On Legendre symbol lattices, II

Katalin Gyarmati, András Sárközy, Cameron L. Stewart

Abstract

In Part I of this paper we constructed a two dimensional binary lattice by using the Legendre symbol and polynomials of two variables, and we studied its pseudorandom properties. We proved that if the polynomial is non-degenerate then under certain conditions the lattice possesses strong pseudorandom properties, while in the degenerate case it may occur that the lattice has only weak pseudorandom properties. In this paper we continue our analysis of the degenerate case and we will give both lower and upper bounds for the pseudorandom measures of the lattices. We will also give an algorithm to decide if a polynomial is degenerate. Finally, we shall construct a large family of non-degenerate polynomials satisfying one of the sufficient conditions for which the corresponding lattices have strong pseudorandom properties.

Research supported by Hungarian National Foundation for Scientific Research, Grants No. K67676, PD72264, K72731, French-Hungarian exchange program FR-33/2009, János Bolyai Research Fellowship, 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

First we recall some definitions, notation and results from Part I [3] of this paper.

In 1997 Mauduit and Sárközy [6] initiated a new, constructive approach to the theory of pseudorandomness of binary sequences. Their paper was followed by many other papers written on this subject (see the survey paper [10] and the references in [2]). This theory has been extended to n dimensions by Hubert, Mauduit and Sárközy [5]. 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 a positive integer, and the other coordinates of $\mathbf{u_i}$ are 0, so $\mathbf{u_i}$ is of the form $(0, \dots, 0, z_i, 0, \dots, 0)$ (where $z_i \in \mathbb{N}$). Let $t_1, t_2, \dots, t_n$ be integers with $0 \le t_1, t_2, \dots, t_n < N$. Then we will call the set

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

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

In [5] 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 [5] 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 [5], 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 applications one needs large families of binary lattices with strong pseudorandom properties. Constructions of this type have been given in [5], [7] and [8]. However, one would expect that, as in one dimension [1], [4], [6], [11], the most promising constructions can be given by using the Legendre symbol. Indeed, in Part I [3] we presented the following construction of this type.

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

$$\eta(x_1, x_2) = \begin{cases} \left(\frac{f(x_1,x_2)}{p}\right) & \textit{if } (f(x_1, x_2), p) = 1, \\ 1 & \textit{if } p \mid f(x_1, x_2). \end{cases} \tag{1.1}$$

In [3] we showed that there are many polynomials $f \in \mathbb{F}_p[x_1, x_2]$ for which the lattice η defined by (1.1) has a very regular structure, so that it certainly cannot be considered of pseudorandom type. All these polynomials belong to the family described in the following definition.

Definition 2 *A polynomial $f \in \mathbb{F}_p[x_1, x_2]$ is called* degenerate *if there exist $\lambda \in \mathbb{F}_p$, $(\gamma_1, \delta_1), \dots, (\gamma_s, \delta_s)$ in $\mathbb{F}_p \times \mathbb{F}_p$, $\varphi_1, \dots, \varphi_s$ in $\mathbb{F}_p[x]$ and ψ in $\mathbb{F}_p[x_1, x_2]$ for which for all (x_1, x_2) in $\mathbb{F}_p \times \mathbb{F}_p$*

$$f(x_1, x_2) = \lambda \left(\prod_{j=1}^{s} \varphi_j(\gamma_j x_1 + \delta_j x_2) \right) \psi^2(x_1, x_2). \tag{1.2}$$

If f cannot be expressed in form (1.2) *then it is said to be* non-degenerate.

Notice that under this definition $f(x_1, x_2) = x_1^p + x_2$ is degenerate since $f(x_1, x_2) = x_1 + x_2$ for all $(x_1, x_2) \in \mathbb{F}_p \times \mathbb{F}_p$. We are interested in f as a function as opposed to a formal polynomial. However if we suppose that f is of degree less than p in x_1 and in x_2 then the two notions coincide and we may view (1.2) as an identity of polynomials.

Our main result in [3] was that if $f \in \mathbb{F}_p[x_1, x_2]$ is non-degenerate and one of 5 sufficient conditions hold then the pseudorandom measures associated with (1.1) are small.

Theorem A *Let $f \in \mathbb{F}_p[x_1, x_2]$ be a polynomial of degree k. Suppose that $f(x_1, x_2)$ cannot be expressed in the form* (1.2) *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 in* x_1 *(or in* x_2*) are odd.*

Then for the binary p*-lattice defined by* (1.1) *we have*

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

In this paper our goal is to continue the study of Construction 1. First we will analyze the degenerate case. In Section 2 we will analyze the structure of the degenerate polynomials $f(x_1, x_2)$, and we will introduce the notion of the normal form and rank $r = r(f)$ of such a polynomial. In Section 3 we will prove that if f is degenerate, $\ell \leq r = r(f)$, η is defined by (1.1) and one of four specified conditions holds, then $Q_\ell(\eta)$ is small.We will also present an algorithm for deciding whether a given polynomial $f(x_1, x_2)$ is degenerate and, if it is, for determining its normal form. In Section 4 we will show that here the upper bound r cannot be replaced by 2^r . In Section 5 we will study the implementation of Construction 1 and, in particular, we will construct a large family of polynomials $f(x_1, x_2)$ which are non-degenerate and satisfy the first sufficient condition in Theorem A so that the binary lattice η in (1.1) possesses strong pseudorandom properties. In particular its pseudorandom measures $Q_\ell(\eta)$ are small for ℓ not very large.Finally, in Section 6, we construct families of polynomials for which the bounds for the pseudorandom measures are essentially optimal.

2 Structure of degenerate polynomials

In this section our goal is to transform the representation (1.2) of a degenerate polynomial into another more useful one. We will need several lemmas.

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

Proof of Lemma 1. See, for example [9, Theorem 207]. □

Lemma 2 *Let $g_1, g_2 \in \mathbb{F}_p[x, y]$ and $f \in \mathbb{F}_p[x]$ be non-zero polynomials. Suppose that for some $(\alpha, \beta) \in \mathbb{F}_p \times \mathbb{F}_p$*

$$g_1(x, y)g_2(x, y) = f(\alpha x + \beta y). \tag{2.1}$$

Then there exist $f_1, f_2 \in \mathbb{F}_p[x]$ such that

$$g_i(x, y) = f_i(\alpha x + \beta y)$$

for $i = 1, 2$.

