$, if $f(x)=a_kx^k+\dots+a_o$, then

$$\begin{aligned}\sum_{x\in I}\left(\frac{f(x)\overline{f(x)}}{p}\right)&=\sum_{x\in I}\left(\frac{\left(a_kx^k+\dots+a_o\right)\overline{\left(a_kx^k+\dots+a_o\right)}}{p}\right)\\&=\sum_{x\in I}\left(\frac{\left(a_kx^k+\dots+a_o\right)\left(\overline{a_k}x^k+\dots+\overline{a_o}\right)}{p}\right).\end{aligned}$$

Here the coefficients of $\left(a_kx^k+\dots+a_o\right)\left(\overline{a_k}x^k+\dots+\overline{a_o}\right)$ are in $\mathbb{F}_p$, since $f(x)$ can be written in the form $p(x)+\theta r(x)$ with $p(x),r(x)\in\mathbb{F}_p[x]$ and then $\overline{f(x)}=\overline{a_k}x^k+\dots+\overline{a_o}=p(x)-\theta r(x)$ so $f(x)\overline{f(x)}=(p(x)+\theta r(x))(p(x)-\theta r(x))=p^2(x)-nq^2(x)\in\mathbb{F}_p[x]$.

Let $b(x)=\left(a_kx^k+\dots+a_o\right)\left(\overline{a_k}x^k+\dots+\overline{a_o}\right)$. Then

$$\sum_{x\in I}\left(\frac{f(x)\overline{f(x)}}{p}\right)=\sum_{x\in I}\left(\frac{b(x)}{p}\right).$$

Here we need Weil's theorem. If the conditions of Lemma 1 and Lemma 2 hold, then using these lemmas we get (33) and (34) which was to be proved. So indeed, we need to prove that the conditions of Lemma 1 and Lemma 2 hold for $b(x)$, so $b(x)$ is not of the form $ch^2(x)$, with $c\in\mathbb{F}_p$, $h(x)\in\mathbb{F}_p[x]$.

Let

$$f(x)=a_k(x-\varepsilon_1)(x-\varepsilon_2)\dots(x-\varepsilon_k)$$

where $a_k\in\mathbb{F}_q$, $\varepsilon_1,\dots,\varepsilon_k\in\overline{\mathbb{F}}_p$. Then for $x\in\mathbb{F}_p$

$$\begin{aligned}\overline{f(x)}&=\overline{a_k}\left(\overline{x}-\overline{\varepsilon_1}\right)\cdots\left(\overline{x}-\overline{\varepsilon_k}\right)\\&=\overline{a_k}\left(x-\varepsilon_1^p\right)\cdots\left(x-\varepsilon_k^p\right).\end{aligned}$$

Then $b(x) = f(x)\overline{f(x)} = a_k\overline{a_k}(x-\varepsilon_1)\cdots(x-\varepsilon_k)(x-\varepsilon_1^p)\cdots(x-\varepsilon_k^p)$. Clearly by (37) we have $a_k\overline{a_k} \in \mathbb{F}_p$. The next question is that when is a product $(x-\varepsilon_1)\cdots(x-\varepsilon_k)\,(x-\varepsilon_1^p)\cdots(x-\varepsilon_k^p)$ of the form $n^2(x)$ with $n(x) \in \mathbb{F}_p[x]$. Let $\alpha_1, \alpha_2, \ldots, \alpha_t$ be the different elements among $\varepsilon_1, \ldots, \varepsilon_k$ which have odd multiplicity in the factorization of $f(x) = a_k(x-\varepsilon_1)\ldots(x-\varepsilon_k)$. Writing $g(x) = (x-\alpha_1)\ldots(x-\alpha_t)$ we get that $f(x)$ is of the form $a_k g(x)h^2(x)$ where $g(x)$ has no multiple roots and $g(x), h(x) \in \overline{\mathbb{F}}_p[x]$. Then

$$b(x) = a_k\overline{a_k}(x-\alpha_1)\ldots(x-\alpha_t)(x-\alpha_1^p)\ldots(x-\alpha_t^p)s^2(x)$$

with $s(x) \in \overline{\mathbb{F}}_p[x]$. Here $(x-\alpha_1)\ldots(x-\alpha_t)(x-\alpha_1^p)\ldots(x-\alpha_t^p)$ is of the form $u^2(x)$ with $u(x) \in \overline{\mathbb{F}}_p[x]$ if and only if $\{\alpha_1, \alpha_2, \ldots, \alpha_t\} = \{\alpha_1^p, \alpha_2^p, \ldots, \alpha_t^p\}$. If $\{\alpha_1, \alpha_2, \ldots, \alpha_t\} = \{\alpha_1^p, \alpha_2^p, \ldots, \alpha_t^p\}$ then for every symmetric polynomial $v \in \mathbb{F}_p[x_1, x_2, \ldots, x_t]$ we have

$$v(\alpha_1, \ldots, \alpha_t) = v(\alpha_1^p, \ldots, \alpha_t^p) = v^p(\alpha_1, \ldots, \alpha_t).$$

Thus $v(\alpha_1, \ldots, \alpha_t) \in \mathbb{F}_p$. So the coefficients of $g(x) = (x-\alpha_1)\ldots(x-\alpha_t)$ are the elements of $\mathbb{F}_p$. Thus the coefficients of $h^2(x) = \frac{f(x)}{a_k g(x)}$ are in $\mathbb{F}_q$.

