On Legendre symbol lattices

Katalin Gyarmati[†], András Sárközy[†], Cameron L . Stewart[‡]

Abstract

In an earlier paper Hubert, Mauduit and Sárközy introduced pseudorandom measures for pseudorandomness of binary lattices, and they gave constructions for binary lattices with strong pseudorandom properties. They gave nearly optimal upper bounds for the pseudorandom measures of the lattices constructed. However, these early constructions also have disadvantages: they are rather artificial, and their implementation is complicated. Thus another construction is presented here which is based on the use of the Legendre symbol. This construction is much more natural and flexible than the earlier ones, and it can be implemented more easily. However, there is a price paid for this: to give upper bounds for the pseudorandom measures one needs the flexibility and generality of Weil's theorem, and here in the two dimensional situation this approach leads to weaker bounds than the optimal ones.

[†]Research partially supported by Hungarian National Foundation for Scientific Research, Grants No. T049693, K67676, PD72264, K72731 and the János Bolyai Research Fellowship.

[‡]Research supported by the Canada Research Chair Program and by Grant A3528 of the Natural Sciences and Engineering Research Council of Canada.

2000 Mathematics Subject Classification: Primary 11K45.

Key words: pseudorandom, binary lattice, Legendre symbol.

1 Introduction

Pseudorandom binary sequences have many important applications. In particular, they are used as a key stream in the classical stream cipher called the Vernam cipher. The standard approach to the theory of pseudorandomness of binary sequences is based on complexity theory. However, this approach has certain limitations and weak points. Thus recently Mauduit and Sárközy [9] (see also the survey paper [12]) initiated a new, constructive approach to the theory of pseudorandomness. They defined and studied new measures of pseudorandomness. These measures provide a quantitative characterization of pseudorandomness of a given binary sequence. In the last 10 years numerous binary sequences have been tested for pseudorandomness.

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 [7]. They introduced the following definitions:

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

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

This set is called an *n-dimensional N-lattice* or briefly an *N-lattice.* Here we will extend this definition 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 non-zero, and the other coordinates of $\mathbf{u_i}$ are 0, so $\mathbf{u_i}$ 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 will call the set

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

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

In [7] 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 $\mathbf{x} = (x_1, \ldots, x_n)$ so that $\eta(\mathbf{x}) = \eta((x_1, \ldots, x_n))$ then we will slightly simplify the notation by writing $\eta(\mathbf{x}) = \eta(x_1, \ldots, x_n)$.

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 [7] Hubert, Mauduit and Sárközy introduced the following pseudorandom measure of binary lattices (here we will present the definition in a slightly modified but equivalent form):

Definition 1 *Let*

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

The pseudorandom measure of order ℓ of η is defined by

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

where the maximum is taken over all distinct $\mathbf{d_1}, \ldots, \mathbf{d}_\ell \in I_N^n$ and all box 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 as a good pseudorandom lattice if for fixed n and ℓ and large N

the measure $Q_\ell(\eta)$ is small (much smaller, than the trivial upper bound N^n). This terminology is justified by the fact that, as was proved in [7], for a truly random binary lattice defined on I_N^n and for fixed ℓ the measure $Q_\ell(\eta)$ is small: It is less than $N^{n/2}$ multiplied by a logarithmic factor.

In one dimension, hence in 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. Unfortunately, this approach in its original form does not readily apply in higher 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. While Fouvry and Katz [3] have simplified the requirements for applying Deligne's theorem the inconvenient assumption of nonsingularity is still required in order to obtain sharp bounds.

In spite of these difficulties, in [7] and [8] 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 the form $x = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n$ with $x_1, x_2, \dots, x_n \in \mathbb{F}_p$. Then $g(x_1, x_2, \dots, x_n) = G(x_1 e_1 + x_2 e_2 + \cdots + x_n e_n) \in \mathbb{F}_p[x_1, x_2, \dots, x_n]$ 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 [2].)

