Uniform Distribution Theory **4** (2009), no.2, 59–80

uniform distribution theory

CONSTRUCTIONS OF PSEUDORANDOM BINARY LATTICES

Katalin Gyarmati — Christian Mauduit — András Sárközy

ABSTRACT. Three constructions for binary lattices with strong pseudorandom properties are given. These constructions are the two dimensional extensions and modifications of three of the most important one dimensional constructions. The upper estimates for the pseudorandom measures of the binary lattices constructed are based on the principle that character sums in two variables can be estimated by fixing one of the variables, then we get a character sum in one variable which can be estimated by using Weil's theorem.

Communicated by Robert F. Tichy

1. Introduction

Pseudorandom binary sequences have many applications. In particular, they are used as the key stream in the classical stream cipher called Vernam cipher and in wireless communication. In 1997 Mauduit and Sárközy [19] (see also the survey paper [27]) initiated a new, constructive approach to the theory of pseudorandomness. They defined and studied new measures of pseudorandomness. In the last 10 years numerous binary sequences have been tested for pseudorandomness. The 4 best constructions are, perhaps, the following:

Let p be a prime number, $f(x) \in \mathbb{F}_p[x]$, and define the binary sequence

$$E_p = (e_1, e_2, \ldots, e_p)$$

2000 Mathematics Subject Classification: 11K45.
Keywords: pseudorandomness, binary lattice, multiplicative inverse, character sum.
Research was partially supported by Hungarian National Foundation for Scientific Research, Grants No. K67676, K72731 and PD72264, French-Hungarian exchange program F-06/48, and the János Bolyai Research Fellowship.

by

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

where $\left(\frac{f(n)}{p}\right)$ is the Legendre symbol (see [7], [19], [28] and [29]),

$$e_n = \begin{cases} +1 & \text{if } 0 \le r_p\big(f(n)\big) < p/2, \\ -1 & \text{if } p/2 \le r_p\big(f(n)\big) < p, \end{cases} \tag{2}$$

where $r_p(n)$ denotes the unique $r \in \{0,1,\dots,p-1\}$ such that $n \equiv r \pmod p$ (see [18]),

$$e_n = \begin{cases} +1 & \text{if } \big(f(n),p\big)=1 \text{ and } 0 \le r_p\left(f(n)^{-1}\right) < p/2, \\ -1, & \text{otherwise,} \end{cases} \tag{3}$$

where $f(n)^{-1}$ denotes the multiplicative inverse of $f(n)$ (see [20]) and

$$e_n = \begin{cases} +1 & \text{if } \big(f(n),p\big)=1 \text{ and } 1 \le \operatorname{ind} f(n) \le \frac{p-1}{2}, \\ -1, & \text{otherwise,} \end{cases} \tag{4}$$

where ind a denotes the index or discrete logarithm of a modulo p with respect to a given primitive root modulo p (see [8], [9], [10], [26]). (See [15], [16], [17], [23], [24], [25] for further related results and constructions.)

In order to encrypt a 2-dimensional digital map or picture via the analog of the Vernam cipher, instead of a pseudorandom binary sequence (as a key stream) one needs a pseudorandom "binary lattice". Thus one needs the n dimensional extension of the theory of pseudorandomness. Such a theory has been developed recently by Hubert, Mauduit and Sárközy [14]. 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 [13] 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

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

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

In [14] the definition of binary sequences is extended to more dimensions by considering functions of type

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

If $\mathbf{x} = (x_1, \dots, x_n)$ so that $\eta(\mathbf{x}) = \eta((x_1, \dots, x_n))$, then we will 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.

In [14] Hubert, Mauduit and Sárközy 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 [13]):

Definition 1. Let

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

Define the pseudorandom measure of order ℓ of η by

$$Q_\ell(\eta) = \max_{B, \mathbf{d_1}, \dots, \mathbf{d}_\ell} \left| \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d_1}) \dots \eta(\mathbf{x} + \mathbf{d}_\ell) \right|, \tag{5}$$

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

Then η is said to have strong pseudorandom properties, or briefly, it is considered as a "good" pseudorandom lattice if for fixed n and ℓ and "large" N the measure $Q_\ell(\eta)$ is "small" (much smaller, then the trivial upper bound N^n). This terminology is justified by the fact that, as was proved in [14], 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.

In one dimension, hence the case of binary sequences, many good constructions have been given. Typically, the really good constructions involve $\mathbb{F}_p$, additive or multiplicative characters and polynomials, and the crucial tool in the estimation of the pseudorandom measures is Weil's theorem [30]. Unfortunately, this approach in its original form does not readily apply in n dimensions. The difficulty is that in n dimensions constructions involving $\mathbb{F}_p$, characters and polynomials $f(x_1, x_2, \dots, x_n) \in \mathbb{F}_p[x_1, x_2, \dots, x_n]$ lead naturally to the n dimensional analogues of Weil's theorem, in particular, they lead to the theorem of Deligne [4]. While Fouvry and Katz [6] have simplified the requirements for applying Deligne's theorem, the inconvenient assumptions of nonsingularity are still required.

In spite of these difficulties in [14], [21], [22] good n-dimensional constructions were presented. In these papers the authors got around the difficulty described

above in the following way: finite fields $\mathbb{F}_q$ with $q = p^n$ and polynomials $G(x) \in \mathbb{F}_q[x]$ are considered. Character sums involving $G(x)$ and characters of $\mathbb{F}_q$ can be estimated by Weil's theorem so that no nonsingularity assumption is needed. On the other hand, if $e_1, e_2, \dots, e_n$ is a basis in $\mathbb{F}_q$, then every $x \in \mathbb{F}_q$ has a unique representation in form

$$x = x_1e_1 + x_2e_2 + \cdots + x_ne_n \quad \text{with} \quad x_1, x_2, \dots, x_n \in \mathbb{F}_q.$$

Then

$$g(x_1, x_2, \dots, x_n) = G(x_1e_1 + x_2e_2 + \cdots + x_ne_n) \in \mathbb{F}_p[x_1, x_2, \dots, x_n]$$

is a well-defined polynomial, and the estimate of n-fold character sums involving $g(x_1, x_2, \dots, x_n)$ can be reduced to the estimate of character sums over $\mathbb{F}_q$ involving G, so that Weil's theorem can be used. (This principle goes back to Davenport and Lewis [3].)