Let $h(x) = x^f + b_{f-1}x^{f-1} + \cdots + b_0$. We will prove by induction that $b_{f-i} \in \mathbb{F}_q$. Indeed the coefficient of x^{2f-1} in $h^2(x)$ is $2b_{f-1}$, thus $b_{f-1} \in \mathbb{F}_q$. Suppose that $b_{f-1}, b_{f-2}, \ldots, b_{f-v} \in \mathbb{F}_p$. We will prove that $b_{f-v-1} \in \mathbb{F}_p$ also holds. Indeed the coefficient of x^{2f-v-1} is of the form $2b_{f-v-1} + j(b_{f-1}, b_{f-2}, \ldots, b_{f-v})$ with $j \in \mathbb{F}_p[x_1, x_2, \ldots, x_v]$. Thus $2b_{f-v-1} + j(b_{f-1}, b_{f-2}, \ldots, b_{f-v})$ is in $\mathbb{F}_q$, and by the inductive hypothesis $j(b_{f-1}, b_{f-2}, \ldots, b_{f-v})$ is in $\mathbb{F}_q$, thus b_{f-v-1} is in $\mathbb{F}_q$. So we proved that $h(x) \in \mathbb{F}_q[x]$. Thus $b(x) = a_k\overline{a_k}(x-\varepsilon_1)\ldots(x-\varepsilon_k)(x-\overline{\varepsilon_1})\ldots(x-\overline{\varepsilon_k})$ is of the form $cn^2(x)$ with $c \in \mathbb{F}_q$, $n(x) \in \mathbb{F}_q[x]$ if and only if $f(x)$ is of the form $cg(x)h^2(x)$ with $c \in \mathbb{F}_q$, $g(x) \in \mathbb{F}_p[x]$, $h(x) \in \mathbb{F}_q[x]$, which was to be proved.

In order to prove Theorem 2 we need one more lemma. Namely:

Lemma 6 *Let $f(x) \in \mathbb{F}_{p^2}[x]$ be an irreducible polynomial in $\mathbb{F}_{p^2}[x]$ of degree k, which is of the form*

$$f(x) = x^k + a_{k-1}x^{k-1} + \dots + a_0,$$

where $a_{k-1} \in \mathbb{F}_p$ but $f(x) \notin \mathbb{F}_p[x]$, so there is an $1 \le i \le k-2$ such that $a_i \notin \mathbb{F}_p$. Then for $d_1, d_2, \dots, d_\ell \in \mathbb{F}_{p^2}$ we have

$$f(x+d_1)f(x+d_2)\dots f(x+d_\ell) \notin \mathbb{F}_p[x].$$

Proof of Lemma 6 Every $f(x) \in \mathbb{F}_{p^2}[x]$ can be uniquely written in the form

$$f(x) = a_k x^k + a_{k-1}x^{k-1} + \dots + a_0$$

with $a_i \in \mathbb{F}_{p^2}$. Then define

$$\tau(f(x)) \stackrel{\text{def}}{=} \overline{a_k}x^k + \overline{a_{k-1}}x^{k-1} + \dots + \overline{a_0}.$$

Clearly,

$$\begin{aligned} \tau(\tau(f(x))) &= f(x) \\ \tau(f(x)+g(x)) &= \tau(f(x)) + \tau(g(x)) \\ \tau(f(x)g(x)) &= \tau(f(x))\tau(g(x)). \end{aligned}$$

Lemma 7 *If $f(x) \in \mathbb{F}_{p^2}[x]$ is irreducible in $\mathbb{F}_{p^2}[x]$, then $\tau(f(x)) \in \mathbb{F}_{p^2}[x]$ is also irreducible in $\mathbb{F}_{p^2}[x]$.*

Proof of Lemma 7 Whenever

$$\tau(f(x)) = g(x)h(x) \text{ with } g(x), h(x) \in \mathbb{F}_{p^2}[x],$$

then

$$f(x) = \tau(\tau(f(x))) = \tau(g(x))\tau(h(x)).$$

Since $f(x)$ is irreducible it follows that $\tau(f(x))$ or $\tau(g(x))$ is constant. From this follows that $f(x)$ or $g(x)$ is constant. But then $\tau(f(x))$ is irreducible.