This detour enables one to give sharp upper bounds, but it also has considerable disadvantages. In particular, in this way we get rather artificial constructions. More natural 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, in other words, for a method which is much more flexible and applicable at the expense of providing weaker but still nontrivial upper bounds. We will show that in the case when $n = 2$, there is such a method, based on the techniques introduced by Gyarmati and Sárközy [5] to estimate certain related character sums. This method allows us to give a simple description of the exceptional polynomials, see Section 2. But the price paid for the flexibility of this method is that the upper bounds are not optimal. For a two dimensional p-lattice they are, up to logarithmic factors, $p^{3/2}$ instead of the optimal bound of p. On the other hand, they improve on the trivial bound of p^2 considerably.

In one dimension the best and most intensively studied construction is based on the use of the Legendre symbol, see [4], [6], [9], [13]. Let p be a prime, $f(x) \in \mathbb{F}_p[x]$ be a polynomial, and define the sequence $E_p = \{e_1, \dots, e_p\}$ by

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

We will identify the elements of $\mathbb{F}_p$ with the residue classes modulo p, and we will not distinguish between the residue classes and their representing elements. The natural two dimensional extension of this construction is the following.

Construction 1 *Let p be an odd prime, $f(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ be a polynomial in two variables. Define $\eta :\ I_p^2 \to \{-1, +1\}$ by*

$$\eta(x_1,x_2)=\begin{cases}\left(\frac{f(x_1,x_2)}{p}\right) & \text{if } (f(x_1,x_2),p)=1,\\ +1 & \text{if } p \mid f(x_1,x_2).\end{cases} \tag{1.2}$$

First, in Section 2, we will show that in two dimensions there are new difficulties arising, and there are many "bad" polynomials $f(x_1, x_2)$. Then, in Section 3, we will formulate Theorem 1, our main result. We will also present several sufficient criteria for a polynomial $f(x_1, x_2)$ for which the corresponding binary p-lattice (1.2) possesses strong pseudorandom properties. The rest of this paper will be devoted to the proof of this main result.

In Part II of this paper we will study (1.2) in the case when $f(x_1, x_2)$ is one of the degenerate polynomials described in Section 2. Moreover, we will also study implementation problems related to some constructions based on Theorem 1.

2 Negative examples

In this section we will present examples of polynomials $f(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ for which the binary p-lattice defined in (1.2) has weak pseudorandom properties.

Example 1 If

$$f(x_1,x_2)=c\,(g(x_1,x_2))^2$$

with $c \in \mathbb{F}_p$, $g(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$, then every element of the lattice defined in (1.2) is $\left(\frac{c}{p}\right)$ except the zeros of $f(x_1, x_2)$. It follows that if the degree of $f(x_1, x_2)$ is not very large, then $Q_1(\eta)$ is large.

Example 2 If $f(x_1, x_2) = g(x_1)$ with a polynomial $g(x) \in \mathbb{F}_p[x]$ of one variable, then we have

$$\eta(x_1,x_2)\eta(x_1,x_2+1)=\left(\frac{g(x_1)}{p}\right)\left(\frac{g(x_1)}{p}\right)=+1$$

(except the zeros of $g(x_1)$) from which it follows that $Q_2(\eta)$ is large.

Example 3 If $f(x_1, x_2) = g(x_1)h(x_2)$ with polynomials $g(x), h(x) \in \mathbb{F}_p[x]$, then it can be shown by a little computation that $Q_4(\eta)$ is large.

The polynomials $f(x_1, x_2)$ occurring in examples 1-3 are special cases of the following:

Definition 2 *The polynomial $f(x_1, x_2)$ is called* degenerate *if it is of the form*

$$f(x_1, x_2) = \left(\prod_{j=1}^{r} f_j(\alpha_j x_1 + \beta_j x_2) \right) g(x_1, x_2)^2, \tag{2.1}$$

where $\alpha_j, \beta_j \in \mathbb{F}_p$, $f_j(x) \in \mathbb{F}_p[x]$ for $j = 1, \ldots, r$, and $g(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$.

A polynomial $f \in \mathbb{F}_p[x, y]$ which can be expressed in the form (2.1) is said to be degenerate and otherwise it is said to be non-degenerate.

As examples 1, 2 and 3 show, if f is degenerate then it may be that the associated binary p-lattice (1.2) has weak pseudorandom properties. We shall analyse the situation when f is degenerate in more detail in a sequel to this paper. In the balance of this paper we shall restrict our attention to binary p-lattices (1.2) for which f is non-degenerate.