Proof of Lemma 2. If $(\alpha, \beta) = (0, 0)$ the result is immediate. Thus we may suppose that $(\alpha, \beta) \neq (0, 0)$ and, without loss of generality, we may assume that $\alpha \neq 0$. Put

$$z = \alpha x + \beta y$$

so that $x = \alpha^{-1}z - \alpha^{-1}\beta y$. We may now define h_1, h_2 in $\mathbb{F}_p[y, z]$ by putting

$$h_i(y, z) = g_i(\alpha^{-1}z - \alpha^{-1}\beta y, y) \quad \text{for } i = 1, 2.$$

From (2.1) we find that

$$h_1(y, z)h_2(y, z) = f(z). \tag{2.2}$$

Write

$$h_1(y,z) = u_a(z)y^a + u_{a-1}(z)y^{a-1} + \cdots + u_0(z),$$
$$h_2(y,z) = v_b(z)y^b + v_{b-1}(z)y^{b-1} + \cdots + v_0(z)$$

and

$$h_1(y,z)h_2(y,z) = w_{a+b}(z)y^{a+b} + w_{a+b-1}(z)y^{a+b-1} + \cdots + w_0(z)$$

where $u_a(z), v_b(z)$ are not the zero polynomial. Clearly we have

$$w_{a+b}(z) = u_a(z)v_b(z). \tag{2.3}$$

But by (2.2), $h_1(y,z)h_2(y,z)$ is a one variable polynomial in z, thus we have

$$w_{a+b}(z) = w_{a+b-1}(z) = \cdots = w_1(z) = 0 \text{ if } a+b > 0. \tag{2.4}$$

It follows from (2.3) and $u_a(z) \neq 0$, $v_b(z) \neq 0$ that $w_{a+b}(z) \neq 0$. Thus by (2.4) we have $a+b=0$ whence $a=b=0$. Then $h_1(y,z) = u_0(z)$, $h_2(y,z) = v_0(z)$ which completes the proof of the lemma. □

We shall identify the elements of $\mathbb{F}_p$ with the p congruence classes modulo p and shall denote the elements of $\mathbb{F}_p \times \mathbb{F}_p$ by (a,b) with a and b integers representing the congruence class of a and of b modulo p. Define the subset T of $\mathbb{F}_p \times \mathbb{F}_p$ by

$$T = \{(0,1),(1,0),(1,1),(2,1),\ldots,(p-1,1)\}.$$

Lemma 3 *Let f be a non-constant degenerate polynomial in $\mathbb{F}_p[x_1,x_2]$ of degree less than p in x_1 and in x_2. Then there exist a non-zero λ in $\mathbb{F}_p$, a non-negative integer r, distinct elements $(\gamma_1,\delta_1),\ldots,(\gamma_r,\delta_r)$ from T, ψ in $\mathbb{F}_p[x_1,x_2]$ and squarefree non-constant polynomials $\varphi_1,\ldots,\varphi_r$ in $\mathbb{F}_p[x]$ for which*

$$f(x_1,x_2) = \lambda\left(\prod_{j=1}^{r} \varphi_j(\gamma_j x_1 + \delta_j x_2)\right)\psi^2(x_1,x_2). \tag{2.5}$$

Further r is uniquely determined and the polynomials $\varphi_j(\gamma_j x_1 + \delta_j x_2)$ and $\psi(x_1, x_2)$ are unique up to constant factors and reordering of $\varphi_1(\gamma_1 x_1 + \delta_1 x_2), \ldots, \varphi_r(\gamma_r x_1 + \delta_r x_2)$.

We shall refer to a decomposition of f as in (2.5) as a normal form of f and to r as the rank of f. Notice that since $(\gamma_1, \delta_1), \ldots, (\gamma_r, \delta_r)$ are distinct elements of T we have

$$\gamma_j \delta_i - \delta_j \gamma_i \neq 0 \quad \text{for } i \neq j. \tag{2.6}$$

Proof of Lemma 3. Let ψ be a polynomial of largest degree for which ψ^2 divides f in $\mathbb{F}_p[x_1, x_2]$. Then since f is degenerate we may write f in the form (1.2) with ψ as above and with $(\gamma_i, \delta_i) \neq (0,0)$ for $i = 1, \ldots, s$. Further we may suppose that $\varphi_1, \ldots, \varphi_s$ are squarefree polynomials in $\mathbb{F}_p[x]$ and that $\varphi_1 \cdots \varphi_s$ is also squarefree.

Suppose that φ is in $\mathbb{F}_p[x]$ and (γ, δ) are in $\mathbb{F}_p \times \mathbb{F}_p \backslash \{(0,0)\}$ and define φ^* in $\mathbb{F}_p[x]$ by

$$\varphi^*(x) = \begin{cases} \varphi(\gamma x) & \text{when } \gamma \neq 0, \\ \varphi(\delta x) & \text{when } \gamma = 0. \end{cases}$$

Then

$$\varphi(\gamma x_1 + \delta x_2) = \begin{cases} \varphi^*(x_1 + \delta \gamma^{-1} x_2) & \text{if } \gamma \neq 0, \\ \varphi^*(x_2) & \text{if } \gamma = 0. \end{cases}$$

Therefore we may write

$$\varphi_1(\gamma_1 x_1 + \delta_1 x_2) \cdots \varphi_s(\gamma_s x_1 + \delta_s x_2)$$

as

$$\varphi_1^*(\gamma_1 x_1 + \delta_1 x_2) \cdots \varphi_s^*(\gamma_s x_1 + \delta_s x_2)$$

where now (γ_i, δ_i) is in T for $i = 1, \ldots, s$. We now collect and multiply together the polynomials φ_i^* for which (γ_i, δ_i) are the same to get a representation for f of the form (2.5).