Lemma 8 *If $f(x) \in \mathbb{F}_{p^2}[x]$ is an irreducible polynomial in $\mathbb{F}_{p^2}[x]$ with leading coefficient 1, but $f(x) \notin \mathbb{F}_p[x]$ then $g(x) \stackrel{def}{=} f(x)\tau(f(x))$ is in $\mathbb{F}_p[x]$ and $g(x)$ is irreducible in $\mathbb{F}_p[x]$.*

Proof of Lemma 8 Define n and θ as in (35) and (36). Then every $f(x) \in \mathbb{F}_{p^2}[x]$ can be uniquely written in the form

$$f(x) = a(x) + \theta b(x)$$

with $a(x), b(x) \in \mathbb{F}_p[x]$. Then

$$\tau(f(x)) = a(x) - \theta b(x).$$

Thus

$$f(x)\tau(f(x)) = (a(x) + \theta b(x))(a(x) - \theta b(x)) = a^2(x) - nb^2(x) \in \mathbb{F}_p[x].$$

Suppose that $f(x)\tau(f(x))$ is not irreducible in $\mathbb{F}_p[x]$, so

$$f(x)\tau(f(x)) = g(x)h(x) \tag{39}$$

with $g(x), h(x) \in \mathbb{F}_p[x]$, where the leading coefficients of $g(x)$ and $h(x)$ are 1 and $\deg g(x), \deg h(x) \geq 1$. Then (39) also holds in $\mathbb{F}_{p^2}[x]$ since $\mathbb{F}_p \subseteq \mathbb{F}_{p^2}$. But there is a unique factorization in $\mathbb{F}_{p^2}[x]$, and $f(x)$ and $\tau(f(x))$ are irreducible polynomials in $\mathbb{F}_{p^2}[x]$ with leading coefficients 1, thus

$$f(x) = g(x),\ \tau(f(x)) = h(x)$$

or

$$f(x) = h(x),\ \tau(f(x)) = g(x).$$

In both cases we get $f(x) \in \mathbb{F}_p[x]$, which is a contradiction.

Now we are ready to prove Lemma 6. Suppose that

$$f(x + d_1) \dots f(x + d_\ell) \in \mathbb{F}_p[x].$$

Let $\alpha \in \overline{\mathbb{F}}_p$ be a root of $f(x + d_1)$, then $f(\alpha + d_1) = 0$, thus

$$f(\alpha + d_1) \dots f(\alpha + d_\ell) = 0.$$

But then the minimal polynomial of α in $\mathbb{F}_p[x]$ divides $f(x+d_1) \dots f(x+d_\ell) \in \mathbb{F}_p[x]$. Next we determine the minimal polynomial of α in $\mathbb{F}_p[x]$. α is a root of $f(x + d_1)\tau(f(x + d_1))$ and by Lemma 8 this polynomial is irreducible in $\mathbb{F}_p[x]$. So the minimal polynomial of α is $f(x+d_1)\tau(f(x+d_1))$ in $\mathbb{F}_p[x]$. Thus

$$f(x + d_1)\tau(f(x + d_1)) \mid f(x + d_1) \dots f(x + d_\ell) \text{ in } \mathbb{F}_p[x].$$

But $\mathbb{F}_p[x] \subseteq \mathbb{F}_{p^2}[x]$, so

$$f(x + d_1)\tau(f(x + d_1)) \mid f(x + d_1) \dots f(x + d_\ell) \text{ in } \mathbb{F}_{p^2}[x].$$

Thus

$$\tau(f(x + d_1)) \mid f(x + d_2) \dots f(x + d_\ell) \text{ in } \mathbb{F}_{p^2}[x].$$

By Lemma 7, $\tau(f(x+d_1))$ is irreducible in $\mathbb{F}_{p^2}[x]$ and its leading coefficient is 1, thus by the unique factorization in $\mathbb{F}_{p^2}[x]$, there is an $2 \le i \le \ell$ such that

$$\tau(f(x+d_1)) = f(x+d_i).$$

Without the loss of generality we may assume

$$\tau(f(x+d_1)) = f(x+d_2). \tag{40}$$

By the definition of $f(x)$ it is of the form

$$f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_0$$

where $a_k = 1$, $a_{k-1} \in \mathbb{F}_p[x]$. Then

$$\begin{aligned} f(x+d_1) = \sum_{i=0}^{k} \Bigg(\binom{k}{i} a_k d_1^{k-i} + \binom{k-1}{i} a_{k-1} d_1^{k-1-i} \\ + \binom{k-2}{i} a_{k-2} d_1^{k-2-i} + \cdots + \binom{i}{i} a_i \Bigg) x^i \end{aligned}$$

and

$$\begin{aligned} f(x+d_2) = \sum_{i=0}^{k} \Bigg(\binom{k}{i} a_k d_2^{k-i} + \binom{k-1}{i} a_{k-1} d_2^{k-1-i} \\ + \binom{k-2}{i} a_{k-2} d_2^{k-2-i} + \cdots + \binom{i}{i} a_i \Bigg) x^i \end{aligned}$$

By the definition of τ

$$\begin{aligned} \tau(f(x+d_1)) = \sum_{i=0}^{k} \Bigg(\binom{k}{i} \overline{a_k}\,\overline{d_1}^{k-i} + \binom{k-1}{i} \overline{a_{k-1}}\,\overline{d_1}^{k-1-i} \\ + \binom{k-2}{i} \overline{a_{k-2}}\,\overline{d_1}^{k-2-i} + \cdots + \binom{i}{i} \overline{a_i} \Bigg) x^i. \end{aligned}$$