3 Sufficient conditions

In one dimension Goubin, Mauduit and Sárközy [4] gave sufficient conditions on the polynomial $f(x)$ to guarantee small pseudorandom measures. Let $\overline{\mathbb{F}}_p$ denote an algebraic closure of $\mathbb{F}_p$.

Theorem A *Let $f(x) \in \mathbb{F}_p[x]$ be a polynomial of degree $k(> 0)$ which has no multiple zero in $\overline{\mathbb{F}}_p$. Define the sequence $E_p \in \{-1, +1\}^p$ by (1.1). Then*

$W(E_p)$, the "well-distribution measure" of E_p, satisfies

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

Moreover assume that one of the following 3 conditions holds:

a) $\ell = 2$,

b) 2 is a primitive root modulo p,

c) $(4k)^\ell < p$ or $(4\ell)^k < p$,

Then $C_\ell(E_p)$, "the correlation measure of order ℓ," satisfies

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

(See [9] for the definition of well-distribution measure and correlation measure.)

We extend their result to the 2 dimensional case:

Theorem 1 *Let $f(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ be a polynomial of degree k. Suppose that $f(x_1, x_2)$ cannot be expressed in the form (2.1) and one of the following 5 conditions holds:*

a) $f(x_1, x_2)$ is irreducible in $\mathbb{F}_p[x_1, x_2]$,

b) $\ell = 2$,

c) 2 is a primitive root modulo p,

d) $4^{k+\ell} < p$,

e) ℓ and the degree of the polynomial $f(x_1, x_2)$ in x_1 (or in x_2) are odd.

Then for the binary p-lattice η defined in (1.2) we have

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

The rest of this paper is devoted to the proof of this theorem.

4 Proof of Theorem 1

For $k > p^{1/2}/10$ the theorem is trivial. Thus we may suppose that

$$k \leq p^{1/2}/10. \tag{4.1}$$

Similarly, we may suppose that

$$k^2 + \ell^2 < p, \tag{4.2}$$

otherwise the theorem is trivial since

$$4k^2\ell^2 > k^2 + \ell^2 \geq p,$$

and so

$$10k\ell p^{3/2} \log p > p^2.$$

Lemma 1 *If $\mathbb{F}$ is a field, then in $\mathbb{F}[x_1, x_2, \ldots, x_n]$ every polynomial has a factorization into irreducible polynomials which is unique apart from constant factors and reordering.*

Proof of Lemma 1 See, for example [11, Theorem 207].

If $f(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$, then we will also write $f(x_1, x_2) = f(\mathbf{x})$ with $\mathbf{x} = (x_1, x_2)$.

Lemma 2 *Let $p \geq 5$ be a prime and χ be a multiplicative character of order d. Suppose that $h(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ is not of the form $cg(x_1, x_2)^d$ with $c \in \mathbb{F}_p$, $g(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$. Let k be the degree of $h(x_1, x_2)$. Then we have*

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

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

We remark that the upper bound in the lemma is nearly sharp: it is easy to see that there are polynomials $h(x_1, x_2)$ of the form $h(x_1, x_2) = f(x_1)$ (so that $h(x_1, x_2)$ depends only one of the two variables) for which the left hand side of the inequality in the lemma with $\mathbb{F}_p^2$ in place of B is $> c(k)p^{3/2}$.

Proof of Lemma 2

It follows easily from Lemma 1 that $h(x_1, x_2)$ cannot be of form both $g_1(x_1)p_1(x_1, x_2)^d$ and $g_2(x_2)p_2(x_1, x_2)^d$ simultaneously with $g_1(x), g_2(x) \in \mathbb{F}_p[x]$ and $p_1(x_1, x_2)$, $p_2(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$. Thus by symmetry reasons we may suppose that $h(x_1, x_2)$ is not of the form $g_2(x_2)p_2(x_1, x_2)^d$.

