Uniform Distribution Theory **2** (2007), no.1, 23–37

uniform distribution theory

ON LARGE FAMILIES OF PSEUDORANDOM BINARY LATTICES

Christian Mauduit — András Sárközy

ABSTRACT. In an earlier paper Hubert and the authors introduced and studied the notion of pseudorandomness of binary lattices, and they also gave a construction for a binary lattice with strong pseudorandom properties. However, in the applications one needs *large families* of "good" binary lattices; here a construction of this type is presented which uses the quadratic characters of finite fields and polynomials.

Communicated by Oto Strauch

Dedicated to Professor Robert F. Tichy on the occasion of his 50th birthday

1. Introduction

In a series of papers the authors (partly with further coauthors) developed a constructive theory of finite pseudorandom binary *sequences*. In particular, in [6] they introduced the measures of pseudorandomness, and they showed that the Legendre symbol sequence $\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \ldots, \left(\frac{p-1}{p}\right)$ has strong pseudorandom properties in terms of these measures. Later constructions for *large families* of "good" sequences (finite binary sequences with strong pseudorandom properties in terms of the introduced measures) were also given. In terms of computational time and bounds for the pseudorandom measures, the best construction is, perhaps, the one in [2].

This construction is based on the use of the *Legendre symbol*:

Assume that p is a prime number, $f(x) \in \mathbb{F}_p[x]$ has degree $k(>0)$, $f(x)$ has no multiple zero in $\overline{\mathbb{F}}_p$ (the algebraic closure of $\mathbb{F}_p$) and define the binary sequence

2000 Mathematics Subject Classification: Primary 11K45.
Keywords: Pseudorandom, binary lattice, finite fields, Legendre symbol.
Research partially supported by the Hungarian National Foundation for Scientific Research, Grants No. T 043623 and T 049693, and by a CNRS–HAS exchange program.

$E_p = (e_1, \dots, e_p)$ by

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

It was shown in [2] that the so-called "well-distribution measure" of E_p is small, and if one of the following conditions holds:

(i) $k < p$ and $\ell = 2$;

(ii) $$(4\ell)^k < p; \tag{1.2}$$

(iii) $k < p$, $\ell < p$, and 2 is a primitive root modulo p, then the "correlation of order ℓ" is also small (see [6] for the definition of the well-distribution measure and correlation measure; see also [8]).

In [5] Hubert, Mauduit and Sárközy extended this constructive theory of pseudorandomness to *several dimensions*. Let I_N^n denote the set of the n-dimensional vectors whose all coordinates are selected from the set $\{0, 1, \dots, N-1\}$:

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

We call this set *n-dimensional N-lattice* or briefly (if n is fixed) *N-lattice*.

Definition 1. A function of the type

$$\eta(\boldsymbol{x}) : I_N^n \to \{-1, +1\} \tag{1.3}$$

is called *n-dimensional binary N-lattice* or briefly *binary lattice*.

(Note that in the special case $n = 1$ these functions are the binary sequences $E_N \in \{-1, +1\}^N$.) In [5] the use of the following measures of pseudorandomness of binary lattices was proposed:

Definition 2. If $\eta = \eta(\boldsymbol{x})$ is an n-dimensional binary N-lattice of the form (1.3), $k \in \mathbb{N}$, and $\boldsymbol{u}_i$ $(i = 1, 2, \dots, n)$ denotes the n-dimensional unit vector whose i-th coordinate is 1 and the other coordinates are 0, then write

$$Q_k(\eta) = \max_{\boldsymbol{B}, \boldsymbol{d}_1, \dots, \boldsymbol{d}_k, \boldsymbol{T}} \Bigg| \sum_{j_1=0}^{t_1} \cdots \sum_{j_n=0}^{t_n} \eta(j_1 b_1 \boldsymbol{u}_1 + \cdots + j_n b_n \boldsymbol{u}_n + \boldsymbol{d}_1) \tag{1.4}$$

$$\dots \eta(j_1 b_1 \boldsymbol{u}_1 + \cdots + j_n b_n \boldsymbol{u}_n + \boldsymbol{d}_k) \Bigg|,$$

where the maximum is taken over all n-dimensional vectors $\boldsymbol{B} = (b_1, \dots, b_n)$, $\boldsymbol{d}_1, \dots, \boldsymbol{d}_k, \boldsymbol{T} = (t_1, \dots, t_n)$ such that their coordinates are non-negative integers, $b_1, \dots, b_n$ are non-zero, $\boldsymbol{d}_1, \dots, \boldsymbol{d}_k$ are distinct, and all the points $j_1 b_1 \boldsymbol{u}_1 + \cdots + j_n b_n \boldsymbol{u}_n + \boldsymbol{d}_i$ occuring in the multiple sum belong to the n-dimensional N-lattice I_N^n. Then $Q_k(\eta)$ is called the *pseudorandom* (briefly PR) *measure of order k of n*.