This detour enables one to give sharp upper bounds, but it also has considerable disadvantages. Namely, in this way we get rather artificial constructions. More naturally arising constructions cannot be tested with this approach. Secondly, the implementation of these artificial constructions is more complicated. Thus one might like to look for a trade-off between applicability of the method and sharpness of the result, i.e., for a method which is much more flexible and applicable at the expense of providing weaker but still nontrivial upper bounds. In [13], for $n = 2$ Gyarmati, Sárközy and Stewart presented such a method based on the techniques introduced by Gyarmati and Sárközy [12] to estimate certain related character sums involving polynomials $f(x, y) \in \mathbb{F}_p[x, y]$. They estimate these sums by fixing one of the two variables, say, x. Then $g(y) = f(x, y)$ is a polynomial of one variable, so that one may try to apply Weil's theorem to estimate the sum. Indeed, they show that apart from a few "bad" polynomials $f(x, y)$ (they give a simple and complete description of these exceptional polynomials), for "almost all" x we get a sum in y in this way which can be estimated by Weil's theorem. However, the price paid for the flexibility of this method is that the upper bounds are not optimal (we get an upper bound p^c with some $1 < c < 2$ so that it improves on the trivial upper bound p^2 but it is worse than the expected optimal bound $p(\log p)^c$). In [13] this method was used for the following two dimensional analogue of the Legendre symbol construction (1): Let p be an odd prime, $f(x, y) \in \mathbb{F}_p[x, y]$ be a polynomial of degree k, and define the two dimensional binary p-lattice $\eta : \ I_p^2 \to \{-1, +1\}$ by

$$\eta(x, y) = \begin{cases} \left(\frac{f(x,y)}{p}\right) & \text{if } \ \big(f(x, y), p\big) = 1, \\ 1 & \text{if } \ p \mid f(x, y). \end{cases}$$

They showed for a large class of polynomials f that if k, ℓ are "not very large" in terms of p then we have

$$Q_\ell(\eta) < 10k\ell p^{3/2} \log p.$$

In this paper our goal is to prove similar theorems on suitable extensions of constructions of (2), (3) and (4). Some elementary lemmas (Lemmas 3 and 7) of independent interest will play a crucial role in the proofs.

Throughout this paper we will use the following notations: $\mathbb{Z}$ and $\mathbb{N}$ denote the set of the integers, resp. positive integers. p denotes an odd prime. We write $e(\alpha) = e^{2\pi i\alpha}$ and $e_p(n) = e\left(\frac{n}{p}\right)$. We will use Vinogradov's notation $\ll$: if $f(x) = O(g(x))$ then we also write $f(x) \ll g(x)$.

2. The two dimensional analogue of construction (2)

We will prove the following theorem:

Theorem 1. *Let p be an odd prime, k an integer with $3 \le k < p$, $g(x) \in \mathbb{F}_p[x]$ and $h(x) \in \mathbb{F}_p[x]$ polynomials with $\deg f = \deg g = k$, and write $f(x,y) = g(x)h(y)$. Define the two dimensional binary p-lattice $\eta : I_p^2 \to \{-1, +1\}$ by*

$$\eta(x,y) = \begin{cases} 1 & \text{if } 0 \le r_p\big(f(x,y)\big) < p/2, \\ -1 & \text{if } p/2 \le r_p\big(f(x,y)\big) < p. \end{cases} \tag{6}$$

Then for $\ell \in \mathbb{N}$,

$$2 \le \ell \le k-1 \tag{7}$$

we have

$$Q_\ell(\eta) \ll kp^{3/2}(\log p)^{\ell+1}. \tag{8}$$

Note that it was shown in [18] that in the one-dimensional case (2) the correlation of "large" order can be large, so that an upper bound for ℓ like the one in (7) is necessary. It could be shown that here the situation is similar but we will not go into the details.

Proof of Theorem 1. The proof will be based on the same lemmas as in the one dimensional case in [18].

Lemma 1. *For any polynomial $F(x) \in \mathbb{F}_p[x]$ of degree $d \ge 2$ and any integers M and K with $1 \le K < p$ we have*

$$\left| \sum_{n=M+1}^{M+K} e_p\big(F(n)\big) \right| \ll dp^{1/2} \log p.$$

P r o o f. This is a consequence of Weil's theorem [30] and it is Lemma 1 in [18]. □

Lemma 2. *For $n \in \mathbb{Z}$ and p an odd prime we have*

$$\frac{1}{p}\sum_{|h|<p/2} v_p(h)e_p(hn) = \begin{cases} +1 & \text{if } r_p(n) < p/2, \\ -1, & \text{otherwise,} \end{cases}$$

where $v_p(h)$ is a function of period p such that

$$v_p(0) = 1, \quad \text{and} \quad v_p(h) = 1 + i\frac{(-1)^h - \cos(\pi h/p)}{\sin(\pi h/p)} \quad \text{for} \quad 1 \le |h| < p/2.$$

Furthermore, $v_p(h)$ satisfies

$$v_p(h) = \begin{cases} O(1) & \text{if } h \text{ is even,} \\ -\frac{2ip}{\pi h} + O(1) & \text{if } h \text{ is odd.} \end{cases}$$

P r o o f. This is Lemma 2 in [18]. □

Lemma 3. *Let p be a prime, $1 \le k < p$, $F(x) \in \mathbb{F}_p[x]$ of degree $d \ge k$, and let $x_1, x_2, \dots, x_k$ be k different elements of $\mathbb{F}_p$. Then for all $(a_1, \dots, a_k) \in \mathbb{F}_p^k \setminus (0, \dots, 0)$, the polynomial*

$$G(x) \stackrel{def}{=} a_1F(x + x_1) + \cdots + a_kF(x + x_k)$$

is of degree $\ge d - k + 1$.

P r o o f. This is Lemma 3 in [18]. □

By (6) and Lemma 2 we have

$$\eta(x, y) = \frac{1}{p}\sum_{|h|<p/2} v_p(h)e_p\left(h\big(f(x, y)\big)\right). \tag{9}$$

Now consider the sum $S(B, \mathbf{d_1}, \dots, \mathbf{d}_\ell)$ in the definition of $Q_\ell(\eta)$ in (5), and write

$$B = \{(xz_1, yz_2) : \ 0 \le xz_1 \le t_1(< p), \ 0 \le yz_2 \le t_2(< p)\},$$
$$\mathbf{d_i} = (r_i, s_i) \ \text{ for } \ i = 1, 2, \dots, \ell,$$

so that, by (9),

$$
\begin{aligned}
&|S(B, \mathbf{d_1}, \dots, \mathbf{d}_\ell)| \\
&= \left| \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d_1}) \cdots \eta(\mathbf{x} + \mathbf{d}_\ell) \right| \\
&= \left| \sum_{0 \le x \le t_1/z_1} \sum_{0 \le y \le t_2/z_2} \eta(xz_1 + r_1, yz_2 + s_1) \cdots \eta(xz_1 + r_\ell, yz_2 + s_\ell) \right| \\
&= \Bigg| \sum_{x=0}^{[t_1/z_1]} \sum_{y=0}^{[t_2/z_2]} \frac{1}{p^\ell} \sum_{|h_1|<p/2} \cdots \sum_{|h_\ell|<p/2} v_p(h_1) \cdots v_p(h_\ell) \\
&\qquad e_p\big(h_1 f(xz_1 + r_1, yz_2 + s_1) + \cdots + h_\ell f(xz_1 + r_\ell, yz_2 + s_\ell)\big) \Bigg| \\
&\le \frac{1}{p^\ell} \sum_{|h_1|<p/2} \cdots \sum_{|h_\ell|<p/2} |v_p(h_1)| \cdots |v_p(h_\ell)| \\
&\qquad \sum_{x=0}^{[t_1/z_1]} \left| \sum_{y=0}^{[t_2/z_2]} e_p\big(H(x, y, h_1, \dots, h_\ell)\big) \right|, \qquad (10)
\end{aligned}
$$

where

$$
\begin{aligned}
H(x, y, h_1, \dots, h_\ell) &= h_1 f(xz_1 + r_1, yz_2 + s_1) + \cdots + h_\ell f(xz_1 + r_\ell, yz_2 + s_\ell) \\
&= h_1 g(xz_1 + r_1) h(yz_2 + s_1) + \cdots + h_\ell g(xz_1 + r_\ell) h(yz_2 + s_\ell). \qquad (11)
\end{aligned}
$$