Since B is a box p-lattice, write it in the form

$$B = \{\mathbf{x} = (v_1 b_1, v_2 b_2) : \ v_1, v_2 \in \mathbb{N}, \ 0 \le v_1 b_1 \le t_1, \ 0 \le v_2 b_2 \le t_2\} \tag{4.3}$$

with $b_1, b_2 \in \mathbb{N}$ and $0 \le t_1, t_2 < p$. Then by the triangle inequality

$$\left| \sum_{\mathbf{x} \in B} \chi\left(h(\mathbf{x})\right) \right| \le \sum_{0 \le v_2 \le [t_2/b_2]} \left| \sum_{0 \le v_1 \le [t_1/b_1]} \chi\left(h(v_1 b_1, v_2 b_2)\right) \right|.$$

For fixed v_2, b_1 and b_2, the polynomial $h(v_1 b_1, v_2 b_2)$ is a polynomial of one variable in v_2. We will use the following consequence of Weil's theorem [14]:

Lemma 3 *Suppose that p is a prime, χ is a non-principal character modulo p of order d, $f(x) \in \mathbb{F}_p[x]$ has s distinct roots in $\overline{\mathbb{F}}_p$, and it is not the constant multiple of the d-th power of a polynomial in $\mathbb{F}_p[x]$. Let y be a real number with $0 < y \le p$. Then for any $x \in \mathbb{F}_p$:*

$$\left| \sum_{x < n \le x+y} \chi(f(n)) \right| < 9sp^{1/2} \log p.$$

Proof of Lemma 3

This is an immediate consequence of Lemma 1 in [1].

If, for fixed v_2, b_1, b_2, the polynomial $h(xb_1, v_2b_2) \in \mathbb{F}_p[x]$ of one variable is not of the form $cg(x)^d$ with $c \in \mathbb{F}_p$, $g(x) \in \mathbb{F}_p[x]$, then by Lemma 3

$$\left| \sum_{0 \le v_1 \le [t_1/b_1]} \chi\left(h(v_1b_1, v_2b_2)\right) \right| \le 9kp^{1/2} \log p.$$

We will show that for fixed b_1 and b_2 there are only few values of v_2 for which the polynomial $h(xb_1, v_2b_2) \in \mathbb{F}_p[x]$ is of the form $cg(x)^d$. For this we need

Lemma 4 *Let $h(x, y) \in \mathbb{F}_p[x, y]$ be a polynomial of two variables, which is not of the form $q(y)p(x, y)^d$ with $q(y) \in \mathbb{F}_p[y]$, $p(x, y) \in \mathbb{F}_p[x, y]$. Denote by n and m the degree of the polynomial $h(x, y)$ in x and y, respectively. Then there are at most $nm + m$ values $y_0 \in \mathbb{F}_p$ such that*

$$h(x, y_0) \in \mathbb{F}_p[x]$$

is of the form $cg(x)^d$ with $c \in \mathbb{F}_p$, $g(x) \in \mathbb{F}_p[x]$.

Proof of Lemma 4 This is Lemma 4 in [5].

Let n and m be the degree of $h(x_1, x_2)$ in x_1 and x_2 respectively. We have assumed that $h(x_1, x_2)$ is not of the form $g_2(x_2)p_2(x_1, x_2)^d$, thus by Lemma 4, there are at most $nm + m$ values of v_2 such that $h(xb_1, v_2b_2)$ is of the form $cg(x)^d$ for some $c \in \mathbb{F}_p$, $g(x) \in \mathbb{F}_p[x]$. Let $\mathcal{V}$ denote the set of these v_2's. Then

$$|\mathcal{V}| \le mn + m \le k^2 + k. \tag{4.4}$$

By (4.3)

$$\left| \sum_{\mathbf{x} \in B} \chi\left(h(\mathbf{x})\right) \right| \le \sum_{v_2 \in \mathcal{V}} \left| \sum_{0 \le v_1 \le [t_1/b_1]} \chi\left(h(v_1b_1, v_2b_2)\right) \right| + \sum_{v_2 \in \mathbb{F}_p \setminus \mathcal{V}} \left| \sum_{0 \le v_1 \le [t_1/b_1]} \chi\left(h(v_1b_1, v_2b_2)\right) \right|.$$