(Note that in the one-dimensional special case $Q_k(\eta)$ is the combined PR-measure Q_k of order k which was also introduced in [6] and which combines the well-distribution measure and correlation measure of order k mentioned above.)

In [5] we proved that for a fixed $k \in \mathbb{N}$ and for a truly random n-dimensional binary N-lattice $\eta(\boldsymbol{x})$, we have

$$N^{n/2} \ll Q_k(\eta) \ll N^{n/2}(\log N^n)^{1/2}$$

with probability $> 1-\varepsilon$, while the trivial upper bound for $Q_k(\eta)$ is N^n. Thus an n-dimensional binary N-lattice η can be considered as a "good" pseudorandom binary lattice, if the PR measure of order k of η is "small" in terms of N (in particular, $Q_k(\eta) = o(N^n)$ for fixed n and $N \to +\infty$) for small k.

Moreover, in [5] we gave an example for a "good" n-dimensional binary lattice (for any n):

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 $v_1, \dots, v_n$ be a basis of this vector space, i.e., assume that $v_1, \dots, v_n$ are linearly independent over $\mathbb{F}_p$. Define the mapping $\eta(\boldsymbol{x})$ of type*

$$\eta(\boldsymbol{x}) : I_p^n \to \{-1, +1\}$$

by

$$\eta(\boldsymbol{x}) = \eta\big((x_1, \dots, x_n)\big) = \begin{cases} \gamma(x_1 v_1 + \dots + x_n v_n) & \text{for } (x_1, \dots, x_n) \neq (0, \dots, 0) \\ 1 & \text{for } (x_1, \dots, x_n) = (0, \dots, 0) \end{cases} \tag{1.5}$$

for any $x_1, \dots, x_n \in \mathbb{F}_p$. Then for any $k \in \mathbb{N}$ we have

$$Q_k(\eta) < kq^{1/2}(1 + \log p)^n.$$

However, in the applications (e.g., in cryptography) one usually needs not just a few "good" PR binary lattices but we need a "large" family of binary lattices with strong PR properties. Thus in this paper *our goal is to construct large families of n-dimensional binary lattices with strong pseudorandom properties*. Indeed, we will show that by using also some ideas from [5], with some further work the one-dimensional construction can be adapted and extended to several dimensions. In particular, in [2] (and later also in [7] and [3]) and addition theorem (formulated as Lemma 3 in [1]) played a crucial role. In [1] we analyzed this theorem, and we showed that it is nearly (apart from a $\log\log p$ factor) the best possible. The original proof of this result cannot be adapted to several dimensions. Here in several dimensions we will present a different proof which will also improve on the original one-dimensional theorem so that in this

sharper form it will give the best possible estimate for $\min(|\mathcal{A}|, |\mathcal{B}|)$ (apart from a constant factor).

Throughout this paper we will use the following notations: we write $e(\alpha) = e^{2\pi i\alpha}$, p denotes an odd prime, $n \in \mathbb{N}$, $q = p^n$, and γ, $v_1, \dots, v_n$ are defined in the same way as in construction (1.5).

2. The construction and pseudorandomness under admissibility assumption

As in [2], first we have to define the notion of admissibility.

Definition 3. If $q = p^n$ is a prime power, $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_q$, and $\mathcal{A} + \mathcal{B}$ represents every element of $\mathbb{F}_q$ with even multiplicity, i.e., for all $c \in \mathbb{F}_q$,

$$a + b = c, \quad a \in \mathcal{A}, \quad b \in \mathcal{B} \tag{2.1}$$

has even number of solutions (including the case when there are no solutions), then the sum $\mathcal{A} + \mathcal{B}$ is said to have *property P*.