Now we group the terms according to the value of s_i. More precisely, denote the distinct values occurring among $s_1, \dots, s_\ell$ by $s'_1, \dots, s'_t$, and for $1 \le j \le t$ write

$$I_j = \{i : \ 1 \le i \le \ell, \ s_i = s'_j\}.$$

Then (11) can be rewritten as

$$H(x, y, h_1, \dots, h_\ell) = \sum_{j=1}^{t} \left(\sum_{i \in I_j} h_i g(xz + r_i) \right) h(yz + s'_j). \qquad (12)$$

Now consider an ℓ-tuple $(h_1, h_2, \dots, h_\ell)$ with

$$(h_1, h_2, \dots, h_\ell) \ne (0, 0, \dots, 0). \qquad (13)$$

Let J denote the set of the integers $1 \le j \le t$ such that there is at least one $i \in I_j$ with $h_i \neq 0$. Then by (13), the set J is nonempty, so that clearly we have

$$0 < |J| \le t \le \ell. \tag{14}$$

For $j \in J$ write

$$u_j(y) = \sum_{i \in I_j} h_i g(y + r_i) \quad \text{and} \quad U_j(x) = u_j(xz_1) = \sum_{i \in I_j} h_i g(xz_1 + r_i).$$

Then (12) can be rewritten as

$$H(x, y, h_1, \dots, h_\ell) = \sum_{j \in J} U_j(x) h(yz_2 + s'_j), \tag{15}$$

where by Lemma 3 and (7) (and since $z_1 \neq 0$),

$$\deg U_j(x) = \deg u_j(y) \ge \deg g(x) - |I_j| + 1 \ge k - \ell + 1 \ge 2,$$

and clearly,

$$\deg U_j(x) \le \deg g(x) = k \tag{16}$$

(for every $j \in J$). Denote the set of the zeros of $U_1(x)$ (which exist by (14)) by $\mathcal{X}$. Then for any fixed x with $x \in \mathbb{F}_p \setminus \mathcal{X}$ we have $U_1(x) \neq 0$, thus again by Lemma 3 and (7) (and $z_2 \neq 0$) as before, the polynomial

$$K_{x,h_1,\dots,h_\ell}(y) \stackrel{\text{def}}{=} \sum_{j \in J} U_j(x) h(yz_2 + s'_j)$$

in (15) is of degree

$$\deg K_{x,h_1,\dots,h_\ell}(y) \ge \deg h(y) - |J| + 1 \ge k - \ell + 1 \ge 2,$$

so the last sum in (10) can be estimated by using Lemma 1. Then estimating the contribution of $h_1 = \cdots = h_\ell = 0$, resp. the x values with $x \in \mathcal{X}$ in the trivial way, by Lemma 1, Lemma 2 and (16) we get from (10):

$$\begin{aligned} |S(B, \mathbf{d_1}, \dots, \mathbf{d}_\ell)| &\ll \frac{1}{p^\ell} \left(p^2 + \left(\sum_{|h| < p/2} |v_p(h)| \right)^\ell \left(|\mathcal{X}|\, p + \sum_{x \in \mathbb{F}_p \setminus \mathcal{X}} k p^{1/2} \log p \right) \right) \\ &\ll \frac{1}{p^\ell} \Big(p^2 + p^\ell (\log p)^\ell \Big(kp + kp^{3/2} \log p \Big) \Big) \ll k p^{3/2} (\log p)^{\ell+1} \end{aligned}$$

which proves (8). □

3. A two dimensional construction using the multiplicative inverse

Now we will present a two dimensional analogue of construction (3). Throughout this section p will denote a fixed odd prime. If $f(x,y) \in \mathbb{F}_p[x,y]$, then the function $g(x,y) = \frac{1}{f(x,y)}$ is defined on those pairs $(a,b) \in \mathbb{F}_p \times \mathbb{F}_p$ for which $f(a,b) \neq 0$, and then $g(a,b)$ is defined as the multiplicative inverse of $f(a,b) \pmod p$, denoted by $f(a,b)^{-1}$.

Theorem 2. *Let $k \in \mathbb{N}$, $k < p$. Assume that $g(x) \in \mathbb{F}_p[x]$ and $h(x) \in \mathbb{F}_p[x]$ have degree k and no multiple zero in $\overline{\mathbb{F}}_p$. Write $f(x,y) = g(x)h(y)$, and define the two dimensional binary p-lattice $\eta : I_p^2 \to \{-1,+1\}$ by*

$$\eta(x,y) = \begin{cases} +1 & \text{if } (f(x,y),p) = 1 \text{ and } 0 \le r_p\left(f(x,y)^{-1}\right) < p/2, \\ -1 & \text{otherwise.} \end{cases}$$

Assume also that $\ell \in \mathbb{N}$ with $2 \le \ell \le p$, and one of the following conditions holds:

(i) $\ell = 2$,

(ii) $(4k)^\ell < p$.

Then we have

$$Q_\ell(\eta) \ll \ell k p^{3/2} (\log p)^{\ell+1}. \tag{17}$$

Proof of Theorem 2. Some parts of the proof will be similar to the proof of Theorem 1, thus we will leave some details to the reader. We will use again Lemma 2, but Lemmas 1 and 3 will be replaced by the following two lemmas:

Lemma 4. *Let p be a prime, let Q/R be a nonzero rational function over $\mathbb{F}_p$, and let s be the number of distinct roots of the polynomial R in $\overline{\mathbb{F}}_p$. Furthermore, let ψ be a nontrivial additive character of $\mathbb{F}_p$ and $1 \le N < p$. If $\deg Q < \deg R$, then*

$$\left| \sum_{\substack{0 \le n < N \\ R(n) \neq 0}} \psi\left(\frac{Q(n)}{R(n)}\right) \right| < (\deg R + s) p^{1/2} \left(\frac{4}{\pi^2} \log p + 0.38 + \frac{0.64}{p} \right) + \frac{N}{p} \left((\deg R + s - 2) p^{1/2} + 1 \right).$$

(Here and in what follows, $\frac{Q(n)}{R(n)}$ is defined for $R(n) \neq 0$ as $Q(n)R(n)^{-1}$, where again $R(n)^{-1}$ is the multiplicative inverse of $R(n)$ in $\mathbb{F}_p$.)

Proof. This is a part of Theorem 2 of Eichenauer-Hermann and Niederreiter in [5]. □

Lemma 5. *Assume that k, ℓ are defined as in Theorem 2, $M \in \mathbb{N}$, $M \le p$, $F(x) \in \mathbb{F}_p[x]$ has degree k, $r \in \mathbb{N}$, $r \le \ell$, $H_1, \dots, H_r$ are integers with $0 < |H_i| < p$ for $i = 1, \dots, r$, and $D_1, \dots, D_r$ are integers with $0 \le D_1 < \dots < D_r < p$. Then writing*

$$Q_{H_1,\dots,H_r}(n) = \sum_{t=1}^{r} H_t \prod_{\substack{1 \le j \le r \\ j \ne t}} F(n + D_j)$$

and

$$R_{H_1,\dots,H_r}(n) = \prod_{j=1}^{r} F(n + D_j)$$

(so that $\deg R_{H_1,\dots,H_r}(n) = kr$*), we have*

$$H_1 F(n + D_1)^{-1} + \dots + H_r F(n + D_r)^{-1} = \frac{Q_{H_1,\dots,H_r}(n)}{R_{H_1,\dots,H_r}(n)}$$

(in $\mathbb{F}_p$) for every n with $F(n + D_1) \ne 0, \dots, F(n + D_r) \ne 0$ or, equivalently $R_{H_1,\dots,H_r}(n) \ne 0$, and here the polynomial $Q_{H_1,\dots,H_r}(n)$ is not the 0 polynomial over $\mathbb{F}_p$.