For $v_2 \in \mathcal{V}$ we use the trivial estimate p for the inner sum. By Lemma 4 and (4.4)

$$\sum_{v_2 \in \mathcal{V}} \left| \sum_{0 \le v_1 \le [t_1/b_1]} \chi\left(h(v_1 b_1, v_2 b_2)\right) \right| \le (k^2 + k)p.$$

For $v_2 \in \mathbb{F}_p \setminus \mathcal{V}$ we use Lemma 3 to deduce that

$$\sum_{v_2 \in \mathbb{F}_p \setminus \mathcal{V}} \left| \sum_{0 \le v_1 \le [t_1/b_1]} \chi\left(h(v_1 b_1, v_2 b_2)\right) \right| < 9kp^{3/2} \log p.$$

Thus by (4.1)

$$\left| \sum_{\mathbf{x} \in B} \chi\left(h(\mathbf{x})\right) \right| < (k^2 + k)p + 9kp^{3/2} \log p < 10kp^{3/2} \log p$$

which completes the proof of Lemma 2.

Lemma 5 *Suppose that $f \in \mathbb{F}_p[x_1, x_2]$ is a polynomial such that there are no distinct $\mathbf{d_1}, \dots, \mathbf{d}_\ell \in \mathbb{F}_p^2$ with the property that $f(\mathbf{x} + \mathbf{d_1}) \dots f(\mathbf{x} + \mathbf{d}_\ell)$ is of the form $cg(\mathbf{x})^2$ with $c \in \mathbb{F}_p$, $g \in \mathbb{F}_p[x_1, x_2]$. Let k be the degree of the polynomial $f(x_1, x_2)$. Then for the binary p-lattice η defined in* (2.1) *we have*

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

Proof of Lemma 5 We have

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

where the maximum is taken over all distinct $\mathbf{d_1}, \dots, \mathbf{d}_\ell \in I_p^2$ and box p-lattices B such that $B + \mathbf{d_1}, \dots, B + \mathbf{d}_\ell \subseteq I_p^2$. Let B be the box p-lattice, $\mathbf{d_1}, \dots, \mathbf{d}_\ell \in I_p^2$ be the vectors for which this maximum is attained so that

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

Write $h(\mathbf{x}) = f(\mathbf{x}+\mathbf{d_1})\cdots f(\mathbf{x}+\mathbf{d}_\ell)$, then

$$Q_\ell(\eta) \le \left| \sum_{\mathbf{x}\in B} \left(\frac{h(\mathbf{x})}{p}\right) \right| + \sum_{\substack{\mathbf{x}\in B\\ h(\mathbf{x})=0}} 1.$$

$h(\mathbf{x})$ is a polynomial of degree $k\ell$. Estimating the number of zeros of $h(\mathbf{x})$ we find that

$$\sum_{\substack{\mathbf{x}\in B\\ h(\mathbf{x})=0}} 1 \le k\ell p. \tag{4.5}$$

By assumption $h(\mathbf{x})$ is not of the form $cg(\mathbf{x})^2$ and its degree is ℓk. Thus by Lemma 2 and (4.5) we have

$$Q_\ell(\eta) \le 10\ell k p^{3/2}\log p + \ell k p,$$

which was to be proved.

Suppose that one of the 5 conditions in Theorem 1 holds. We will prove that the product

$$h(\mathbf{x}) = f(\mathbf{x}+\mathbf{d_1})\dots f(\mathbf{x}+\mathbf{d}_\ell)$$

cannot be the constant multiple of a perfect square. Then by Lemma 5 we get Theorem 1.

Next we will introduce three definitions.

Definition 3 *Let G be a group with respect to addition. Let A and B be subsets of G and suppose that for all c in G the number of solutions of*

$$a+b=c,$$

with a in A and b in B is even. Then (A,B) is said to have property P.

Definition 4 *Let r, ℓ, and m be positive integers with $r, \ell \leq m$. The triple (r, ℓ, m) is said to be admissible if there are no $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_m$ such that $|\mathcal{A}| = r$, $|\mathcal{B}| = \ell$, and $(\mathcal{A}, \mathcal{B})$ possesses property P.*

We shall also introduce an equivalence relation on $\mathbb{F}_p[x_1, x_2]$ as in the proof of Theorem A in [4].