Suppose that, in addition to (2.5),

$$f(x_1, x_2) = \lambda_1 \left(\prod_{j=1}^{s} \rho_j(\theta_j x_1 + \beta_j x_2) \right) \psi_1^2(x_1, x_2)$$

with $(\theta_1, \beta_1), \ldots, (\theta_s, \beta_s)$ distinct elements of T, λ_1 a non-zero element of $\mathbb{F}_p$, ψ_1 in $\mathbb{F}_p[x_1, x_2]$ and squarefree non-constant polynomials $\rho_1, \ldots, \rho_s$ in $\mathbb{F}_p[x]$. By Lemma 1 $\psi(x)$ is a constant times $\psi_1(x)$ since $\psi^2(x)$ and $\psi_1^2(x)$ correspond to the greatest square factor of f in $\mathbb{F}_p[x_1, x_2]$. Next note that for each j from 1 to s we may decompose $\rho_j(\theta_j x_1 + \beta_j x_2)$ into irreducibles and by Lemma 2

$$\rho_j(\theta_j x_1 + \beta_j x_2) = \rho_{j,1}(\theta_j x_1 + \beta_j x_2) \cdots \rho_{j,t}(\theta_j x_1 + \beta_j x_2)$$

where $\rho_{j,1}, \ldots, \rho_{j,t}$ are irreducible polynomials in $\mathbb{F}_p[x]$. Thus each irreducible $\rho_{j,k}(\theta_j x_1 + \beta_j x_2)$ occurs in the essentially unique decomposition of $\varphi_m(\gamma_m x_1 + \delta_m x_2)$ into irreducibles for some m. Notice that if a polynomial $g(x, y) = f_1(\gamma_1 x + \beta_1 y) = f_2(\gamma_2 x + \beta_2 y)$ with $f_1, f_2 \in \mathbb{F}[x]$ and $\gamma_1 \beta_2 - \gamma_2 \beta_1 \neq 0$ then $g(x, y)$ is a constant. (Indeed, fix $a, b, c, d \in \mathbb{F}_p$ and we will prove that $g(a, b) = g(c, d)$. Since $\gamma_1 \beta_2 - \gamma_2 \beta_1 \neq 0$ the system of linear equations

$$\begin{aligned} \gamma_1 x + \beta_1 y &= \gamma_1 a + \beta_1 b \\ \gamma_2 x + \beta_2 y &= \gamma_2 c + \beta_2 d \end{aligned}$$

has a unique solution in $x, y \in \mathbb{F}_p$. Then

$$\begin{aligned} g(a, b) &= f_1(\gamma_1 a + \beta_1 b) = f_1(\gamma_1 x + \beta_1 y) = g(x, y) = f_2(\gamma_2 x + \beta_2 y) \\ &= f_2(\gamma_2 c + \beta_2 d) = g(c, d).) \end{aligned}$$

Thus, by (2.6), $(\theta_j, \beta_j) = (\gamma_m, \delta_m)$. Repeating this argument with all the irreducible factors of ρ_j and all the irreducible factors of $\varphi_m(\gamma_m x_1 + \delta_m x_z)$ we find that $\varphi_m(\gamma_m x_1 + \delta_m x_2)/\rho_j(\theta_j x_1 + \beta_j x_2)$ is a constant. From this it readily follows that $r = s$ and the result follows. □

We remark that we may determine if a polynomial f is degenerate by first replacing it with a polynomial f^* of degree at most $p-1$ in each variable by using the fact that $x^p = x$ for all x in $\mathbb{F}_p$. We then factor f^* and write f^* as a product of irreducibles multiplied by its largest square divisor. Each irreducible must be tested to see if it is of the form $g(\gamma x + \beta y)$ with $g \in \mathbb{F}_p[x]$ and $(\gamma, \beta) \in T$. Given (γ, β) in T if suffices to check that the irreducible is constant on the lines in $\mathbb{F}_p \times \mathbb{F}_p$ given by $\gamma x + \beta y = c$ for c in $\mathbb{F}_p$ and this is a finite process. Furthermore T is a finite set. Either there is an irreducible not of the form $g(\gamma x + \beta y)$ for any $g \in \mathbb{F}[x]$ and (γ, β) in T in which case f^* is non-degenerate or f^* is degenerate and we may produce the normal form as in the proof of Lemma 3.

3 The pseudorandom measures of small order in the degenerate case.

We will show that if $f(x_1, x_2)$ is a degenerate polynomial and the order ℓ of the pseudorandom measure Q_ℓ is not greater than the rank of f then, for the binary lattice η defined in (1.1), $Q_\ell(\eta)$ is small. In fact our estimates are the same as in the non-degenerate case studied in Theorem A.

Theorem 1 *Let $f(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ be a non-constant degenerate polynomial of reduced normal form* (2.5) *with degree k. Suppose that ℓ, the order of the pseudorandom measure is not greater than the rank r of $f(x_1, x_2)$, 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) $(4k)^\ell < p$ *or* $(4\ell)^k < p$*,*

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 lattice η *defined in* (1.1) *we have*

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

Proof of Theorem 1. The proof will be based on the following result.

Lemma 4 *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* $cq(\mathbf{x})^2$ *with* $c \in \mathbb{F}_p$*,* $q \in \mathbb{F}_p[x_1, x_2]$*. Let* k *be the degree of the polynomial* $f(x_1, x_2)$*. Then for the binary* p*-lattice* η *defined in* (1.1) *we have*

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

Proof of Lemma 4. This is Lemma 5 in [3] (note that we proved it by using a consequence of Weil's theorem [12]). □

In order to ensure the applicability of this lemma, we have to show that it follows from one of the 5 assumptions in Theorem 1 that there are not distinct $\mathbf{d_1}, \dots, \mathbf{d}_\ell \in \mathbb{F}_p^2$ such that the polynomial

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

is of the form $cq(\mathbf{x})^2$ with $c \in \mathbb{F}_p$, $q \in \mathbb{F}_p[x_1, x_2]$. Indeed, if this is proved, then the statement of Theorem 1 follows from Lemma 4 immediately.

We will prove this by contradiction. Assume that

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

is the constant multiple of a perfect square. Then we will prove

$$r + 1 \leq \ell,$$

where r denotes the rank of f, which contradicts our assumption.

Write

$$\mathbf{d}_i = (d'_i, d''_i)$$

for $i = 1, \dots, l$.