P r o o f. Apart from the notation, this is Lemma 5 in [20]. □

Now define $B, \mathbf{d_1}, \dots, \mathbf{d}_\ell$ and $S(B, \mathbf{d_1}, \dots, \mathbf{d}_\ell)$ in the same way as at the beginning of the proof of Theorem 1. In the same way as in (10), we get that

$$\begin{aligned}
&|S(B, \mathbf{d_1}, \dots, \mathbf{d}_\ell)| \\
&= \left| \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d_1}) \dots \eta(\mathbf{x} + \mathbf{d_r}) \right| \\
&= \Bigg| \sum_x \sum_y \frac{1}{p^\ell} \sum_{|h_1| < p/2} \dots \sum_{|h_\ell| < p/2} v_p(h_1) \cdots v_p(h_\ell) e_p\big(h_1 f(xz_1 + r_1, yz_2 + s_1)^{-1} + \dots \\
&\qquad \cdots + h_\ell f(xz_1 + r_\ell, yz_2 + s_\ell)^{-1}\big) \Bigg| + O(k\ell p), \qquad (18)
\end{aligned}$$

where $\sum_x$ denotes the summation over x such that $0 \le x \le t_1/z_1$ and there is no j with $g(xz_1 + r_j) = 0$, $1 \le j \le \ell$; $\sum_y$ denotes the summation over y such that $0 \le y \le t_2/z_2$ and there is no j with $h(yz_2 + s_j) = 0$; finally, the $O(k\ell p)$ term estimates the contribution of the terms with x, y such that

$$f(xz_1 + r_j, yz_2 + s_j) = g(xz_1 + r_j) h(yz_2 + s_j) = 0 \text{ for some } 1 \le j \le \ell. \qquad (19)$$

Indeed, all these terms contribute by a bounded error, and (19) holds if either

$$1 \le j \le \ell,\ g(xz_1 + r_j) = 0 \quad \text{and} \quad x \in \mathbb{F}_p \tag{20}$$

or

$$1 \le j \le \ell,\ h(yz_2 + s_j) = 0 \quad \text{and} \quad y \in \mathbb{F}_p, \tag{21}$$

and both (20) and (21) hold for at most ℓkp triples j, x, y.

It follows from (18) that

$$|S(B, \mathbf{d_1}, \dots, \mathbf{d}_\ell)| \tag{22}$$
$$\le \frac{1}{p^\ell} \sum_{|h_1|<p/2} \dots \sum_{|h_\ell|<p/2} |v_p(h_1)| \dots |v_p(h_\ell)| \sum_x \left| \sum_y e_p(H(x, y, h_1, \dots, h_\ell)) \right|,$$

where

$$H(x, y, h_1, \dots, h_\ell)$$
$$= h_1 g(xz_1 + r_1)^{-1} h(yz_2 + s_1)^{-1} + \dots + h_\ell g(xz_1 + r_\ell)^{-1} h(yz_2 + s_\ell)^{-1}. \tag{23}$$

Now we group the terms in the same way as in (11). Defining $s'_1, \dots, s'_t, I_1, \dots, I_t$ in the same way as there, we get from (23):

$$H(x, y, h_1, \dots, h_\ell) = \sum_{j=1}^{t} \left(\sum_{i \in I_j} h_i g(xz_1 + r_i)^{-1} \right) h(yz_2 + s'_j)^{-1}. \tag{24}$$

Consider an ℓ-tuple $(h_1, h_2, \dots, h_\ell)$ with

$$(h_1, h_2, \dots, h_\ell) \ne (0, 0, \dots, 0). \tag{25}$$

Let J denote the set of the integers $1 \le j \le t$ such that there is at least one $i \in I_j$ with $h_i \ne 0$. Then by (25), the set J is nonempty, so that clearly we have

$$0 < |J| \le t \le \ell. \tag{26}$$

For $j \in J$ write

$$u_j(y) = \sum_{i \in I_j} h_i g(y + r_i)^{-1} \quad \text{and} \quad U_j(x) = u_j(xz_1) = \sum_{i \in I_j} h_i g(xz_1 + r_i)^{-1}.$$

Then (24) can be rewritten as

$$H(x, y, h_1, \dots, h_\ell) = \sum_{j \in J} U_j(x) h(yz_2 + s'_j)^{-1}, \tag{27}$$

where by Lemma 5, $U_j(x)$ is a nonzero rational function whose numerator is of degree

$$\le |J|\, k \le \ell k$$

by (14), thus it has at most ℓk zeros. Denote the set of the zeros of the rational function $U_1(x)$ (which exist by (26)) by $\mathcal{X}$ so that

$$|\mathcal{X}| \le \ell k. \tag{28}$$

Then for any fixed x with $x \in \mathbb{F}_p \setminus \mathcal{X}$ we have $U_1(x) \neq 0$, thus again by Lemma 5 for such an x, the rational function

$$K_{x,h_1,\dots,h_\ell}(y) \stackrel{\text{def}}{=} \sum_{j\in J} U_j(x)h(yz_2 + s'_j)^{-1}$$

in (27) is a nonzero rational function whose denominator is higher degree than its numerator, and its denominator is again of degree $\le |J|\, k \le \ell k$ by (14). Thus for such an x the last sum in (22) can be estimated by using Lemma 4, and then estimating the contribution of $h_1 = \cdots = h_\ell = 0$, resp. the x values with $x \in \mathcal{X}$ in the trivial way, by Lemma 2, Lemma 4 and (28) we get from (22):

$$|S(B, \mathbf{d_1}, \dots, \mathbf{d}_\ell)| \ll \frac{1}{p^\ell}\left(p^2 + \left(\sum_{|h|<p/2} |v_p(h)|\right)^\ell \left(|\mathcal{X}|\, p + \sum_{x\in\mathbb{F}_p\setminus\mathcal{X}} \ell k p^{1/2}\log p\right)\right)$$

$$\ll \frac{1}{p^\ell}\left(p^2 + p^\ell (\log p)^\ell \Big(\ell k p + \ell k p^{3/2}\log p\Big)\right) \ll \ell k p^{3/2}(\log p)^{\ell+1}$$

which proves (17). □

4. A two dimensional construction using the index

In this section we will extend construction (4) to two dimensions. As in [13] this construction can be handled using multiplicative characters. Correspondingly, we will use several ideas from [8], [9], [10], [13] and [26], and we will skip some details.

Throughout this section let p be an odd prime and g be a fixed primitive root modulo p. ind n is defined as the unique integer with

$$g^{\text{ind } n} \equiv n \pmod p, \quad \text{and} \quad 1 \le \text{ind } n \le p-1.$$

Theorem 3. *Let p be an odd prime, $f(x,y) \in \mathbb{F}_p[x,y]$ be a polynomial of degree k. Suppose that $f(x,y)$ is squarefree and it is not of the form*

$$\prod_{j=1}^{r} f_j(\alpha_j x + \beta_j y), \tag{29}$$

where $\alpha_j, \beta_j \in \mathbb{F}_p$ *and* $f_j(x) \in \mathbb{F}_p[x]$ *is a one variable polynomial for* $j = 1, 2, \ldots, r$. *Assume also that* $\ell \in \mathbb{N}$ *and one of the following conditions holds:*

a) $f(x, y)$ *is irreducible,*

b) $\ell = 2$,

c) $(4k)^\ell \le p$.