By (40) we get that for $0 \le i \le k$

$$\binom{k}{i}\overline{a_k}\,\overline{d_1}^{k-i} + \binom{k-1}{i}\overline{a_{k-1}}\,\overline{d_1}^{k-1-i} + \binom{k-2}{i}\overline{a_{k-2}}\,\overline{d_1}^{k-2-i} + \cdots + \binom{i}{i}\overline{a_i}$$
$$= \binom{k}{i}a_k d_2^{k-i} + \binom{k-1}{i}a_{k-1}d_2^{k-1-i} + \binom{k-2}{i}a_{k-2}d_2^{k-2-i} + \cdots + \binom{i}{i}a_i. \tag{41}$$

For $i = k-1$ this gives

$$\binom{k}{k-1}\overline{a_k}\,\overline{d_1} + \binom{k-1}{k-1}\overline{a_{k-1}} = \binom{k}{k-1}a_k d_2 + \binom{k-1}{k-1}a_{k-1}. \tag{42}$$

By the conditions of Lemma 6 we have $a_k = 1$ and $a_{k-1} \in \mathbb{F}_p$, thus $\overline{a_k} = a_k$ and $\overline{a_{k-1}} = a_{k-1}$, so from (42)

$$\overline{d_1} = d_2 \tag{43}$$

follows.

Next we prove by induction that $a_i \in \mathbb{F}_p$. Indeed, by the conditions of Lemma 6, a_k and $a_{k-1} \in \mathbb{F}_p$. Next suppose that $a_k, a_{k-1}, \dots, a_{i+1} \in \mathbb{F}_p$. We will prove that $a_i \in \mathbb{F}_p$. Indeed by $a_k, a_{k-1}, \dots, a_{i+1} \in \mathbb{F}_p$ then

$$a_k = \overline{a_k}, a_{k-1} = \overline{a_{k-1}}, \dots, a_{i+1} = \overline{a_{i+1}}$$

By this, (41) and (43) we get

$$\overline{a_i} = a_i,$$

so $a_i \in \mathbb{F}_p$ which was to be proved. Thus $a_k, a_{k-1}, \dots, a_0 \in \mathbb{F}_p$. But then $f(x) \in \mathbb{F}_p[x]$, which is contradiction. Thus we proved Lemma 6.

Next we return to the proof of Theorem 2. For $N = 2$ the theorem is trivial. For $N \ge 3$ let p be an odd prime for which

$$N^{1/2} < p < 2N^{1/2}. \tag{44}$$

(By Chebysev's theorem such a prime p exists.) Let $q = p^2$ and let n be a quadratic non-residue modulo p, so $\left(\frac{n}{p}\right) = -1$. Let $\theta \in \mathbb{F}_{p^2}$ be a number for which

$$\theta^2 = n$$

in $\mathbb{F}_q$. Then $\{1, \theta\}$ is a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$.

Let $f(x)$ be an irreducible polynomial of degree $k \geq 2$ which is of the form

$$f(x) = x^k + a_{k-2}x^{k-2} + \cdots + a_0$$

(so the coefficient of the term x^{k-1} is 0) but

$$f(x) \notin \mathbb{F}_p[x].$$

By (17) the number of such polynomials is

$$R \stackrel{\text{def}}{=} N_{p^2}(k) - N_p(k) \geq \frac{1}{2k}p^{2k-1} - \frac{1}{k}p^{k-1} > 0,$$

thus such a polynomial exists, indeed.

Define the binary lattice $\eta : I_p^2 \to \{-1, +1\}$ by

$$\eta(\underline{x}) = \eta((x_1, x_2)) = \gamma(f(x_1 + \theta x_2)).$$

Lemma 9

$$Q_\ell(\eta) \leq k\ell\left(p(1 + \log p)^2\right) \ll k\ell N^{1/2}(\log N)^2. \tag{45}$$

Proof of Lemma 9 We remark that this construction is a shifted version of the construction in Theorem 1 in [13]. We cannot use Theorem 1 in [13] because none of the conditions a), b) and c) holds in Theorem 1 in [13].

However, similarly to the proof of Theorem 1 in [13], it is easy to prove that (45) holds:

Write $\boldsymbol{d}_i = (d_1^{(i)}, d_2^{(i)})$ (for $i = 1, \ldots, \ell$), and consider the general term of the n-fold sum in (11):

$$\begin{aligned}
&\sum_{\mathbf{x}\in B} \eta(\mathbf{x}+\mathbf{d_1})\ldots\eta(\mathbf{x}+\mathbf{d}_\ell) \\
&= \sum_{j_1=0}^{[t_1/b_1]} \sum_{j_2=0}^{[t_2/b_2]} \eta\big((j_1b_1+d_1^{(1)}, j_2b_2+d_2^{(1)})\big)\ldots\eta\big((j_1b_1+d_1^{(\ell)}, j_2b_2+d_2^{(\ell)})\big), \quad (46)
\end{aligned}$$

where B is a box-lattice of form

$$B = \{\mathbf{x} = (j_1b_1, j_2b_2) :\ 0 \le j_1b_1 \le t_1(< p),\ 0 \le j_2b_2 \le t_2(< p),\ j_1, j_2 \in \mathbb{N}\}.$$