Definition 5 *Two polynomials $\varphi(x_1, x_2), \psi(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ are equivalent if there are $a_1, a_2 \in \mathbb{F}_p$ such that*

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

Write the polynomial $f(x_1, x_2)$ in the theorem as a product of irreducible polynomials in $\mathbb{F}_p[x_1, x_2]$. (Recall that the lattice η is determined by this polynomial $f(x_1, x_2)$, the definition of η is presented in (1.2).) Let us group these factors so that in each group the equivalent irreducible factors are collected. Consider a typical group $\varphi(x_1 + a_{1,1}, x_2 + a_{2,1}), \varphi(x_1 + a_{1,2}, x_2 + a_{2,2}), \ldots, \varphi(x_1 + a_{1,s}, x_2 + a_{2,s})$. Then $f(x_1, x_2)$ is of the form

$$f(x_1, x_2) = \varphi(x_1 + a_{1,1}, x_2 + a_{2,1}) \cdots \varphi(x_1 + a_{1,s}, x_2 + a_{2,s}) g(x_1, x_2),$$

where $g(x_1, x_2)$ has no irreducible factor equivalent with any $\varphi(x_1 + a_{1,i}, x_2 + a_{2,i})$ $(1 \leq i \leq s)$.

We will use the following lemma:

Lemma 6 *Let $\varphi(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ be nonzero and let $c, a_1, a_2 \in \mathbb{F}_p$ with $(a_1, a_2) \neq (0, 0)$ be such that*

$$\varphi(x_1, x_2) = c\varphi(x_1 + a_1, x_2 + a_2), \tag{4.6}$$

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

$$\varphi(x_1, x_2) = g(a_2 x_1 - a_1 x_2). \tag{4.7}$$

Proof of Lemma 6. We will use repeatedly the fact that if two polynomials of degree less than p in each variable define the same polynomial function, then they must also be identical polynomials.

By considering the highest degree terms in (4.6), we get $c = 1$ so that

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

It follows from this that for every $t \in \mathbb{F}_p$

$$\varphi(x_1, x_2) = \varphi(x_1 + ta_1, x_2 + ta_2). \tag{4.8}$$

One of a_1 and a_2 is nonzero and, without loss of generality, we may suppose that $a_2 \neq 0$. Then write $\varphi(x_1, x_2)$ in the form

$$\begin{aligned}\varphi(x_1, x_2) &= \varphi(a_2^{-1}((a_2x_1 - a_1x_2) + a_1x_2), x_2)\\ &= q_n(a_2x_1 - a_1x_2)x_2^n + q_{n-1}(a_2x_1 - a_1x_2)x_2^{n-1} + \cdots + q_0(a_2x_1 - a_1x_2),\end{aligned} \tag{4.9}$$

where $q_i(x) \in \mathbb{F}_p[x]$ are polynomials of one variable. For fixed x_1, x_2 write $A = \varphi(x_1, x_2)$ and $Q_i = q_i(a_2x_1 - a_1x_2) = q_i(a_2(x_1 + ta_1) - a_1(x_2 + ta_2))$. Then by (4.8) and (4.9) for every $t \in \mathbb{F}_p$:

$$A = \varphi(x_1, x_2) = \varphi(x_1 + ta_1, x_2 + ta_2) = Q_n(x_2 + ta_2)^n + \cdots + Q_0.$$

Both A and the expression on the right above are polynomials in t of degree at most p. These polynomials define the same function and so they are the same polynomials, which is possible only if $n = 0$. It follows that

$$q_0(a_2x_1 - a_1x_2) - \varphi(x_1, x_2) = Q_0 - A = 0,$$

for every $x_1, x_2 \in \mathbb{F}_p$. Since both q_0 and φ have degree less than p in x_1 and x_2, thus

$$q_0(a_2x_1 - a_1x_2) = \varphi(x_1, x_2)$$

as formal polynomials, which proves (4.7).