Definition 4. If $q = p^n$ is a prime power, $k, \ell \in \mathbb{N}$ and $k, \ell \le q$, then (k, ℓ, q) is said to be an *admissible triple* if there are no $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_q$ such that $|\mathcal{A}| = k$, $|\mathcal{B}| = \ell$, and $\mathcal{A} + \mathcal{B}$ possesses property P.

We will prove the following theorem:

Theorem 1. *Assume that $q = p^n$ is the power of an odd prime, $f(x) \in \mathbb{F}_q[x]$ has degree ℓ with*

$$0 < \ell < p, \tag{2.2}$$

$f(x)$ has no multiple zero in $\overline{\mathbb{F}}_q$, and define the n-dimensional binary p-lattice

$$\eta(\boldsymbol{x}) : I_p^n \to \{-1, +1\}$$

by

$$\eta(\boldsymbol{x}) = \eta\big((x_1, \dots, x_n)\big) = \\ = \begin{cases} \gamma\big(f(x_1v_1 + \cdots + x_nv_n)\big) & \text{for } f(x_1v_1 + \cdots + x_nv_n) \neq 0 \\ 1 & \text{for } f(x_1v_1 + \cdots + x_nv_n) = 0. \end{cases}$$

Assume also that $k \in \mathbb{N}$ and the triple (r, k, q) is admissible for all $r \le \ell$. Then we have

$$Q_k(\eta) < k\ell\big(q^{1/2}(1 + \log p)^n + 2\big). \tag{2.3}$$

We remark that if we take

$$f(x) = \prod_a \big(x + (a, 0, \dots, 0)\big)$$

where a runs over the elements of the prime field $\mathbb{F}_p$ of $\mathbb{F}_q$, then clearly we have

$$f(x) = f\big(x + (b, 0, \dots, 0)\big) \text{ for all } b \in \mathbb{F}_p.$$

Thus for $k = 2$, $\boldsymbol{d}_1 = (0, 0, \dots, 0)$, $b \in \mathbb{F}_p$, $b \neq 0$, $\boldsymbol{d}_2 = (b, 0, \dots, 0)$ every term of the n-fold sum in (1.5) is

$$\gamma\big(f(j_1 b_1 \boldsymbol{u}_1 + \dots + j_n b_n \boldsymbol{u}_n)\big)\gamma\big(f(j_1 b_1 \boldsymbol{u}_1 + \dots + j_n b_n \boldsymbol{u}_n + (b, 0, \dots, 0))\big) =$$
$$= \gamma^2\big(f(j_1 b_1 \boldsymbol{u}_1 + \dots + j_n b_n \boldsymbol{u}_n)\big) = 1$$

if $f(j_1 b_1 \boldsymbol{u}_1 + \dots + j_n b_n \boldsymbol{u}_n) \neq 0$, and the terms with $f(j_1 b_1 \boldsymbol{u}_1 + \dots + j_n b_n \boldsymbol{u}_n) = 0$ are also 1 by the definition of η. Thus we have

$$Q_2(\eta) = \max_{t_1, t_2, \dots, t_n} (t_1 + 1)(t_2 + 1) \dots (t_n + 1) = p^n = q$$

so that one cannot give a nontrivial bound for $Q_2(\eta)$. This example shows that an assumption of type (2.2) is necessary.

P r o o f o f T h e o r e m 1. Write $\boldsymbol{d}_i = (d_1^{(i)}, \dots, d_n^{(i)})$ (for $i = 1, \dots, k$), and consider the general term of the n-fold sum in (1.4):

$$\eta\big(j_1 b_1 \boldsymbol{u}_1 + \dots + j_n b_n \boldsymbol{u}_n + \boldsymbol{d}_1\big) \dots \eta\big(j_1 b_1 \boldsymbol{u}_1 + \dots + j_n b_n \boldsymbol{u}_n + \boldsymbol{d}_k\big) = \tag{2.4}$$
$$= \eta\big((j_1 b_1 + d_1^{(1)}, \dots, j_n b_n + d_n^{(1)})\big) \dots \eta\big((j_1 b_1 + d_1^{(k)}, \dots, j_n b_n + d_n^{(k)})\big).$$