Now write

$$z = j_1b_1 + j_2b_2\theta \tag{47}$$

so that z belongs to the box

$$B' = \{j_1b_1 + j_2b_2\theta :\ 0 \le j_1b_1 \le t_1,\ 0 \le j_2b_2 \le t_2,\ j_1, j_2 \in \mathbb{N}\}, \tag{48}$$

and set

$$z_i = d_1^{(i)} + d_2^{(i)}\theta. \tag{49}$$

If $z \in B'$ then $f(z+z_1)\ldots f(z+z_k) \neq 0$, and by the definition of η and the multiplicativity of γ, the product in (46) is

$$\gamma\big(f(z+z_1)\big)\ldots\gamma\big(f(z+z_k)\big) = \gamma\big(f(z+z_1)\ldots f(z+z_k)\big).$$

Then from (46) we get

$$\sum_{\mathbf{x}\in B} \eta(\mathbf{x}+\mathbf{d_1})\ldots\eta(\mathbf{x}+\mathbf{d}_\ell) = \sum_{z\in B'} \gamma\left(f(z+z_1)\ldots f(z+z_\ell)\right) \tag{50}$$

Now we need the following result of Winterhof:

Lemma 10 *Let p be a prime, $n \geq 1$ be an integer, $q = p^n$ and let $v_1, v_2, \dots, v_n$ be a basis of the vector space $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. Let χ be a multiplicative character of $\mathbb{F}_q$ of order $d > 1$, $f \in \mathbb{F}_q[x]$ be a nonconstant polynomial which is not a d-th power of a polynomial of $\overline{\mathbb{F}}_p[x]$ and which has m distinct zeros in its splitting field over $\mathbb{F}_q$, and $k_1, \dots, k_n$ are non-negative integers with $k_1 \leq p, \dots, k_n \leq p$, then, writing $B = \left\{ \sum_{i=1}^{n} x_i v_i : \ 0 \leq j_i < k_i \right\}$, we have*

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

Proof of Lemma 10 This is a part of Theorem 2 in [17] (where its proof was based on A. Weil's theorem [16]).

Write $h(z) = f(z+z_1) \dots f(z+z_k)$. Then in order to prove (45), it suffices to show:

Lemma 11 *$h(x)$ has at least one zero in $\overline{\mathbb{F}}_p$ whose multiplicity is odd.*

Proof of Lemma 11 Since $z_1, z_2, \dots, z_\ell$ are different the irreducible polynomials $f(z+z_1), \dots, f(z+z_\ell)$ are different. (Indeed, the coefficients of x^{k-1} are different.) So $h(x)$ has a zero in $\overline{\mathbb{F}}_q$ whose multiplicity is odd. Thus $h(x)$ cannot be the constant multiple of a square. Applying Lemma 10 we obtain from (50)

$$\sum_{x \in B} \eta(\mathbf{x} + \mathbf{d_1}) \dots \eta(\mathbf{x} + \mathbf{d}_\ell) \ll k\ell p (1 + \log p)^2 \ll k\ell N^{1/2} (\log N)^2,$$

which was to be proved.

In [7] we reduced the two dimensional case to the one dimensional one by the following way: To any 2-dimensional binary p-lattice

$$\eta(\underline{x}) : \ I_p^2 \to \{-1, +1\} \tag{51}$$

we may assign a unique binary sequence $E_{p^2} = E_{p^2}(\eta) = \{e_1, e_2, \dots, e_{p^2}\} \in \{-1, +1\}^{p^2}$ by taking the first (from the bottom) row of the lattice (51) then we continue the binary sequence by taking the second row of the lattice, then the third row follows, etc.; in general, we set

$$e_{ip+j} = \eta((j-1, i)) = \gamma(f((j-1) + i\theta))$$
$$\text{for } i = 0, 1, \dots, p-1,\ j = 1, 2, \dots, p.$$

Thus we obtain a sequence of length p^2

$$E_{p^2} \stackrel{\text{def}}{=} \{e_1, e_2, \dots, e_{p^2}\}.$$

Now $N < p^2 < 4N$. Consider the first N elements of E_{p^2}, they form a sequence of length N:

$$E_N \stackrel{\text{def}}{=} \{e_1, e_2, \dots, e_N\}.$$

We state that E_N satisfies the conditions of the lemma.