Suppose that f has the normal form

$$f(x_1, x_2) = \lambda \prod_{j=1}^{r} f_j(\alpha_j x_1 + \beta_j x_2) \psi^2(x_1, x_2)$$

with $\lambda \in \mathbb{F}_p \backslash \{0\}$, $(\alpha_1, \beta_1), \dots, (\alpha_r, \beta_r)$ distinct elements of T, $f_1, \dots, f_r$ square-free non-constant polynomials in $\mathbb{F}_p[x]$ and $\psi \in \mathbb{F}_p[x_1, x_2]$. Then it follows that

$$\prod_{j=1}^{r} f_j(\alpha_j x_1 + \beta_j x_2 + \alpha_j d'_1 + \beta_j d''_1) f_j(\alpha_j x_1 + \beta_j x_2 + \alpha_j d'_2 + \beta_j d''_2) \cdots$$
$$f_j(\alpha_j x_1 + \beta_j x_2 + \alpha_j d'_\ell + \beta_j d''_\ell). \qquad (3.1)$$

is a non-zero multiple of the square of a polynomial in $\mathbb{F}_p[x_1, x_2]$.

Now we will introduce an equivalence relation which is similar to the one used in the proof of Theorem 1 in [1].

Definition 3 *Two polynomials $\varphi(x_1, x_2)$, $\psi(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ are t-equivalent (t for translation) if there are $a_1, a_2 \in \mathbb{F}_p$ such that*

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

Consider any two factors $f_{j_1}(\alpha_{j_1} x_1 + \beta_{j_1} x_2 + \alpha_{j_1} d'_{v_1} + \beta_{j_1} d''_{v_1}) = f^*_{j_1}(\alpha_{j_1} x_1 + \beta_{j_1} x_2)$ and $f_{j_2}(\alpha_{j_2} x_1 + \beta_{j_2} x_2 + \alpha_{j_2} d'_{v_2} + \beta_{j_2} d''_{v_2}) = f^*_{j_2}(\alpha_{j_2} x_1 + \beta_{j_2} x_2)$ with $j_1 \neq j_2$

on the right hand side of (3.1), factor them into irreducible polynomials, and consider an irreducible factor φ_1 of the former polynomial and φ_2 of the latter polynomial. Then by Lemma 2, these irreducible factors are of the form $\varphi_1(\alpha_{j_1}x_1 + \beta_{j_1}x_2)$, and $\varphi_2(\alpha_{j_2}x_1 + \beta_{j_2}x_2)$. Assume that these two polynomials are t-equivalent, so that there exist $a, b \in \mathbb{F}_p$ such that

$$\begin{aligned}\varphi_1(\alpha_{j_1}x_1 + \beta_{j_1}x_2) &= \varphi_2(\alpha_{j_2}(x_1 + a) + \beta_{j_2}(x_2 + b)) \\ &= \varphi_2((\alpha_{j_2}x_1 + \beta_{j_2}x_2) + (\alpha_{j_2}a + \beta_{j_2}b)) = \varphi_3(\alpha_{j_2}x_1 + \beta_{j_2}x_2)\end{aligned} \tag{3.2}$$

(where $\varphi_3(z) = \varphi_2(z + (\alpha_{j_2}a + \beta_{j_2}b))$). Both the first and last polynomial in (3.2) are in normal form, and since the normal form is unique, we must have $(\alpha_{j_1}, \beta_{j_1}) = (\alpha_{j_2}, \beta_{j_2})$ whence $j_1 = j_2$.

Thus if two factors $f_{j_1}(\alpha_{j_1}x_1 + \beta_{j_1}x_2 + \alpha_{j_1}d'_{v_1} + \beta_{j_1}d''_{v_1})$ and $f_{j_2}(\alpha_{j_2}x_1 + \beta_{j_2}x_2 + \alpha_{j_2}d'_{v_2} + \beta_{j_2}d''_{v_2})$ on the right hand side of (3.1) have t-equivalent irreducible factors then $j_1 = j_2$. But then the expression (3.1) is of the form $cq(x_1, x_2)^2$ if and only if

$$f_j(\alpha_j x_1 + \beta_j x_2 + \alpha_j d'_1 + \beta_j d''_1) \cdots f_j(\alpha_j x_1 + \beta_j x_2 + \alpha_j d'_\ell + \beta_j d''_\ell)$$

is the constant multiple of a square for every $1 \leq j \leq r$. Writing $z = \alpha_j x_1 + \beta_j x_2$ and $d^*_j(i) = \alpha_j d'_i + \beta_j d''_i \in \mathbb{F}^*_p$ we obtain for $1 \leq j \leq r$:

$$f_j(z + d^*_j(1)) f_j(z + d^*_j(2)) \cdots f_j(z + d^*_j(\ell))$$

is of the form $cq(z)^2$. Let D_j be the set of terms of the sequence $(d^*_j(1), \ldots, d^*_j(\ell))$ which occur with odd multiplicity. If D_j is not empty, then

$$\prod_{d \in D_j} f_j(z + d)$$

is the constant multiple of a perfect square. By the proof of Lemma 2 in [1] this is not possible (note that by Lemma 2, in case a) the one-variable polynomial $f(z)$ is also irreducible). It remains to consider the case when D_j is empty for $j = 1, \ldots, r$. Then, for $1 \le j \le r$, in the sequence

$$(\alpha_j d'_1 + \beta_j d''_1,\ \alpha_j d'_2 + \beta_j d''_2, \ldots,\ \alpha_j d'_\ell + \beta_j d''_\ell)$$

every term occurs with even multiplicity, hence every term occurs with multiplicity at least 2. Then for every j, there is a number $2 \le i(j) \le \ell$ such that

$$\alpha_j d'_1 + \beta_j d''_1 = \alpha_j d'_{i(j)} + \beta_j d''_{i(j)}.$$

We will prove that $1, i(1), i(2), \ldots, i(r)$ are different numbers. It is clear that none of $i(1), i(2), \ldots, i(r)$ is equal to 1. It remains to prove that

$$x = i(j_1) = i(j_2) \tag{3.3}$$

is not possible. Suppose that (3.3) holds. Then

$$\begin{aligned} \alpha_{j_1} d'_1 + \beta_{j_1} d''_1 &= \alpha_{j_1} d'_x + \beta_{j_1} d''_x, \\ \alpha_{j_2} d'_1 + \beta_{j_2} d''_1 &= \alpha_{j_2} d'_x + \beta_{j_2} d''_x. \end{aligned}$$