Now write

$$z = j_1(b_1 v_1) + \dots + j_n(b_n v_n) \tag{2.5}$$

so that z belongs to the box

$$B' = \Big\{ \sum_{i=1}^{n} j_i (b_i v_i) : \ 0 \leq j_i < t_i \text{ for } i = 1, \dots, n \Big\}, \tag{2.6}$$

and set

$$z_i = d_1^{(i)} v_1 + \dots + d_n^{(i)} v_n. \tag{2.7}$$

If $z \in B'$ is such that $f(z + z_1) \dots f(z + z_k) \neq 0$, and we write $f(z) = c f_1(z)$ with $c \in \mathbb{F}_q$, where $f_1(z)$ is a monic polynomial, then by the definition of η and the multiplicativity of γ, the product in (2.4) is

$$\gamma\big(f(z + z_1)\big) \dots \gamma\big(f(z + z_k)\big) = \gamma(c^k)\gamma\big(f_1(z + z_1) \dots f_1(z + z_k)\big).$$

It follows that

$$\Big|\sum_{j_1=0}^{t_1}\cdots\sum_{j_n=0}^{t_n}\eta(j_1b_1\boldsymbol{u}_1+\cdots+j_nb_n\boldsymbol{u}_n+\boldsymbol{d}_1)\dots\eta(j_1b_1\boldsymbol{u}_1+\cdots+j_nb_n\boldsymbol{u}_n+\boldsymbol{d}_k)-$$

$$-\gamma(c^k)\sum_{z\in B'}\gamma\big(f_1(z+z_1)\dots f_1(z+z_k)\big)\Big|\le$$

$$\le\sum_{\substack{z\in B'\\ f(z+z_1)\dots f(z+z_k)=0}}(1+1)\le 2\sum_{\substack{z\in\mathbb{F}_q\\ f(z+z_1)\dots f(z+z_k)=0}}1\le 2k\ell. \tag{2.8}$$

Now we need the following result of Winterhof:

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

$$\Big|\sum_{z\in B}\chi(f(z))\Big|<mq^{1/2}(1+\log p)^n.$$

Proof of Lemma 1. This is a part of Theorem 2 in [10] (where its proof was based on A. Weil's theorem [9]).

Write $h(z)=f_1(z+z_1)\dots f_1(z+z_k)$. Then in order to prove (2.3), it suffices to show:

Lemma 2. *If q,f,k,ℓ are defined as in Theorem 1, then $h(x)$ has at least one zero in $\overline{\mathbb{F}}_q$ whose multiplicity is odd.*

Indeed, assuming that Lemma 2 has been proved, the proof of (2.3) can be completed in the following way: by Lemma 2, we may apply Lemma 1 with γ, 2, $h(x)$ and B' in place of χ, d, $f(x)$ and B, respectively (since $h(x)$ has at least one zero of odd multiplicity, it cannot be a square). The number m of the distinct zeros of $h(x)$ is $\le\deg h(x)=k\deg f_1=k\ell$, thus applying Lemma 1 we obtain

$$\Big|\sum_{z\in B'}\gamma(h(z))\Big|<k\ell q^{1/2}(1+\log p)^n. \tag{2.9}$$

(2.3) follows from (2.8) and (2.9).

Thus it remains to prove Lemma 2.

Proof of Lemma 2. We will say that the polynomials $\varphi(x) \in \mathbb{F}_q[x]$, $\psi(x) \in \mathbb{F}_q[x]$ are equivalent: $\varphi \sim \psi$ if there is an $a \in \mathbb{F}_q$ such that $\psi(x) = \varphi(x + a)$. Clearly, this is an equivalence relation.

Write $f_1(x)$ as the product of irreducible monic polynomials over $\mathbb{F}_q$. It follows from our assumption on $f(x)$ that these irreducible factors are distinct, and by (2.2), their degree is $\leq \deg f_1 = \deg f = \ell < p$. Let us group these factors so that in each group the equivalent irreducible factors are collected. Consider a typical group $\varphi(x + a_1), \ldots, \varphi(x + a_r)$.

Then writing $h(x)$ as the product of monic irreducible polynomials over $\mathbb{F}_q$, all the polynomials $\varphi(x + a_i + z_j)$ with $1 \leq i \leq r$, $1 \leq j \leq k$ occur amongst the factors. All these polynomials are equivalent, and no other irreducible factor belonging to this equivalence class will occur amongst the irreducible factors of $h(x)$.