First we estimate $|V(E_N, M, D)|$. Let $m_p(x)$ denote the unique integer x for which

$$m_p(x) \equiv x \pmod p, \quad 0 \le m_p(x) < p.$$

Then

$$e_{n+d_i} = e_{\left[\frac{n+d_i-1}{p}\right]p + m_p(n+d_i-1)+1}$$

and so

$$\begin{aligned} e_{n+d_i} &= \eta\left(m_p(n+d_i-1), \left[\frac{n+d_i-1}{p}\right]\right) \\ &= \gamma\left(f\left(n+d_i-1+\left[\frac{n+d_i-1}{p}\right]\theta\right)\right). \end{aligned} \tag{52}$$

If $1 \leq n \leq M < p$ then $\left[\frac{n+d_i-1}{p}\right]$ may take two different values, namely q_i and $q_i + 1$. Indeed, define q_i and s_i by $d_i = q_i p + s_i$ where $0 \leq s_i \leq p-1$. Then

$$\begin{aligned}\left[\frac{n+d_i-1}{p}\right] &= \left[\frac{q_i p + s_i + n - 1}{p}\right] = q_i + \left[\frac{s_i + n - 1}{p}\right] \\ &= \begin{cases} q_i & \text{if } n \leq p - s_i, \\ q_i + 1 & \text{if } n > p - s_i. \end{cases}\end{aligned}$$

Moreover there exists a number $b_i = \min\{M, p - s_i\}$ such that for $n \leq b_i \leq M$ $\left[\frac{n+d_i-1}{p}\right] = q_i$ and for $b_i < n \leq M$ we have $\left[\frac{n+d_i-1}{p}\right] = q_i + 1$. Let $I_i = [0, b_i]$, $J_i = [b_i + 1, M]$ (if $b_i = M$ then $J_i = \emptyset$).

Then $\{1, b_1 + 1, b_2 + 1, \ldots, b_\ell + 1, M + 1\}$ is a multiset which contains integers $1 = c_1 < c_2 < \cdots < c_m = M + 1$ with $m \leq \ell + 2$. Then $[0, M] = \cup_{j=1}^{m-1} [c_j, c_{j+1} - 1]$.

$$V(E_N, M, D) = \sum_{n=1}^{M} e_{n+d_1} \ldots e_{n+d_\ell} = \sum_{j=1}^{m-1} \sum_{n \in [c_j, c_{j+1}-1]} e_{n+d_1} \ldots e_{n+d_\ell} \tag{53}$$

By the definition of the c_j's, $c_j < b_i + 1 < c_{j+1}$ is not possible, thus $c_{j+1} - 1 \leq b_i$ or $b_i \leq c_j - 1$, so $[c_j, c_{j+1} - 1] \subseteq [0, b_i]$ or $[c_j, c_{j+1} - 1] \subseteq [b_i + 1, M]$. Each interval $[c_j, c_{j+1} - 1]$ is either $\subseteq I_i$ or $\subseteq J_i$ for every $1 \leq i \leq \ell$. Thus for every $d_1, d_2, \ldots, d_\ell$ and for every interval $[c_j, c_{j+1} - 1]$ there exist fixed numbers $h_1, h_2, \ldots, h_\ell$ (depending only on $d_1, d_2, \ldots, d_\ell$ and j) such that for

$n \in [c_j, c_{j+1}-1]$

$$\begin{aligned} e_{n+d_1}e_{n+d_2}\dots e_{n+d_\ell} &= \gamma\left(f(n+d_1-1+h_1\theta)\right)\gamma\left(f(n+d_2-1+h_2\theta)\right)\dots \\ &\quad \gamma\left(f(n+d_\ell-1+h_\ell\theta)\right) \\ &= \gamma\Big(f(n+d_1-1+(h_1+1)\theta)f(n+d_2-1+(h_2+1)\theta) \\ &\quad \dots f(n+d_\ell-1+(h_\ell+1)\theta)\Big). \end{aligned}$$

Hence

$$\begin{aligned} &\sum_{n\in[c_j,c_{j+1}-1]} e_{n+d_1}\dots e_{n+d_\ell} \\ &= \sum_{n\in[c_j,c_{j+1}-1]} \gamma\left(f(n+d_1-1+h_1\theta)\cdots f(n+d_\ell-1+h_\ell\theta)\right). \end{aligned} \tag{54}$$

Next we prove that the irreducible polynomials $f(x+d_1-1+h_1\theta), \cdots, f(x+d_\ell-1+h_\ell\theta)$ are different. Since if $i \neq j$ and

$$f(x+d_i-1+h_i\theta) = f(x+d_j-1+h_j\theta),$$

then

$$h_i \equiv h_j \pmod p \text{ and } d_i \equiv d_j \pmod p. \tag{55}$$

This can be proved by considering the coefficient x^{k-1} in the polynomials $f(x+d_i-1+h_i\theta)$ and $f(x+d_j-1+h_j\theta)$. By (52) we have $h_i = \left[\frac{n+d_i-1}{p}\right]$ and $h_j = \left[\frac{n+d_j-1}{p}\right]$ for $n \in [c_j, c_{j+1}-1]$. $h_i \equiv h_j \pmod p$, by $0 \leq h_i = \left[\frac{n+d_i-1}{p}\right]$, $h_j = \left[\frac{n+d_j-1}{p}\right] < p$ then $h_i = h_j$. So for $n \in [c_j, c_{j+1}-1]$