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

$$\eta(x,y) = \begin{cases} +1 & \text{if } (f(x,y),p) = 1 \text{ and } 1 \le \operatorname{ind} f(x,y) \le \frac{p-1}{2}, \\ -1, & \text{otherwise.} \end{cases} \tag{30}$$

Then

$$Q_\ell(\eta) \ll \ell k p^{3/2} (\log p)^{\ell+1}.$$

We remark that the use of index (discrete logarithm) makes the application of this construction very slow and impractical. However, as in one dimension, one can make this construction much faster and more practical along the lines presented in [8] and [10].

P r o o f o f T h e o r e m 3. The theorem is trivial for $k^2 \gg p$ or $\ell^2 \gg p$, thus we may assume

$$(k + \ell)(k + \ell - 1)/2 \le p.$$

We will use the following lemma.

Lemma 6. *Let* $p \ge 5$ *be a prime and* χ *be a multiplicative character of order* d. *Suppose that* $h(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ *is not of the form* $cg(x_1, x_2)^d$ *with* $c \in \mathbb{F}_p$, $g(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$. *Let* k *be the degree of* $h(x_1, x_2)$. *Then we have*

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

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

P r o o f o f L e m m a 6. This is Lemma 2 in [13]. □

In the same way as in [26] we get

$$\begin{aligned} \eta(x,y) &= \frac{2}{p-1} \sum_{\chi \ne \chi_0} \overline{\chi}(f(x,y)) \sum_{k=1}^{(p-1)/2} \chi^k(g) \\ &= \frac{2}{p-1} \sum_{\chi \ne \chi_0} \overline{\chi}(f(x,y)) \frac{\chi(g) - \chi^{(p+1)/2}(g)}{1 - \chi(g)} \end{aligned} \tag{31}$$

Now consider the sum $S(B, \mathbf{d_1}, \dots, \mathbf{d}_\ell)$ in the definition of $Q_\ell(\eta)$ in (5) and write

$$B = \{(xz_1, yz_2) : \ 0 \le xz_1 \le t_1 (< p), \ 0 \le yz_2 \le t_2 (< p)\},$$
$$\mathbf{d_i} = (r_i, s_i) \text{ for } i = 1, 2, \dots, \ell,$$

so that, by (5),

$$\begin{aligned} &|S(B, \mathbf{d_1}, \mathbf{d_2}, \dots, \mathbf{d}_\ell)| \\ &= \left| \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d_1}) \cdots \eta(\mathbf{x} + \mathbf{d}_\ell) \right| \\ &= \left| \sum_{0 \le x \le t_1/z_1} \sum_{0 \le y \le t_2/z_2} \eta(xz_1 + r_1, yz_2 + s_1) \cdots \eta(xz_1 + r_\ell, yz_2 + s_\ell) \right|. \end{aligned}$$

By this, (31) and the triangle-inequality

$$\begin{aligned} &|S(B, \mathbf{d_1}, \mathbf{d_2}, \dots, \mathbf{d}_\ell)| \le \frac{2^\ell}{(p-1)^\ell} \Bigg| \sum_{0 \le x \le t_1/z_1} \sum_{0 \le y \le t_2/z_2} \sum_{\chi_1 \ne \chi_0} \cdots \sum_{\chi_\ell \ne \chi_0} \\ &\overline{\chi_1}(f(xz_1 + r_1, yz_2 + s_1)) \dots \overline{\chi_\ell}(f(xz_1 + r_\ell, yz_2 + s_\ell)) \prod_{j=1}^{\ell} \frac{\chi_j(g) - \chi_j^{(p+1)/2}(g)}{1 - \chi_j(g)} \Bigg| \\ &\le \frac{2^\ell}{(p-1)^\ell} \sum_{\chi_1 \ne \chi_0} \cdots \sum_{\chi_\ell \ne \chi_0} \Bigg| \sum_{0 \le x \le t_1/z_1} \sum_{0 \le y \le t_2/z_2} \\ &\chi_1(f(xz_1 + r_1, yz_2 + s_1)) \dots \chi_\ell(f(xz_1 + r_\ell, yz_2 + s_\ell)) \Bigg| \left| \prod_{j=1}^{\ell} \frac{1 - \chi_j^{(p-1)/2}(g)}{1 - \chi_j(g)} \right|. \end{aligned} \tag{32}$$

Now, let χ be a generator of the group formulated by the modulo p (multiplicative) characters, e.g., χ can be chosen as the character uniquely defined by $\chi(g) = e\left(\frac{1}{p-1}\right)$. Then the order of χ is $p-1$. Let

$$\chi_u = \chi^{\delta_u} \quad \text{for } u = 1, 2, \dots, \ell, \tag{33}$$

where, by

$$\chi_1 \ne \chi_0, \dots, \chi_\ell \ne \chi_0,$$

we may take

$$1 \le \delta_u < p - 1 \quad \text{for } u = 1, 2, \dots, \ell.$$

Thus in (32) we have

$$\begin{aligned}&\chi_1(f(xz_1+r_1,yz_2+s_1))\ \cdots\ \chi_\ell(f(xz_1+r_\ell,yz_2+s_\ell))\\ =&\chi^{\delta_1}(f(xz_1+r_1,yz_2+s_1))\cdots\chi^{\delta_\ell}(f(xz_1+r_\ell,yz_2+s_\ell))\\ =&\chi(f^{\delta_1}(xz_1+r_1,yz_2+s_1)\ \cdots\ f^{\delta_\ell}(xz_1+r_\ell,yz_2+s_\ell)).\end{aligned}$$

By Lemma 6 it follows that if $f^{\delta_1}(xz_1+r_1,yz_2+s_1)\cdots f^{\delta_\ell}(xz_1+r_\ell,yz_2+s_\ell)$ is not a perfect $(p-1)$-st power, then

$$\begin{aligned}&\left|\sum_{0\le x\le t_1/z_1}\sum_{0\le y\le t_2/z_2}\chi_1(f(xz_1+r_1,yz_2+s_1))\ \cdots\ \chi_\ell(f(xz_1+r_\ell,yz_2+s_\ell))\right|\\ &=\left|\sum_{0\le x\le t_1/z_1}\sum_{0\le y\le t_2/z_2}\chi(f^{\delta_1}(xz_1+r_1,yz_2+s_1)\ \cdots\ f^{\delta_\ell}(xz_1+r_\ell,yz_2+s_\ell))\right|\\ &\ll kp^{3/2}\log p.\end{aligned}$$