Distinct monic irreducible polynomials cannot have a common zero, and if $\varphi(x) \in \mathbb{F}_q[x]$, $0 < \deg \varphi < p$ and $b, c \in \mathbb{F}_q$, $b \neq c$, then $\varphi(x + b) \neq \varphi(x + c)$. (Namely, if $h \in \mathbb{F}_q$, $h \neq 0$, then $\varphi(y + h) \neq \varphi(y)$ since the derivative of $\varphi(y)$ is not identically 0 by $0 < \deg \varphi < p$.) Thus the conclusion of Lemma 2 fails, i.e., each of the zeros of $h(x)$ is of even multiplicity, if and only if in each group, formed by equivalent irreducible factors $\varphi(x + a_i + z_j)$ of $h(x)$, every polynomial of the form $\varphi(x + c)$ occurs with even multiplicity, i.e., for even number of pairs a_i, z_j. In other words, writing $\mathcal{A} = \{a_1, \ldots, a_r\}$, $\mathcal{Z} = \{z_1, \ldots, z_k\}$, for each group $\mathcal{A} + \mathcal{Z}$ must possess property P. Now consider any of these groups (by $\deg f > 0$ there is at least one such group).

Since $\mathcal{A} + \mathcal{Z}$ possesses property P, thus (r, k, q) (with $r = |\mathcal{A}|$) is *not* an admissible triple. Here we have $r \leq \deg f_1 = \deg f = \ell$ which contradicts our assumption in Theorem 1 on the triples r, k, q so that, indeed, the conclusion of Lemma 2 cannot fail, and this completes the proof of Theorem 1. □

3. Criteria for admissibility

To be able to use Theorem 1 one needs sufficient criteria for admissibility. We will prove two criteria of this type.

Theorem 2. (i) *For every prime power $q = p^n$ and for $\ell \in \mathbb{N}$, $\ell < p$ the triple $(\ell, 2, q)$ is admissible.*

(ii) *If $q = p^n$ is a prime power, $k, \ell \in \mathbb{N}$, and*

$$4^{n(k+\ell)} < p, \tag{3.1}$$

then the triple (k, ℓ, q) is admissible.

Note that in the special case $q = p$ in [2], Theorem 2 there was a further criterion: if p is a prime such that 2 is a primitive root modulo p, then every triple (k, ℓ, p) with $k < p$, $\ell < p$ is admissible. Unfortunately, we have not been able to prove a similar criterion for general q; we will return to this subject in Section 4.

P r o o f o f T h e o r e m 2. Some of the ideas in the proof was also used in the proof of Theorem 2 in [2], thus we will leave some details to the reader.

(i) Assume that contrary to the assertion

$$0 < \ell < p, \tag{3.2}$$

and there are $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_q$ such that $|\mathcal{A}| = \ell$, $|\mathcal{B}| = 2$, and (2.1) has even number of solutions for all $c \in \mathbb{F}_q$, and write $\mathcal{B} = \{b, b + d\}$ (with $d \neq 0$). Then every element of $\mathcal{A} + b$ has at least 2 representations in form (2.1) whence it follows that $\mathcal{A}+b = \mathcal{A}+b+d$. Therefore, $\mathcal{A}+b = \mathcal{A}+b+rd$ for any $r \in \{0, 1, \dots, p-1\}$. For any fixed $a \in \mathcal{A}$ we have $a + b + rd \in \mathcal{A} + b + rd = \mathcal{A} + b$ whence

$$\ell = |\mathcal{A}| = |\mathcal{A} + b| \geq \big|\{a + b + rd : \ r \in \{0, 1, \dots, p - 1\}\}\big| = p$$

which contradicts (3.2).