First we study the case when condition a) holds in Theorem 1, so when $f(x_1, x_2)$ is irreducible in $\mathbb{F}_p[x_1, x_2]$. As before let $\mathbf{d_1}, \dots, \mathbf{d}_\ell$ be distinct elements of I_p^2 and put $h(x) = f(\mathbf{x} + \mathbf{d_1}) \cdots f(\mathbf{x} + \mathbf{d}_\ell)$. Then by Lemma 6 the irreducible polynomials $f(\mathbf{x} + \mathbf{d_j})$ are different since $f(x_1, x_2)$ is not of the form (2.1). By Lemma 1, there is unique factorization in $\mathbb{F}_p[x_1, x_2]$, thus $h(\mathbf{x})$ cannot be the constant multiple of a perfect square. By using Lemma 5 we get the statement.

Next we prove parts b), c) and d) in Theorem 1. Write $f(x_1, x_2)$ in the form $u(x_1, x_2)(v(x_1, x_2))^2$ where $u(x_1, x_2)$ is squarefree, so, in other words, there is no non-constant irreducible polynomial $h(x_1, x_2)$ with $(h(x_1, x_2))^2$ a divisor of $u(x_1, x_2)$. Since $f(x_1, x_2)$ is not of the form (2.1), in the factorization of $u(x_1, x_2)$ there is an irreducible factor $\overline{u}(x_1, x_2)$ which cannot be written in the form

$$\overline{u}(x_1, x_2) = u(\alpha x_1 + \beta x_2). \tag{4.10}$$

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

We shall prove that $h(\mathbf{x}) = f(\mathbf{x} + \mathbf{d_1}) \cdots f(\mathbf{x} + \mathbf{d}_\ell)$ is not a constant multiple of a perfect square. We shall suppose that $h(\mathbf{x})$ is the constant multiple of a perfect square. Then $h_1(\mathbf{x}) = u(\mathbf{x} + \mathbf{d_1}) \cdots u(\mathbf{x} + \mathbf{d}_\ell)$ is also a constant multiple of a perfect square.

Write $h_1(\mathbf{x})$ as a product of irreducible polynomials in $\mathbb{F}_p[x_1, x_2]$. 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 factors belonging to this equivalence class will occur amongst the irreducible factors of $h_1(\mathbf{x})$. By Lemma 6 all polynomials $\overline{u}(\mathbf{x} + \mathbf{c})$ for $\mathbf{c} \in \mathbb{F}_p^2$ are distinct since $\overline{u}$ is not of the form (4.10). Thus in the collection, formed by the equivalent factors $\overline{u}(\mathbf{x}+\mathbf{a_i}+\mathbf{d_j})$, every polynomial must occur an even number of times. As a consequence every $c \in \mathbb{F}_p^2$ occurs an even number of times in the form $a_i + d_j$ with $1 \le i \le r$ and $1 \le j \le \ell$.

Lemma 7 *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 7 Suppose that for some pair (i, j) with $1 \le i < j \le \ell$ we have

$$d_i' + \lambda d_i'' = d_j' + \lambda d_j''.$$

Then $d_i'' \ne d_j''$, otherwise we obtain $(d_i', d_i'') = (d_j', d_j'')$. Thus for every $i \ne j$ at most one λ exists such that

$$d_i' + \lambda d_i'' = d_j' + \lambda d_j''.$$

The number of pairs (i, j) with $1 \le i < j \le \ell$ is $\ell(\ell-1)/2$. Thus at most $\ell(\ell-1)/2$ values of λ exist such that

$$d_i' + \lambda d_i'' = d_j' + \lambda d_j''$$

for some $i \ne j$. Since $\ell(\ell-1)/2 < p$ the lemma follows.

We have $\mathcal{A} = \{\mathbf{a_1}, \dots, \mathbf{a_r}\}$ and $\mathcal{D} = \{\mathbf{d_1}, \dots, \mathbf{d_\ell}\} \subseteq \mathbb{F}_p^2$, where $r \le k$. By Lemma 7 we may choose $\lambda \in \mathbb{F}_p$ such that both sets

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

and

$$\mathcal{D}' = \{d' + \lambda d'' : \ (d', d'') \in \mathcal{D}\}$$

contain different elements.