By this, (32), (33) and the triangle-inequality we have

$$\begin{aligned}&|S(B,\mathbf{d_1},\mathbf{d_2},\dots,\mathbf{d}_\ell)|\le\frac{2^\ell}{(p-1)^\ell}\sum_{\chi_1\ne\chi_0}\cdots\sum_{\chi_\ell\ne\chi_0}\left|\sum_{0\le x\le t_1/z_1}\sum_{0\le y\le t_2/z_2}\right.\\ &\left.\chi_1(f(xz_1+r_1,yz_2+s_1))\dots\chi_\ell(f(xz_1+r_\ell,yz_2+s_\ell))\right|\left|\prod_{j=1}^{\ell}\frac{1-\chi_j^{(p-1)/2}(g)}{1-\chi_j(g)}\right|\\ &=\frac{2^\ell}{(p-1)^\ell}\sum_{\delta_1=1}^{p-2}\cdots\sum_{\delta_\ell=1}^{p-2}\left|\sum_{0\le x\le t_1/z_1}\sum_{0\le y\le t_2/z_2}\right.\\ &\left.\chi(f^{\delta_1}(xz_1+r_1,yz_2+s_1)\cdots f^{\delta_\ell}(xz_1+r_\ell,yz_2+s_\ell))\right|\left|\prod_{j=1}^{\ell}\frac{1-\chi^{\delta_j(p-1)/2}(g)}{1-\chi^{\delta_j}(g)}\right|\\ &\le\frac{2^\ell}{(p-1)^\ell}\sum_{\delta_1=1}^{p-2}\cdots\sum_{\delta_\ell=1}^{p-2}kp^{3/2}\log p\left|\prod_{j=1}^{\ell}\frac{1-\chi^{\delta_j(p-1)/2}(g)}{1-\chi^{\delta_j}(g)}\right|\\ &+\frac{2^\ell}{(p-1)^\ell}\sum_{\substack{1\le\delta_1,\dots,\delta_\ell\le p-2\\ f^{\delta_1}(xz_1+r_1,yz_2+s_1)\cdots f^{\delta_\ell}(xz_1+r_\ell,yz_2+s_\ell)\\ \text{is a perfect }(p-1)\text{-st power}}}(p-1)^2\left|\prod_{j=1}^{\ell}\frac{1-\chi^{\delta_j(p-1)/2}(g)}{1-\chi^{\delta_j}(g)}\right|\\ &=\frac{2^\ell}{(p-1)^\ell}\sum\nolimits_1+\frac{2^\ell}{(p-1)^\ell}\sum\nolimits_2.\end{aligned}\tag{34}$$

By [13, p. 384] we have

$$\frac{2^\ell}{(p-1)^\ell}\sum\nolimits_1 \ll k\ell 4^\ell p^{3/2}(\log p)^{\ell+1}. \tag{35}$$

It remains to prove that $\sum_2 = 0$. We will prove this by adapting the method used in [13].

Lemma 7. *Suppose that the conditions of Theorem 3 hold. Let*

$$z_1, z_2, r_1, \dots, r_\ell,\ s_1, \dots, s_\ell \in \mathbb{F}_p \quad \text{and} \quad 1 \le \delta_1, \dots, \delta_\ell \le p-2.$$

Then

$$f^{\delta_1}(xz_1 + r_1, yz_2 + s_1) \cdots f^{\delta_\ell}(xz_1 + r_\ell, yz_2 + s_\ell) \in \mathbb{F}_p[x, y]$$

is not a constant times the $(p-1)$-st power of a polynomial.

Proof of Lemma 7. We will need the following definitions:

Definition 2. Let $\mathcal{A}$ and $\mathcal{B}$ be multisets of the elements of $\mathbb{F}_p^n$. If $\mathcal{A}+\mathcal{B}$ represents every elements of $\mathbb{F}_p^n$ with multiplicity divisible by $p-1$, i.e., for all $c \in \mathbb{F}_p^n$, the number of solutions of

$$a + b = c, \qquad a \in \mathcal{A},\ b \in \mathcal{B}$$

(the a's and b's are counted with their multiplicities) is divisible by $p-1$, then $\mathcal{A}+\mathcal{B}$ is said to have property $\mathcal{P}$.

Definition 3. If $r, \ell, p \in \mathbb{N}$, where p is a prime and $r, \ell \le p-1$, then $(r, \ell, p-1)$ is said to be an *admissible triple* if there are no $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_p^2$ such that $\mathcal{A}$ contains r, $\mathcal{B}$ contains ℓ distinct elements, and $\mathcal{A}+\mathcal{B}$ possesses property $\mathcal{P}$.

Similarly to the proof of Theorem A in [7], we introduce an equivalence relation:

Definition 4. Two polynomials $\varphi(x,y), \psi(x,y) \in \mathbb{F}_p[x,y]$ are equivalent, $\varphi \sim \psi$, if there are $a_1, a_2 \in \mathbb{F}_p$ such that

$$\psi(x,y) = \varphi(x + a_1, y + a_2).$$

Write $f(x,y)$ as a product of irreducible polynomials in $\mathbb{F}_p[x,y]$. Let us group these factors so that in each group the equivalent irreducible factors are collected. Consider a typical group

$$\varphi(x + a_{1,1}, x_2 + a_{2,1}), \varphi(x + a_{1,2}, y + a_{2,2}), \dots, \varphi(x + a_{1,s}, y + a_{2,s}).$$

Since $f(x,y)$ is squarefree, each $\varphi(x + a_{1,i}, y + a_{2,i})$ has multiplicity 1 in the factorization $f(x,y)$. Then $f(x,y)$ is of the form

$$f(x,y) = \varphi(x + a_{1,1}, y + a_{2,1}) \cdots \varphi(x + a_{1,s}, y + a_{2,s}) g(x,y),$$

where $g(x,y)$ has no irreducible factor equivalent with any $\varphi(x+a_{1,i}, y+a_{2,i})$ $(1 \le i \le s)$.

We will use the following lemma:

Lemma 8. *Let $\varphi(x,y) \in \mathbb{F}_p[x,y]$ be nonzero and let $c, a_1, a_2 \in \mathbb{F}_p$ with $(a_1,a_2) \neq (0,0)$ be such that*

$$\varphi(x,y) = c\varphi(x+a_1, y+a_2). \tag{36}$$

Suppose that the degree of $\varphi(x,y)$ is $< p$. Then $\varphi(x,y)$ is of the form

$$\varphi(x,y) = g(a_2x - a_1y) \tag{37}$$

for a polynomial $g(x) \in \mathbb{F}_p[x]$.

Proof of Lemma 8. This is Lemma 6 in [13]. □

Now we are ready to complete the proof of Lemma 7. Let

$$h(x,y) = f^{\delta_1}(xz_1 + r_1, yz_2 + s_1) \cdots f^{\delta_\ell}(xz_1 + r_\ell, yz_2 + s_\ell).$$

Let

$$\tilde{f}(x,y) = f(xz_1, yz_2) \quad \text{and} \quad \mathbf{x} = (x,y),$$

then

$$h(\mathbf{x}) = \tilde{f}^{\delta_1}(\mathbf{x} + \mathbf{d_1}) \cdots \tilde{f}^{\delta_\ell}(\mathbf{x} + \mathbf{d}_\ell).$$

First we study the case when condition a) holds in Theorem 3, i.e., when $f(x,y)$ is irreducible in $\mathbb{F}_p[x,y]$. Then $f(x,y)$ and so $\tilde{f}(x,y)$ are not of the form (29). Then $f(x,y)$ is not of the form $g(a_2x - a_1y)$ for a polynomial $g(x) \in \mathbb{F}_p[x]$. Using Lemma 8 we get that the irreducible polynomials $\tilde{f}(\mathbf{x} + \mathbf{d_j})$ are distinct. There is unique factorization in $\mathbb{F}_p[x,y]$, thus the product $h(\mathbf{x})$ can be a constant multiple of the $(p-1)$-st power of a polynomial if and only if

$$p - 1 \mid \delta_1, \ldots, \delta_\ell.$$

Since we assumed that

$$1 \le \delta_1, \ldots, \delta_\ell \le p - 2$$

thus this cannot hold.