(ii) For $a \in \mathbb{Z}$, let $r(a)$ denote the absolute least residue of a modulo p, i.e., define $r(a) \in \mathbb{Z}$ by

$$r(a) \equiv a \pmod p, \quad |r(a)| \leq \frac{p-1}{2}.$$

First we will prove

Lemma 3. *If p is an odd prime, $t \in \mathbb{N}$,*

$$4^t < p \tag{3.3}$$

and $h_1, \dots, h_t \in \mathbb{Z}$, then there is an integer m such that $0 < m < p$ and

$$|r(mh_i)| \leq \left[\frac{p}{4}\right]. \tag{3.4}$$

Proof of Lemma 3. For $h \in \mathbb{Z}$ define $y(h)$ as the least non-negative such that h is congruent to one of the integers in the interval

$$\left(y(h)\Big(\Big[\frac{p}{4}\Big] + 1\Big), (y(h) + 1)\Big(\Big[\frac{p}{4}\Big] + 1\Big)\right]$$

modulo p. Clearly, we have $y(h) \in \{0, 1, 2, 3\}$ for every y. For $u = 1, 2, \dots, p$, consider the t-tuple $\big(y(uh_1), \dots, y(uh_t)\big)\big(\in \{0, 1, 2, 3\}^t\big)$. The number of these t-tuples is p which, by (3.3), is greater than the number of the distinct t-tuples

in $\{0,1,2,3\}^t$. Thus by the pigeonhole principle there are at least two of these t-tuples which coincide:

$$\big(y(uh_1),\dots,y(uh_t)\big) = \big(y(vh_1),\dots,y(vh_t)\big) \quad \text{with } 1 \le u < v \le t.$$

Then writing $m = v - u$, it follows from $y(uh_i) = y(vh_i)$ that

$$|r(mh_i)| = |r\big((v-u)h_i\big)| = |r(vh_i - uh_i)| \le \left[\frac{p}{4}\right] \quad \text{for } i = 1,\dots,t$$

which proves (3.4).

In order to complete the proof of case (ii) in Theorem 2, clearly it suffices to show:

Lemma 4. *If $q = p^n$, $k, \ell \in \mathbb{N}$,*

$$4^{n(k+\ell)} < p, \tag{3.5}$$

$\mathcal{A}, \mathcal{B} \subset \mathbb{F}_q$, $|\mathcal{A}| = k$ and $|\mathcal{B}| = \ell$, then there is a $c \in \mathbb{F}_q$ such that the equation

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

has exactly one solution.

We remark that in the special case $q = p$ in [2] we used a weaker result of this type (in which (3.5) was replaced by a stronger assumption). The proof given in [2] cannot be extended to the case of general q. However, introducing new ideas and, in particular, an "ordering" as defined below, we can prove this both more general and sharper result here.

Proof of Lemma 4. Again we represent every element $u \in \mathbb{F}_q$ in the form

$$u = x_1 v_1 + \cdots + x_n v_n$$

where $v_1,\dots,v_n$ is a basis for the vector space $\mathbb{F}_q$ over $\mathbb{F}_p$, and $x_1,\dots,x_n$ belong to the prime field $\mathbb{F}_p$. We identify $\mathbb{F}_p$ by the field of the residue classes $\bmod p$, and we do not distinguish between the residue classes and their representant elements. We write $x_i = x_i(u)$. Now we apply Lemma 3 with the numbers $x_i(a)$ (with $i = 1,\dots,n$, $a \in \mathcal{A}$) and $x_j(b)$ (with $j = 1,\dots,n$, $b \in \mathcal{B}$) in place of $h_1,\dots,h_t$. Then we have

$$t = n|\mathcal{A}| + n|\mathcal{B}| = n(k+\ell)$$

so that (3.3) holds by (3.1) and thus, indeed, Lemma 3 can be applied. We obtain that there is an $m \in \mathbb{N}$ with

$$0 < m < p \tag{3.6}$$

and

$$\big|r\big(mx_i(a)\big)\big|,\ \big|r\big(mx_j(b)\big)\big| \le \left[\frac{p}{4}\right] \quad \text{for } i=1,\dots,n,\ a\in\mathcal{A},\ j=1,\dots,n,\ b\in\mathcal{B}. \tag{3.7}$$

Let W denote the set of the n tuples $(w_1,\dots,w_n)$ with $-\left[\frac{p}{4}\right] \le w_i \le +\left[\frac{p}{4}\right]$ for $i=1,\dots,n$. We introduce an ordering in W: if $\boldsymbol{w}=(w_1,\dots,w_n)\in W$, $\boldsymbol{w}'=(w_1',\dots,w_n')\in W$ and $\boldsymbol{w}\ne\boldsymbol{w}'$, then we say that $\boldsymbol{w}<\boldsymbol{w}'$ if and only if defining i by $w_1=w_1',\dots,w_{i-1}=w_{i-1}',\ w_i\ne w_i'$ (if $w_1\ne w_1'$ then we take $i=1$), we have $w_i<w_i'$. This ordering clearly possesses the following fundamental properties:

(i) if $\boldsymbol{w}\in W$, $\boldsymbol{w}'\in W$, then exactly one of the relations $\boldsymbol{w}=\boldsymbol{w}'$, $\boldsymbol{w}<\boldsymbol{w}'$, $\boldsymbol{w}'<\boldsymbol{w}$ holds;

(ii) it is transitive: $\boldsymbol{w}<\boldsymbol{w}'$, $\boldsymbol{w}'<\boldsymbol{w}''$ implies $\boldsymbol{w}<\boldsymbol{w}''$.

Then clearly, any subset of W has a uniquely determined the greatest element. By (3.7), both sets $W_{\mathcal{A}}=\big\{\big(r(mx_1(a)),\dots,r(mx_n(a))\big)\ :\ a\in\mathcal{A}\big\}$ and $W_{\mathcal{B}}=\big\{\big(r(mx_1(b)),\dots,r(mx_n(b))\big)\ :\ b\in\mathcal{B}\big\}$ are subsets of W. Denote the greatest elements of $\mathcal{A}$ and $\mathcal{B}$ by $\boldsymbol{w}_{\mathcal{A}}$ and $\boldsymbol{w}_{\mathcal{B}}$, and assume that they correspond to $\overline{a}\in\mathcal{A}$ and $\overline{b}\in\mathcal{B}$, respectively: $\boldsymbol{w}_{\mathcal{A}}=\big(r(mx_1(\overline{a})),\dots,r(mx_n(\overline{a}))\big)$, $\boldsymbol{w}_{\mathcal{B}}=\big(r(mx_1(\overline{b})),\dots,r(mx_n(\overline{b}))\big)$. Then by the maximality of $\boldsymbol{w}_{\mathcal{A}}$ and $\boldsymbol{w}_{\mathcal{B}}$, the sum $\boldsymbol{w}_{\mathcal{A}}+\boldsymbol{w}_{\mathcal{B}}$ has no other representation in the form

$$\boldsymbol{w}+\boldsymbol{w}' \quad \text{with } \boldsymbol{w}\in W_{\mathcal{A}},\ \boldsymbol{w}'\in W_{\mathcal{B}}. \tag{3.8}$$

By (3.7), the coordinates of any sum of form (3.8) belong to the interval

$$\left[-2\left[\frac{p}{4}\right],+2\left[\frac{p}{4}\right]\right]\subset\left[-\left[\frac{p}{2}\right],+\left[\frac{p}{2}\right]\right],$$

and the integers in this interval are incongruent modulo p. Thus if two sums of the form (3.8) are different (as vectors from $\mathbb{Z}^n$), then they are also different modulo p (i.e., as vectors from $\mathbb{F}_p^n$). But then for any $a\in\mathcal{A}$, $b\in\mathcal{B}$ we have

$$\begin{aligned} m(\overline{a}+\overline{b}) &= \big(r(mx_1(\overline{a}))+r(mx_1(\overline{b}))\big)v_1+\dots+\big(r(mx_n(\overline{a}))+r(mx_n(\overline{b}))\big)\ne\\ &\ne\big(r(mx_1(a))+r(mx_1(b))\big)v_1+\dots+\big(r(mx_n(a))+r(mx_n(b))\big)v_n=\\ &= m(a+b). \end{aligned}$$

It follows that writing $c=\overline{a}+\overline{b}$, this element of $\mathbb{F}_q$ has exactly one representation in the form

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

namely, the one with $a=\overline{a}$, $b=\overline{b}$, and this completes the proof of Lemma 4 and thus also of (ii) in Theorem 2. □

4. Examples

Finally, we remark that we conjecture that, as in [2], a further sufficient criterion can be added to Theorem 2:

(iii) If $q = p^n$ is a prime power such that

$$2 \text{ is a primitive root modulo } p, \tag{4.1}$$

then for every pair $k, \ell \in \mathbb{N}$ with

$$k < p, \quad \ell < p, \tag{4.2}$$

the triple (k, ℓ, q) is admissible.