Thus

$$\begin{aligned} \alpha_{j_1}(d'_1 - d'_x) - \beta_{j_1}(d''_1 - d''_x) &= 0, \\ \alpha_{j_2}(d'_1 - d'_x) - \beta_{j_2}(d''_1 - d''_x) &= 0. \end{aligned} \tag{3.4}$$

Since $(d'_1, d''_1) \ne (d'_x, d''_x)$ from (3.4) we obtain

$$\alpha_{j_1}\beta_{j_2} - \alpha_{j_2}\beta_{j_1} = 0,$$

from which $j_1 = j_2$ follows. Thus $1 < i(1), i(2), \ldots, i(r) \le \ell$ and $i(1), i(2), \ldots, i(r)$ are different numbers, so that

$$r + 1 \le \ell$$

which contradicts the conditions of Theorem 1 and this completes the proof of the theorem. □

4 The pseudorandom measures of large order in the degenerate case

In Section 3 we showed that in the degenerate case if $\ell \le r$ then $Q_\ell(\eta)$ is small. Now we will prove that $Q_\ell(\eta)$ is large for some ℓ with ℓ at most 2^r.

Theorem 2 *Let $f \in \mathbb{F}_p[x_1, x_2]$ be a degenerate polynomial with rank r and degree m and n in x_1 and x_2, respectively. Then there exists a positive integer ℓ with ℓ at most 2^r for which*

$$Q_\ell(\eta) \ge p^2 - 4rp^{3/2} - 2\ell(m+n)p.$$

Proof of Theorem 2 We may assume that $r \le p^{1/2}/4$ since otherwise the theorem is immediate. Suppose that $f(x_1, x_2)$ has the normal form

$$f(x_1, x_2) = \lambda \prod_{j=1}^{r} f_j(\alpha_j x_1 + \beta_j x_2)\psi(x_1, x_2)^2$$

with $(\alpha_1, \beta_1), \dots, (\alpha_r, \beta_r)$ distinct elements from T. We distinguish two cases. In the first case all of the α_i's are non-zero. In the second case one of the α_i's is zero and in that case we may suppose, without loss of generality, that $(\alpha_1, \beta_1) = (0, 1)$. There exists an integer γ_i with $1 \le |\gamma_i| \le p^{1/2} + 1$ such that $\gamma_i \alpha_i$ is congruent modulo p to a positive integer of size at most $p^{1/2}$ for $i = 1, \dots, r$ in the first case and $i = 2, \dots, r$ in the second case. To see this consider the first $[p^{1/2}] + 2$ multiples of α_i in $\mathbb{F}_p$. Two of them have representations which differ by at most $(p-1)/([p^{1/2}]+1)$, so by at most $p^{1/2}$, and the difference gives the result. In the second case we may take $\gamma_1 = 1$ so $\gamma_1 \beta_1 = 1$.

Put

$$E = \{\boldsymbol{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_r) \text{ with } \varepsilon_i \in \{0, 1\} \text{ for } i = 1, \dots, r\}$$

and for each $\boldsymbol{\varepsilon}$ in E put

$$\mathbf{d}(\boldsymbol{\varepsilon}) = \varepsilon_1(\beta_1, -\alpha_1)\gamma_1 + \cdots + \varepsilon_r(\beta_r, -\alpha_r)\gamma_r.$$

Notice that for each $\boldsymbol{\varepsilon}$ in E, $\mathbf{d}(\boldsymbol{\varepsilon})$ has coordinates represented by integers between $-r(p^{1/2}+1)$ and $r(p^{1/2}+1)$.

Lemma 5

$$\prod_{\boldsymbol{\varepsilon}\in E} f(\mathbf{x}+\mathbf{d}(\boldsymbol{\varepsilon}))$$

is the square of a polynomial in $\mathbb{F}_p[x_1, x_2]$.

Proof of Lemma 5. Write

$$\overline{f_j}(x_1, x_2) = f_j(\alpha_j x_1 + \beta_j x_2),$$

for $j = 1, \ldots, r$, so that

$$f(\mathbf{x}) = \lambda \prod_{j=1}^{r} \overline{f_j}(x_1, x_2)\psi^2(x_1, x_2). \tag{4.1}$$

For each integer j with $1 \le j \le r$ we may split E into two disjoint sets E_j^0 and E_j^1 where $\boldsymbol{\varepsilon}$ in E is in E_j^0 if $\varepsilon_j = 0$ and is in E_j^1 if $\varepsilon_j = 1$. For $\boldsymbol{\varepsilon}$ in E_j^0 let $\boldsymbol{\varepsilon}^1$ denote the element of E_j^1 with the same coordinates as $\boldsymbol{\varepsilon}$ except for the j-th coordinate which is 1. Then, for $\boldsymbol{\varepsilon}$ in E_j^0,

$$\overline{f_j}(\mathbf{x}+\mathbf{d}(\boldsymbol{\varepsilon})) = \overline{f_j}(\mathbf{x}+\mathbf{d}(\boldsymbol{\varepsilon}^1))$$

and so

$$\begin{aligned}\prod_{\boldsymbol{\varepsilon}\in E} \overline{f_j}(\mathbf{x}+\mathbf{d}(\boldsymbol{\varepsilon})) &= \prod_{\boldsymbol{\varepsilon}\in E_j^0} (\overline{f_j}(\mathbf{x}+\mathbf{d}(\boldsymbol{\varepsilon}))\overline{f_j}(\mathbf{x}+\mathbf{d}(\boldsymbol{\varepsilon}^1))) \\ &= \left(\prod_{\boldsymbol{\varepsilon}\in E_j^0} \overline{f_j}(\mathbf{x}+\mathbf{d}(\boldsymbol{\varepsilon}))\right)^2.\end{aligned}$$

The result now follows from (4.1) since $|E|$ is even. □

Let D be the set of $\mathbf{d} = \mathbf{d}(\boldsymbol{\varepsilon})$ which occur with odd multiplicity among the terms $\mathbf{d}(\boldsymbol{\varepsilon})$ with $\boldsymbol{\varepsilon}$ in E. It follows from Lemma 5 that if D is non-empty then

$$\prod_{\mathbf{d} \in D} f(\mathbf{x} + \mathbf{d}) \tag{4.2}$$

is the square of a polynomial in $\mathbb{F}_p[x_1, x_2]$.