Lemma 8 *$(\mathcal{A}', \mathcal{D}')$ possesses property P.*

Proof of Lemma 8 In order to verify the lemma we need to prove that for any $c \in \mathbb{F}_p$ the number of solutions

$$a + d = c, \quad a \in \mathcal{A}', \ d \in \mathcal{D}' \tag{4.11}$$

is even. Indeed, it is clear that the number of solutions of (4.11) is the same as the number of solutions of

$$\begin{aligned} (a', a'') + (d', d'') = (c', c''), \quad (a', a'') \in \mathcal{A}, \ (d', d'') \in \mathcal{D} \\ c' + \lambda c'' = c. \end{aligned} \tag{4.12}$$

Since $(\mathcal{A}, \mathcal{D})$ possesses property P, for each $(c', c'') \in \mathbb{F}_p^2$ 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 even. Thus the number of solutions of the system (4.12) is also even, and equivalently, the number of solutions of (4.11) is also even. This proves Lemma 8.

By Lemma 8 $(\mathcal{A}', \mathcal{D}')$ possesses property P. Thus (r, ℓ, p) is not an admissible triple. By contrast we have the following lemma.

Lemma 9 *(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

$$4^{\ell+r} < p,$$

then (r, ℓ, p) is admissible.

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

Proof of Lemma 9 Parts (i) and (iii) are Theorem 2 in [4] while part (ii) is Theorem 2 in [10].

Since (r, ℓ, p) is not admissible parts b), c) and d) of Theorem 1 follow from Lemma 9. In the proofs of b) and d) we could have replaced Lemma 8 by Lemma 4 in [10], however the lemma there does not suffice to prove part c) in Theorem 1, thus we have preferred to prove Lemma 8 here.

In order to prove part e) in Theorem 1 we note that the degree of the polynomial $h(x_1, x_2)$ in x_1 is odd, thus it cannot be the constant multiple of a perfect square. Using Lemma 5 again part e) follows.

Acknowledgement We would like to thank László Mérai for his valuable remarks and comments.

References

[1] R. Ahlswede, C. Mauduit, A. Sárközy, *Large families of pseudorandom sequences of k symbols and their complexity, Part I*, General Theory of Information Transfer and Combinatorics, eds. R. Ahlswede et al., LNCS 4123, Springer, Berlin 2006; pp. 293-307.

[2] H. Davenport, D. J. Lewis, *Character sums and primitive roots in finite fields*, Rend. Circ. Mat. Palermo (2) 12 (1963), 129-136.

[3] E. Fouvry, N. Katz, *A general stratification theorem for exponential sums, and applications*, J. Reine Angew. Math. 540 (2001), 115-166.

[4] L. Goubin, C. Mauduit, A. Sárközy, *Construction of large families of pseudorandom binary sequences*, J. Number Theory 106 (2004), 56–69.

[5] K. Gyarmati, A. Sárközy, *Equations in finite fields with restricted solution sets, I. (Character sums.)*, Acta Math. Hungar. 118 (2008), 129-148.

[6] J. Hoffstein, D. Lieman, *The distribution of the quadratic symbol in function fields and a faster mathematical stream cipher*, Progress in Computer Science and Applied Logic, Vol. 20, Birkhäuser, Verlag, Basel, 2001; pp. 59-68.

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

[8] C. Mauduit, A. Sárközy, *Construction of pseudorandom binary lattices by using the multiplicative inverse*, Monatshefte Math., to appear.

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

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

[11] L. Rédei, *Algebra*, Pergamon Press, Oxford-New York-Toronto, Ont. 1967.

[12] A. Sárközy, *On finite pseudorandom binary sequences and their applications in cryptography*, Tatra Mt. Math. Publ. 37 (2007), 123-136.

[13] A. Sárközy, C. L. Stewart, *On pseudorandomness in families of sequences derived from the Legendre symbol*, Periodica Math. Hungar. 54 (2007), 163-173.

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

Department of Algebra and Number Theory
Eötvös Loránd University
H-1117 Budapest, Pázmány Péter sétány 1/c
Hungary
e-mail: gykati@cs.elte.hu

Department of Algebra and Number Theory
Eötvös Loránd University
H-1117 Budapest, Pázmány Péter sétány 1/c
Hungary
e-mail: sarkozy@cs.elte.hu

Department of Pure Mathematics
University of Waterloo
N2L 3G1 Waterloo, Ontario
Canada
e-mail: cstewart@uwaterloo.ca