$$\left[\frac{n+d_i-1}{p}\right] = \left[\frac{n+d_j-1}{p}\right] \tag{56}$$

By (55),

$$n+d_i-1 \equiv n+d_j-1 \pmod p. \tag{57}$$

We get from (56) and (57) that

$$n + d_i - 1 = n + d_j - 1$$

So

$$d_i = d_j$$

which is a contradiction. Thus

$$q_j(x) \overset{\text{def}}{=} f(x + d_1 - 1 + h_1\theta)f(x + d_2 - 1 + h_2\theta) \cdots f(x + d_\ell - 1 + h_\ell\theta) \quad (58)$$

has no multiple root. Here by definition $f(x) \notin \mathbb{F}_p[x]$, by using Lemma 6 $q_j(x) \notin \mathbb{F}_p[x]$ and it has no multiple root. Thus it is not of the form $cg(x)h^2(x)$ with $c \in \mathbb{F}_p$, $g(x) \in \mathbb{F}_p[x]$, $h(x) \in \mathbb{F}_q[x]$. By the triangle inequality, Lemma 4, (53), (54) and (58) we get

$$\begin{aligned} |V(E_N, M, D)| &\le \sum_{j=1}^{m-1} \left| \sum_{n \in [c_j, c_{j+1}-1]} \gamma(q_j(n)) \right| \ll \sum_{j=1}^{m-1} (\deg\, q_j) p^{1/2} \log p \\ &\ll \ell(\deg\, q_j) p^{1/2} \log p \ll \ell^2 k p^{1/2} \log p \\ &\ll \ell^2 k N^{1/4} \log N \end{aligned}$$

which proves (7), since we may choose $\deg f = k$ as $k = 4$.

Next we prove (8). By Lemma 9 we have $Q_\ell(\eta) \ll k\ell N^{1/2}(\log N)^2$. By Theorem 3 (which we will prove later) $C_\ell(E_N) \ll C_\ell(E_{p^2}) \ll k\ell^2 N^{1/2}(\log N)^2 \ll k\ell N^{1/2}(\log N)^2$, since k can be chosen as $k = 4$ this proves (8).

Next we prove (9). We split E_N into $\left[\frac{N-1}{p}\right] + 1$ different subsequences: $E^{(1)} = \{e_1, e_2, \dots, e_p\}$, $E^{(2)} = \{e_{p+1}, e_{p+2}, \dots, e_{2p}\}, \dots,$ $E^{\left(\left[\frac{N-1}{p}\right]+1\right)} =$

$\{e_{([\frac{N-1}{p}]p+1)}, \dots, e_N\}$. By the triangle-inequality

$$W(E_N) \leq \sum_{j=1}^{[\frac{N-1}{p}]+1} W(E_j). \tag{59}$$

Here $E_j = \{e_{(j-1)p+1}, \dots, e_{jp}\} = \{f_1, f_2, \dots, f_p\}$ for $1 \leq j \leq \left[\frac{N-1}{p}\right]$ and $E_j = \{e_{(j-1)p+1}, \dots, e_N\} = \{f_1, f_2, \dots, f_{N-(j-1)p}\}$ for $j = \left[\frac{N-1}{p}\right] + 1$. By Lemma 4

$$\begin{aligned} W(E_j) &= \max_{a,b,t} \left| \sum_{n=0}^{t} f_{a+bn} \right| = \max_{a,b,t} \left| \sum_{n=0}^{t} e_{(j-1)p+a+bn} \right| \\ &= \max_{a,b,t} \left| \sum_{n=0}^{t} \gamma \left(f \left((j-1)p + a + bn - 1 + \left(j - 1 + \left[\frac{a+bn-1}{p} \right] \right) \theta \right) \right) \right| \\ &= \max_{a,b,t} \left| \sum_{n=0}^{t} \gamma \left(f \left(a + bn + (j-1)\theta \right) \right) \right| \ll kp^{1/2} \log p \ll kN^{1/2} \log N. \end{aligned}$$

By this and (59)

$$W(E_N) \ll \frac{N}{p} kp^{1/2} \log p \ll \frac{N}{N^{1/2}} kN^{1/4} \log N \ll kN^{3/4} \log N.$$

Since k can be chosen as $k = 4$ we proved Theorem 2.

Proof of Theorem 3 For $x \in \mathbb{Z}$ let

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

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

By definition

$$e_{xN+y+1} = \eta(y,x) \text{ for } 0 \leq x \leq N-1,\ 0 \leq y \leq N-1$$

and thus

$$e_n = \eta(m_N(n-1), r_N(n-1)).$$

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

$$e_{n+d_i} = \eta(m_N(n + d_i - 1), r_N(n + d_i - 1)). \tag{60}$$

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

$$r_N(n + d_i - 1) = r_N(n-1) + r_N(d_i)$$

$$m_N(n + d_i - 1) = m_N(n-1) + m_N(d_i)$$

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

$$r_N(n + d_i - 1) = r_N(n-1) + r_N(d_i) + 1$$

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

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

$$r_N(n + d_i - 1) = r_N(n-1) + r_N(d_i)$$

$$m_N(n + d_i - 1) = m_N(n-1) + m_N(d_i) \tag{61}$$

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

$$r_N(n + d_i - 1) = r_N(n-1) + r_N(d_i) + 1$$

$$m_N(n + d_i - 1) = m_N(n-1) + m_N(d_i) - N. \tag{62}$$

Then $\{1, a_1 + 1, a_2 + 1, \ldots, a_\ell + 1, m_N(M-1) + 1, N\}$ is a multiset which contains integers $1 = c_1 < c_2 < \cdots < c_m \le N$ where $m \le \ell + 3$. By (61) and