Now we assume that b) or c) holds in Theorem 3. Since $f(x,y)$ is not of the form (29), in the factorization of $\tilde{f}(x,y)$ there is an irreducible factor $\overline{u}(x,y)$ which cannot be written in the form

$$\overline{u}(x,y) = u_j(\alpha_j x + \beta_j y). \tag{38}$$

Consider the polynomials $\overline{u}(\mathbf{x} + \mathbf{a_i})$ for $i = 1, 2, \ldots, r$ which are equivalent with $\overline{u}(\mathbf{x})$ and appear in the factorization of $u(\mathbf{x})$.

We prove by contradiction that

$$h(\mathbf{x}) = \tilde{f}^{\delta_1}(\mathbf{x} + \mathbf{d_1}) \cdots \tilde{f}^{\delta_\ell}(\mathbf{x} + \mathbf{d}_\ell)$$

is not a constant multiple of the $(p-1)$-st power of a polynomial. Again we suppose that

$$h(\mathbf{x}) = \tilde{f}^{\delta_1}(\mathbf{x}+\mathbf{d_1})\cdots\tilde{f}^{\delta_\ell}(\mathbf{x}+\mathbf{d}_\ell)$$

is the constant multiple of the $(p-1)$-st power of a polynomial.

Write $h(\mathbf{x})$ as a product of irreducible polynomials in $\mathbb{F}_p[x,y]$. Then all polynomials $\overline{u}(\mathbf{x}+\mathbf{a_i}+\mathbf{d_j})$ $(1\le i\le s,\ 1\le j\le \ell)$ occur amongst the factors. These polynomials $\overline{u}(\mathbf{x}+\mathbf{a_i}+\mathbf{d_j})$ are equivalent, and no other factor belonging to this equivalence class will occur amongst the irreducible factor of $h(\mathbf{x})$. Write

$$\mathcal{A}=\{\mathbf{a_1},\dots,\mathbf{a_r}\} \quad \text{and} \quad \mathcal{D}=\{\underbrace{\mathbf{d_1},\dots,\mathbf{d_1}}_{\delta_1 \text{ times}},\dots,\underbrace{\mathbf{d}_\ell,\dots,\mathbf{d}_\ell}_{\delta_\ell \text{ times}}\}\subseteq\mathbb{F}_p^2,$$

where $r\le k$. By Lemma 8 all polynomials $\overline{u}(\mathbf{x}+\mathbf{c})$ for $\mathbf{c}\in\mathbb{F}_p^2$ are distinct since $\overline{u}$ is not of form (38). Thus in the collection, formed by the equivalent factors $\overline{u}(\mathbf{x}+\mathbf{a_i}+\mathbf{d_j})$, every polynomial $\overline{u}(\mathbf{x}+\mathbf{c})$ must occur with multiplicity divisible by $p-1$. Then $\mathcal{A}+\mathcal{D}$ possesses property $\mathcal{P}$. □

Lemma 9. *Let $s(s-1)/2<p$ and*

$$\mathbf{d_i}=(d_i',d_i'')\in\mathbb{F}_p^2 \quad (1\le i\le s)$$

be different vectors. Then there exists a $\lambda\in\mathbb{F}_p^*$ such that

$$d_i'+\lambda d_i''\in\mathbb{F}_p \quad (1\le i\le s)$$

are different.

Proof of Lemma 9. This is Lemma 7 in [13]. □

By Lemma 9 we may choose $\lambda\in\mathbb{F}_p$ so that both the sums

$$a'+\lambda a'' \quad \text{with} \quad (a',a'')\in\mathcal{A}$$

and

$$d'+\lambda d' \quad \text{with} \quad (d',d'')\in\mathcal{D}$$

are distinct. Write now

$$\mathcal{A}'=\{a'+\lambda a'':\ (a',a'')\in\mathcal{A}\}$$

and let $\mathcal{D}'$ be the multiset which contains $r_i+\lambda s_i$ with multiplicity δ_i, where

$$\mathbf{d_i}=(r_i,s_i)\in\mathcal{D}$$

with multiplicity δ_i:

$$\mathcal{D}'=\{\underbrace{r_i+\lambda s_i}_{\delta_i \text{ times}}:\ (r_i,s_i)\in\mathcal{D}\}.$$

Lemma 10. *$\mathcal{A}' + \mathcal{D}'$ possesses property P.*

Proof of Lemma 10. In order to prove the lemma we have to show that for any $c \in \mathbb{F}_p$ the number of solutions

$$a + d = c, \quad a \in \mathcal{A}', \ d \in \mathcal{D}' \tag{39}$$

is divisible by $p - 1$. Indeed, it is clear that the number of solutions of (39) is the same as the number of solutions of

$$(a', a'') + (d', d'') = (c', c''), \quad (a', a'') \in \mathcal{A}, \ (d', d'') \in \mathcal{D},$$
$$c' + \lambda c'' = c. \tag{40}$$

Since $\mathcal{A} + \mathcal{D}$ possesses property P, for any $(c', c'') \in \mathbb{F}_p^2$ the number of solutions of the equation

$$(a', a'') + (d', d'') = (c', c''), \quad (a', a'') \in \mathcal{A}, \ (d', d'') \in \mathcal{D}$$

is divisible by $p - 1$. Thus the number of solutions of the system (40) is also divisible by $p - 1$, and equivalently, the number of solutions of (39) is also divisible by $p - 1$. This proves Lemma 10. □

By Lemma 10 $\mathcal{A}' + \mathcal{D}'$ possesses property P. Thus $(r, \ell, p - 1)$ is not an admissible triple. By the following lemma this is not possible:

Lemma 11.

(i) *For every prime p and $r \in \mathbb{N}$ the triple $(r, 2, p)$ is admissible.*

(ii) *If p is prime, $r, \ell \in \mathbb{N}$ and $(4k)^\ell < p$, then $(r, \ell, p - 1)$ is admissible.*

(iii) *If p is a prime such that 2 is primitive root modulo p, then for every pair $(r, \ell) \in \mathbb{N}$ with $r < p$, $\ell < p$ the triple $(r, \ell, p - 1)$ is admissible.*

Proof of Lemma 11. This is proved in the proof of Lemma 1 in [8]. □

Note that replacing Lemma 9 by Lemma 4 in [21], it could be shown that (ii) in Lemma 11 and thus c) in Theorem 3 also holds if the inequalities are replaced by

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

So we get a contradiction, thus we have proved that b) and c) in Theorem 3 also imply the conclusion of Lemma 7. □

Note that the implementation and handling of this construction is rather complicated and slow, since there is no fast algorithm computing the index. Gyarmati [8], [10] worked out a fast version of the one dimensional construction (4); in a similar manner one could work out a fast version of construction (30) in Theorem 3.