We claim that $(0, 0)$ is in D. Certainly $\mathbf{d}(0, \dots, 0) = (0, 0)$. Further if $\boldsymbol{\varepsilon}$ is in E and $\mathbf{d}(\boldsymbol{\varepsilon}) = (0, 0)$ then $\varepsilon_1\alpha_1\gamma_1 + \cdots + \varepsilon_r\alpha_r\gamma_r = 0$. Since $\alpha_i\gamma_i$ is congruent to a positive integer of size at most $p^{1/2}$ and r is at most $p^{1/2}/4$ we see that $\varepsilon_1 = \cdots = \varepsilon_r = 0$ in the first case and that $\varepsilon_2 = \cdots = \varepsilon_r = 0$ in the second case. But in the second case we find that $\mathbf{d}(\boldsymbol{\varepsilon}) = (\varepsilon_1\beta_1\gamma_1, 0) = (\varepsilon_1, 0)$ so $\varepsilon_1 = 0$. Therefore if $\boldsymbol{\varepsilon}$ is in E and $\mathbf{d}(\boldsymbol{\varepsilon}) = (0, 0)$ we see that $\boldsymbol{\varepsilon} = (0, \dots, 0)$ and this shows that $(0, 0)$ is in D. Clearly, $|D| \equiv |E| \pmod 2$ and since $|E| = 2^r$ we conclude that

$$2 \leq |D| \leq |E| = 2^r.$$

Let $\mathbf{d} = (d_1, d_2)$ in D. Then d_1 and d_2 are integers between $-r(p^{1/2} + 1)$ and $r(p^{1/2} + 1)$. Put

$$d_1^1 = \min_{\mathbf{d} \in D} d_1, \quad d_2^1 = \min_{\mathbf{d} \in D} d_2$$

and

$$\mathbf{d}_0 = (d_1^1, d_2^1).$$

Then $\mathbf{d} - \mathbf{d}_0 \in I_p^2$ for $\mathbf{d} \in D$ since $r \leq p^{1/2}/4$. Next put

$$B = \{(x_1, x_2) \in I_p^2 \mid 0 \leq x_i < p - 2r(p^{1/2} + 1) \text{ for } i = 1, 2\}.$$

Notice that

$$|B| \geq (p - 2r(p^{1/2} + 1))^2 \geq p^2 - 4rp^{3/2}. \tag{4.3}$$

Put

$$F(\mathbf{x}) = \prod_{\mathbf{d}\in D} f(\mathbf{x}+\mathbf{d}-\mathbf{d}_0).$$

$F(\mathbf{x})$ is the square of a polynomial in $\mathbb{F}_p[x_1,x_2]$ by (4.2). Let $\ell = |D|$. With η defined by (1.1) we find that

$$\begin{aligned} Q_\ell(\eta) &\geq \left|\sum_{\mathbf{x}\in B}\prod_{\mathbf{d}\in D}\eta(\mathbf{x}+\mathbf{d}-\mathbf{d}_0)\right| = \left|\sum_{\substack{\mathbf{x}\in B\\ F(\mathbf{x})\neq 0}}\left(\frac{F(\mathbf{x})}{p}\right) + \sum_{\substack{\mathbf{x}\in B\\ F(\mathbf{x})=0}}\prod_{\mathbf{d}\in D}\eta(\mathbf{x}+\mathbf{d}-\mathbf{d}_0)\right| \\ &\geq \sum_{\substack{\mathbf{x}\in B\\ F(\mathbf{x})\neq 0}} 1 - \sum_{\substack{\mathbf{x}\in B\\ F(\mathbf{x})=0}} 1 \geq |\mathcal{B}| - 2\sum_{\substack{\mathbf{x}\in\mathbb{F}_p^2\\ F(\mathbf{x})=0}} 1. \end{aligned} \tag{4.4}$$

It is easy to see that if a polynomial $F \in \mathbb{F}_p[x_1,x_2]$ is of degree u and v in x_1 and x_2, respectively, then the number of its zeros $\mathbf{x}\in\mathbb{F}_p^2$ is at most $(u+v)p$. Thus it follows from (4.3) and (4.4) that

$$Q_\ell(\eta) \geq p^2 - 4rp^{3/2} - 2\ell(m+n)p$$

which proves Theorem 2. □

5 Generating a large family of suitable polynomials

In this section we construct a large family of polynomials which are non-degenerate.

Theorem 3 *Let $f \in \mathbb{F}_p[x_1,x_2]$ be a polynomial of the form*

$$f(x_1,x_2) = x_1^k + x_1x_2g(x_1,x_2) + x_2h(x_2) \tag{5.1}$$

with $g \in \mathbb{F}_p[x_1, x_2]$*,* $\deg g \le k-3$*,* $h \in \mathbb{F}_p[x_2]$*,* $\deg h(x_2) \le k-2$ *and* $x_2 \nmid h(x_2)$*. Then for the binary lattice* η *defined in* (1.1) *we have*

$$Q_\ell(\eta) < 11k\ell p^{3/2}\log p. \tag{5.2}$$

Proof of Theorem 3. We will need the following generalization of the Schönemann-Eisenstein theorem.

Lemma 6 *If* $f(x) = a_0x^n + \cdots + a_n$ *is a polynomial over an integral domain* R *and* $\mathfrak{a}$ *is a maximal ideal of* R *with*

$$\begin{aligned} a_0 &\not\equiv 0 \pmod{\mathfrak{a}}, \\ a_1 \equiv \cdots \equiv a_n &\equiv 0 \pmod{\mathfrak{a}}, \\ a_n &\not\equiv 0 \pmod{\mathfrak{a}^2} \end{aligned}$$

then $f(x)$ *cannot be decomposed in* $R[x]$ *into a product of non-constant factors.*

Proof of Lemma 6. See, for example [9, Theorem 282]. □

$R = \mathbb{F}_p[x_2]$ is an integral domain and $\mathfrak{a} =< x_2 >$ is a maximal ideal in it. Then the conditions of Lemma 6 hold for the polynomial $f(x_1, x_2) \in R[x_1]$ in (5.1), thus $f(x_1, x_2)$ is irreducible.