(62) 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

$$r_N(n+d_i-1) = r_N(n) + r_N(d_i-1) + b_{i,j}$$
$$m_N(n+d_i-1) = m_N(n) + m_N(d_i-1) - f_{i,j} \tag{63}$$

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

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

Thus

$$[0,M] = \cup_{j=1}^{m-1}\{n : \ n = r_N(N-1)N + m_N(n-1) + 1,$$
$$c_j \le m_N(n-1) \le c_{j+1}-1, \ r_N(n-1) \in \{0,1,2,\dots,T_j\}\} \tag{64}$$

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, (60) and (61)

$$V(E_N,M,D) = \sum_{n=1}^{M} e_{n+d_1}\dots e_{n+d_\ell} = \sum_{j=1}^{m-1} \sum_{\substack{c_j \le m_N(n-1) \le c_{j+1}-1 \\ 1 \le n \le M}} e_{n+d_1}\dots e_{n+d_\ell}$$
$$= \sum_{j=1}^{m-1} \sum_{\substack{c_j \le m_N(n-1) \le c_{j+1}-1 \\ 1 \le n \le M}}$$
$$\prod_{i=1}^{\ell} \eta(m_N(n-1) + m_N(d_i) - f_{i,j}, r_N(n-1) + r_N(d_i) + b_{i,j})$$

By (64)

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

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

Using this and (63) we get

$$\begin{aligned} V(E_N, M, D) = &\sum_{j=1}^{m-1} \sum_{x=0}^{T_j} \sum_{y=c_j}^{c_{j+1}-1} \\ &\prod_{i=1}^{\ell} \eta(x + m_N(d_i) - f_{i,j}, y + r_N(d_i) + b_{i,j}) \le (m-1)Q_\ell(\eta) \\ &\le (\ell+2)Q_\ell(\eta) \end{aligned}$$

which was to be proved. Here we used the fact that 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 $1, 2, \ldots, \ell$. Indeed if

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

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

$$N r_N(d_{i_1}) + m_N(d_{i_1}) = N r_N(d_{i_2}) + m_N(d_{i_2})$$

$$d_{i_1} = d_{i_2}$$

which is a contradiction.

References

[1] R. Ahlswede, C. Mauduit, A. Sárközy, *Large families of pseudorandom sequences of k symbols and their complexity, Part I, Part II.*, Lecture

Notes in Computer Science, Springer Berlin / Heidelberg 2006, Volume 4123/2006, 293-325.

[2] N. Alon, Y. Kohayakawa, C. Mauduit, C.G. Moreira, V. Rödl, *Measures of pseudorandomness for finite sequences: typical values*, Proc. Lond. Math. Soc. (3) 95 (2007), no. 3, 778–812.

[3] J. Bourgain, T. Cochrane, J. Paulhus and C. Pinner, *On the parity of k-th powers mod p, a generalization of a problem of Lehmer*, Acta Arith. 147 (2011), 173-203.

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

[5] C. F. Gauss, *Untersuchungen Über höhere Arithmetik*, Chelsea publishing company, second edition, reprinted, New York 1981.

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

[7] K. Gyarmati, C. Mauduit, A. Sárközy, *Pseudorandom binary sequences and lattices*, Acta Arith. 135 (2008), 181-197.

[8] K. Gyarmati, A. Sárközy and C. L. Stewart, *On Legendre symbol lattices*, Unif. Distrib. Theory 4 (2009), 81-95.

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

[10] N. M. Katz, *An estimate for character sums*, J. Amer. Math. Soc. Vol 2, No 2 (1989), 197-200.

[11] R. Lidl, H. Niderreiter, *Finite Fields*, Second edition, Cambridge University Press. 1997.

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

[13] C. Mauduit, A. Sárközy, *On large families of pseudorandom binary lattices*, Unif. Distrib. Theory 2 (2007), no. 1, 23-37.

[14] G. I. Perel'muter, I. Shparlinski, *Distribution of primitive roots in finite fields* Uspechi Matem. Nauk 45 (1990), no. 1, 185-186 (in Russian).

[15] D. Wan, *Generators and irreducible polynomials over finite fields*, Math. Comput. 66 (219) (1997), 1195-1212.

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

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

Katalin Gyarmati

Eötvös Loránd University

Department of Algebra and Number Theory

H-1117 Budapest, Pázmány Péter sétány 1/C, Hungary e-mail: gykati@cs.elte.hu

fax: 36-13812146