Remark 1. In each of the three constructions we estimated the only pseudorandom measure $Q_\ell(\eta)$. One may also introduce and study further, independent measures of pseudorandomness and, indeed, in a forthcoming series this will be our goal. One may also study the connection between different measures of pseudorandomness. E.g., in the one dimensional case Brandstätter and Winterhof [2] were the first to observe that from the upper bounds for the correlation of "not very large" order of a binary sequence one can deduce a lower bound for the linear complexity of it, and later Andics [1] proved another similar inequality. One might like to look for the multidimensional analogues of these results. Then the first problem is how to extend the notion of linear complexity to n-dimensional lattices? The simplest although not quite satisfactory way would be to stretch the lattice into a binary sequence in the way described and studied in [11] (first we take the elements of the first row of the lattice, then we continue with the elements of the second row, etc.), and then to study the linear complexity of the binary sequence obtained in this way. One might like to go beyond this simple way and also introduce and study notion(s) of more multidimensional nature of linear complexity of lattices.

All our constructions and results presented in this paper could be extended from two dimensional lattices to n-dimensional ones at the expense of extending some technical lemmas from two dimensions to n dimensions (and working with lenghtier formulas). In general in n dimensions the trivial upper bound for the pseudorandom measure $Q_\ell(\eta)$ of an N-lattice is $O(N^n)$, our approach gives $O(N^{n-1/2+o(1)})$, and the expected optimal bound would be $O(N^{n/2+o(1)})$ (so that while in two dimensions our estimates roughly halve the gap between the trivial resp. optimal bound, as the dimension increases the saving relative to the size of the gap decreases rapidly).

As we referred to it earlier, to close this gap one would need the application of Deligne's theorem. Unfortunately, in order to apply this result one needs the inconvenient assumption of nonsingularity. This requirement could be ensured in the estimate of $Q_1(\eta)$, but no matter how strong assumptions (absolute irreducibility, etc.) we have on our polynomials $f(x, y)$, for $\ell \geq 2$ the estimate of $Q_\ell(\eta)$ leads to character sums involving a large set of complicated polynomials and one cannot guarantee that all these polynomials satisfy the nonsingularity requirement.

REFERENCES

[1] ANDICS, Á.: *On the linear complexity of binary sequences*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **48** (2005), 173–180.

[2] BRANDSTÄTTER, N. – WINTERHOF, A.: *Linear complexity profile of binary sequences with small correlation measure*, Period. Math. Hungar. **52** (2006), 1–8.
[3] DAVENPORT, H. – LEWIS, D. J.: *Character sums and primitive roots in finite fields*, Rend. Circ. Mat. Palermo (2) **12** (1963), 129–136.
[4] DELIGNE, P.: *La conjecture de Weil, I,* Inst. Hautes Études Sci. Publ. Math. **43** (1974), 273–307.
[5] EICHENAUER-HERMANN, J. – NIEDERREITER, H.: *Bounds for exponential sums and their applications to pseudorandom numbers*, Acta Arith. **67** (1994), 269–281.
[6] FOUVRY, E. – KATZ, N.: *A general stratification theorem for exponential sums and applications*, J. Reine Angew. Math. **540** (2001), 115–166.
[7] GOUBIN, L. – MAUDUIT, C. – SÁRKÖZY, A.: *Construction of large families of pseudorandom binary sequences*, J. Number Theory **106** (2004), 56–69.
[8] GYARMATI, K.: *A note to the paper "On a fast version of a pseudorandom generator"*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **49** (2006), 87–93.
[9] GYARMATI, K.: *On a family of pseudorandom binary sequences*, Period. Math. Hungar. **49** (2004), no. 2, 45–63.
[10] GYARMATI, K.: On a fast version of a pseudorandom generator, in: *General Theory of Information Transfer and Combinatorics*, Lecture Notes in Comput. Sci. **4123**, Springer, Berlin,2006, pp. 326–342.
[11] GYARMATI, K. – MAUDUIT, C. – SÁRKÖZY, A.: *Pseudorandom binary sequences and lattices*, Acta Arith. **135** (2008), 181–197.
[12] GYARMATI, K. – SÁRKÖZY, A.: *Equations in finite fields with restricted sets, I. (Character sums.)*, Acta Math. Hungar. **118** (2008), 129–148.
[13] GYARMATI, K. – SÁRKÖZY, A. – STEWART, C. L.: *On Legendre symbol lattices*, Uniform Distribution Theory, **4** (2009), no. 1, 81–95.
[14] HUBERT, P. – MAUDUIT C. – SÁRKÖZY, A.: *On pseudorandom binary lattices*, Acta Arith. **125** (2006), 51–62.
[15] LIU, H.: *New pseudorandom sequences constructed using multiplicative inverses*, Acta Arith. **125** (2006), no. 1, 11–19.
[16] LIU, H.: *New pseudorandom sequences constructed by quadratic residues and Lehmer numbers*, in: Proc. Amer. Math. Soc. **135** (2007), no. 5, AMS, Providence, RI, pp. 1309–1318.
[17] LIU, H.: *A family of pseudorandom binary sequences constructed by the multiplicative inverse*, Acta Arith. **130** (2007), no. 2, 167–180.
[18] MAUDUIT, C. – RIVAT, J. – SÁRKÖZY, A.: *Construction of pseudorandom binary sequences using additive characters*, Monatsh. Math. **141** (2004), 197–208.
[19] MAUDUIT, C. – SÁRKÖZY, A.: *On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol*, Acta Arith. **82** (1997), 365–377.
[20] MAUDUIT, C. – SÁRKÖZY, A.: *Construction of pseudorandom binary sequences by using the multiplicative inverse*, Acta Math. Hungar. **108** (2005), 239–252.

[21] MAUDUIT, C. – SÁRKÖZY, A.: *On large families of pseudorandom binary lattices*, Uniform Distribution Theory **2** (2007), no. 1, 23–37.

[22] MAUDUIT, C. – SÁRKÖZY, A.: *Constructions of pseudorandom binary lattices by using the multiplicative inverse*, Monatsh. Math. **153** (2008), 217–231.

[23] MÉRAI, L. : *Construction of large families of pseudorandom binary sequences*, Ramanujan J. **18** (2009), 341–349.

[24] MÉRAI, L.: *A construction of pseudorandom binary sequences using rational functions*, Uniform Distribution Theory **4** (2009), no. 1, 35–49.

[25] MÉRAI, L.: *A construction of pseudorandom binary sequences using both additive and multiplicative characters*, Acta Arith. (to appear).

[26] SÁRKÖZY, A.: *A finite pseudorandom binary sequence*, Studia Sci. Math. Hungar. **38** (2001), 377–384.

[27] SÁRKÖZY, A.: *On finite pseudorandom binary sequences and their applications in cryptography*, Tatra Mt. Math. Publ. **37** (2007), 123–136.

[28] SÁRKÖZY, A. – STEWART, C. L. : *On pseudorandomness in families of sequences derived from the Legendre symbol*, Period. Math. Hungar. **54** (2007), 163–173.

[29] SÁRKÖZY, A. – WINTERHOF, A.: *Measures of pseudorandomness for binary sequences constructed using finite fields*, Discrete Math. **309** (2009), 1327–1333.

[30] WEIL, A.: *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Actualités Sci. Ind. **1041**, Publ. Inst. Math. Univ. Strasbourg 7 (1945), Hermann et Cie., Paris, 1948.

Received June 24, 2009
Accepted November 25, 2009

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

Christian Mauduit
Institute de Mathématiques de Luminy
CNRS, UMR 6206
163 avenue de Luminy, Case 907
FR-13288 Marseille Cedex 9,
FRANCE
E-mail: mauduit@iml.univ-mrs.fr