In order to use Theorem 1 we prove that $f(x_1, x_2)$ is not of the form (2.5). Since $f(x_1, x_2)$ is irreducible we have to prove that $f(x_1, x_2)$ is not of the form

$$f(x_1, x_2) = f_1(\alpha_1 x_1 + \beta_1 x_2). \tag{5.3}$$

Let h be the degree of f_1 and consider the terms of degree h in f_1, so

$$f_1(\alpha_1 x_1 + \beta_1 x_2) = c(\alpha_1 x_1 + \beta_1 x_2)^h + f_2(\alpha_1 x_1 + \beta_1 x_2),$$

where the degree of $f_2(\alpha_1 x_1 + \beta_1 x_2)$ is $\leq h-1$ and $c \neq 0 \in \mathbb{F}_p$. Clearly, $c(\alpha_1 x_1 + \beta_1 x_2)^h$ equals the sum of the terms of degree k of $f(x_1, x_2)$, thus by the conditions of Theorem 2 we have

$$c(\alpha_1 x_1 + \beta_1 x_2)^h = x_1^k.$$

We may suppose that k is less than p since the result is immediate otherwise. It then follows that $h = k$, $c = \alpha_1 = 1$ and $\beta_1 = 0$, thus from (5.3)

$$f(x_1, x_2) = f_1(x_1). \tag{5.4}$$

On the other hand $f(x_1, x_2)$ contains a power of x_2, and this contradicts (5.4). Thus $f(x_1, x_2)$ is not of the form (2.5). We have also proved that $f(x_1, x_2)$ is irreducible, and by using Theorem 1 a) we obtain the result. □

6 A Legendre symbol construction with optimal bounds

As we remarked already in [3], our upper bounds are not optimal; in particular, in (5.2) the optimal upper bound would be, up to logarithmic factors, p (with a factor depending on k and ℓ). On the other hand this construction is more natural than the ones using finite fields in [5], [7] or [8] (where the bounds are sharper), and it can be implemented faster. However, we will show that for a certain (rather special) family of polynomials the finite field construction presented in [7] is equivalent to a Legendre symbol construction of type (1.1). Thus in this case we obtain a family of binary lattices which combines the advantages of the two constructions: as in [7] we have optimal bounds, and as a Legendre symbol construction it can be implemented fast and easily.

Indeed, combining Theorems 1 and 2 of [7], we get the following result:

Theorem A. *Let p be an odd prime, $n \in \mathbb{N}$, $q = p^n$, and denote the quadratic character of $\mathbb{F}_q$ by γ (setting also $\gamma(0) = 0$). Consider the linear vector space formed by the elements of $\mathbb{F}_q$ over $\mathbb{F}_p$, and let $v_1, \ldots, v_n$ be a basis of this vector space. Let $f(\mathbf{x}) \in \mathbb{F}_q[\mathbf{x}]$ be a polynomial of degree k with*

$$0 < k < p \tag{6.1}$$

which has no multiple zero. Define the n-dimensional binary p-lattice $\eta(\mathbf{x}) : I_p^n \to \{-1, +1\}$ by

$$\begin{aligned} \eta(\mathbf{x}) &= \eta((x_1, \ldots, x_n)) \\ &= \begin{cases} \gamma(f(x_1 v_1 + \cdots + x_n v_n)) & \text{for } f(x_1 v_1 + \cdots + x_n v_n) \neq 0 \\ 1 & \text{for } f(x_1 v_1 + \cdots + x_n v_n) = 0. \end{cases} \end{aligned} \tag{6.2}$$

Assume also that $\ell \in \mathbb{N}$ with

$$4^{n(k+\ell)} < p. \tag{6.3}$$

Then we have

$$Q_\ell(\eta) < k\ell \left(q^{1/2}(1 + \log p)^n + 2 \right). \tag{6.4}$$

Our next result follows from Theorem A in the case that $n = 2$ and for a special choice of v_1, v_2 and the polynomial f.

Theorem 4 *Let p be an odd prime and let r be a quadratic non-residue modulo p. Then the polynomial $x^2 - r$ is irreducible over $\mathbb{F}_p$; denote one of its zeros by θ, and consider the extension of $\mathbb{F}_p$ by θ: $\mathbb{F}_p[\theta] (\cong \mathbb{F}_{p^2})$. Let k and ℓ be integers which satisfy* (6.1) *and* (6.3), *and assume that $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k \in \mathbb{F}_p$ satisfy*

$$a_i + b_i\theta \neq a_j + b_j\theta \text{ and } a_i + b_i\theta \neq a_j - b_j\theta \text{ for } 1 \leq i < j \leq k. \tag{6.5}$$

Put

$$\tilde{f}(x_1, x_2) = \prod_{i=1}^{k} \big((x_1 - a_i)^2 - r(x_2 - b_i)^2\big) \tag{6.6}$$

and

$$\tilde{\eta}(\mathbf{x}) = \tilde{\eta}(\mathbf{x}) = \tilde{\eta}((x_1, x_2)) = \begin{cases} \left(\frac{\tilde{f}(x_1,x_2)}{p}\right) & \textit{if } (\tilde{f}(x_1, x_2), p) = 1 \\ 1 & \textit{if } p \mid \tilde{f}(x_1, x_2). \end{cases} \tag{6.7}$$

For each positive integer ℓ with

$$4^{2(\ell+k)} < p \tag{6.8}$$

we have

$$Q_\ell(\tilde{\eta}) < \ell k \left(p(1 + \log p)^2 + 2\right).$$

Proof of Theorem 4. By the definition of θ and Euler's lemma, we have

$$\theta^p = (\theta^2)^{\frac{p-1}{2}}\theta = r^{\frac{p-1}{2}}\theta = -\theta. \tag{6.9}$$

We will use Theorem A with $n = 2$, $q = p^2$, $v_1 = 1$, $v_2 = \theta$, so that now the elements of $\mathbb{F}_q = \mathbb{F}_{p^2}$ are represented in the form $x_1 + x_2\theta$. Then by the generalization of Euler's lemma to $\mathbb{F}_q$ and (6.9), for $x_1 + x_2\theta \in \mathbb{F}^*_{p^2}$, so with $(x_1, x_2) \neq (0, 0)$, we have

$$\begin{aligned} \gamma(x_1 + x_2\theta) &= (x_1 + x_2\theta)^{\frac{p^2-1}{2}} = (x_1 + x_2\theta)^{\frac{p^2-p}{2}}(x_1 + x_2\theta)^{\frac{p-1}{2}} \\ &= ((x_1 + x_2\theta)^p)^{\frac{p-1}{2}} (x_1 + x_2\theta)^{\frac{p-1}{2}} = (x_1^p + x_2^p\theta^p)^{\frac{p-1}{2}} (x_1 + x_2\theta)^{\frac{p-1}{2}} \\ &= (x_1 - x_2\theta)^{\frac{p-1}{2}}(x_1 + x_2\theta)^{\frac{p-1}{2}} = (x_1^2 - x_2^2\theta^2)^{\frac{p-1}{2}} = (x_1^2 - rx_2^2)^{\frac{p-1}{2}} \\ &= \left(\frac{x_1^2 - rx_2^2}{p}\right). \end{aligned}$$

By the multiplicativity of γ and the Legendre symbol, it follows that writing

$$f(x_1 + x_2\theta) = \prod_{i=1}^{k} ((x_1 + x_2\theta) - (a_i + b_i\theta)) \tag{6.10}$$

and defining $\eta(\mathbf{x}) = \eta((x_1, x_2))$ as in (6.2) we have

$$\begin{aligned}
\eta(\mathbf{x}) = \gamma(f(x_1 + x_2\theta)) = \gamma\left(\prod_{i=1}^{k}((x_1 + x_2\theta) - (a_i + b_i\theta))\right) \\
= \prod_{i=1}^{k} \gamma\left((x_1 + x_2\theta) - (a_i + b_i\theta)\right) = \prod_{i=1}^{k} \gamma\left((x_1 - a_i) + (x_2 - b_i)\theta\right) \\
= \prod_{i=1}^{k} \left(\frac{(x_1 - a_i)^2 - r(x_2 - b_i)^2}{p}\right) = \left(\frac{\prod_{i=1}^{k}((x_1 - a_i)^2 - r(x_2 - b_i)^2)}{p}\right) \\
= \left(\frac{\tilde{f}(x_1, x_2)}{p}\right) = \tilde{\eta}(\mathbf{x}) \quad (\text{for } f(x_1 + x_2\theta) \neq 0) \qquad (6.11)
\end{aligned}$$

with the polynomial $\tilde{f}$ and the lattice $\tilde{\eta}$ defined by (6.6) and (6.7), respectively, and trivially we have

$$\eta(\mathbf{x}) = \tilde{\eta}(\mathbf{x}) \text{ for } f(x_1 + x_2\theta) = 0. \qquad (6.12)$$

By (6.5) and the definition of r, the polynomial $\tilde{f}$ has no multiple zero, and now (6.3) holds by (6.8). Thus Theorem A can be applied, and then we obtain from (6.4), (6.11) and (6.12) that

$$Q_\ell(\eta) = Q_\ell(\tilde{\eta}) < \ell k \left(p(1 + \log p)^2 + 2\right)$$

which completes the proof of Theorem 4.

We remark that the construction in Theorem 4 could be extended by also considering higher degree factors in (6.10). Even more generally, we may consider polynomials f which are not given in a product form. In either case, we may use the fact that if $f(x_1 + x_2\theta) = p(x_1, x_2) + \theta q(x_1, x_2)$ (with $f(z) \in \mathbb{F}_p[z]$, $p(x_1, x_2)$, $q(x_1, x_2) \in \mathbb{F}_p[x_1, x_2]$ and θ, r defined as above), then we have

$$\gamma(f(x_1 + \theta x_2)) = \gamma(p(x_1, x_2) + \theta q(x_1, x_2)) = \left(\frac{p^2(x_1, x_2) - rq^2(x_1, x_2)}{p}\right).$$

However this would make the polynomial $\tilde{f}$ in (6.6) in Theorem 4 much more complicated.

Finally, we would like to discuss the implementation of the construction in Theorem 4. The critical point of the implementation is to find a quadratic non-residue r. If p is fixed, then it is known that the GRH implies that the least quadratic non-residue modulo p is less than $(\log p)^c$ (with some positive constant c), and since the quadratic character of a given residue can be decided in polynomial time (by using Jacobi symbols), r can be chosen as the least quadratic non-residue modulo p which can be determined in polynomial time. On the other hand, no algorithm is known for finding the least quadratic non-residue in polynomial time without any unproved hypothesis. However, in most cases one need not fix p, and this difficulty can be avoided. Namely, we may start out from the fact that if p is a prime of the form $4k-1$, then -1 is a quadratic non-residue modulo p. Thus it is worthwhile to make first a long sequence of primes $p_1 = 3 < p_2 < \cdots < p_t$ of the form $4k-1$ with say, $p_i < p_{i+1} < 2p_i$, and if we need a prime p of size about N with $p \equiv -1 \pmod 4$, then we take the first prime from this sequence greater than N, and we take $r = -1$. (If we want a large prime p of the form $4k-1$, then we may use the fact that the Mersenne primes are of the form $4k-1$.)

References

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

[2] K. Gyarmati, C. Mauduit and A. Sárközy, *Measures of pseudorandomness of binary lattices, I (The measures Q_k, normality.)*, Acta Arith.

144 (2010), 295–313.

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

[4] J. Hoffstein and 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.

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

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

[7] C. Mauduit and A. Sárközy, *On large families of pseudorandom binary lattices*, Unif. Distr. Theory 2 (2007), 23-37.

[8] C. Mauduit and A. Sárközy, *Construction of pseudorandom binary lattices by using the multiplicative inverse*, Monatsh. Math. 153 (2008), 217-231.

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

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

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

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