In the special case $q = p$ in [2] we proved this but the proof given there cannot be adapted to the general case, and we have not been able to find a proof of different nature to prove the conjecture.

Note that in the conjecture above both conditions (4.1) and (4.2) are necessary. Indeed, we proved in [2] that if 2 is not a primitive root modulo p, then there are $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_p$ such that $1 < |\mathcal{A}|, |\mathcal{B}| < p$ and $\mathcal{A} + \mathcal{B}$ possesses property P (in $\mathbb{F}_p$). Then clearly, for each $i = 1, 2, \ldots, n$, the sum of the sets

$$\mathcal{A}^{(i)} = \{av_i : \ a \in \mathcal{A}\}$$

and

$$\mathcal{B}^{(i)} = \{bv_i : \ b \in \mathcal{B}\}$$

possesses property P in $\mathbb{F}_q$, which shows that (4.1) is necessary.

Moreover, if $\mathcal{A}$ is the prime field $\mathbb{F}_p$ of $\mathbb{F}_q$, $\mathcal{B}$ is any subset of $\mathbb{F}_p$ with $|\mathcal{B}| = 2$, then we have $|\mathcal{A}| = k = p$ and $|\mathcal{B}| = \ell = 2$ (so that the first inequality in (4.2) just fails while the second one holds for $p > 2$), and clearly, (2.1) has exactly 2 solutions for every $c \in \mathbb{F}_p$ and 0 solution for $c \in \mathbb{F}_q \setminus \mathbb{F}_p$ so that $\mathcal{A} + \mathcal{B}$ possesses property P, and thus the triple $(k, \ell, q) = (p, 2, q)$ is not admissible.

In this counterexample we constructed subsets $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_q$ such that

$$1 < |\mathcal{A}|, |\mathcal{B}| < q, \tag{4.3}$$

$$\mathcal{A} + \mathcal{B} \ \text{ possesses property } P, \tag{4.4}$$

and $\mathcal{A}$ was a subspace of the linear vector space formed by $\mathbb{F}_q$ over $\mathbb{F}_p$. It is easy to construct further examples such that (4.3) and (4.4) hold, and

$$\text{either } \mathcal{A} \text{ or } \mathcal{B} \text{ is a subspace of the linear vector space } \mathbb{F}_q \text{ over } \mathbb{F}_p; \tag{4.5}$$

we may call these examples trivial examples.

One can construct nontrivial examples in the following way: in [2] we presented primes and subsets $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_p$ such that $1 < |\mathcal{A}|$, $|\mathcal{B}| < p$, and $\mathcal{A}+\mathcal{B}$ possesses property P in $\mathbb{F}_p$ (see Examples 1, 2 and 3 there). Further one-dimensional examples can be constructed in a similar manner.

It is much more difficult to construct nontrivial examples which are more than one-dimensional. The polynomial method described in Section 4 of [2], which was also used in [2] for proving the special case $q = p$ of the conjecture above, can be extended easily to a method involving polynomials in several variables, which can be used for looking for nontrivial examples but, unfortunately, we have not been able to prove the general form of this conjecture in this way. This method of polynomials in several variables is the following:

To simplify and shorten the discussion we restrict ourselves to the special case $q = p^2$. Then again we represent every element of $\mathbb{F}_q$ as $x_1 + x_2 v$, where $0 \le x_1, x_2 < p$ and $v \in \mathbb{F}_q \setminus \mathbb{F}_p$. Then to any $\mathcal{C} \in \mathbb{F}_q$ we assign the polynomial $P_{\mathcal{C}}(x, y) \in \mathbb{F}_2[x, y]$ defined by

$$P_{\mathcal{C}}(x, y) = \sum_{x_1 + x_2 v \in \mathbb{F}_q} x^{s(x_1)} y^{s(x_2)}$$

where $s(n)$ denotes the least non-negative element of the residue class n modulo p. Moreover, if

$$f(x, y) = \sum_{m \in \mathcal{M}} \sum_{n \in \mathcal{N}} x^m y^n \in \mathbb{F}[x, y],$$

then define $\varphi(f(x, y))$ by

$$\varphi(f(x, y)) = \sum_{m \in \mathcal{M}} \sum_{n \in \mathcal{N}} x^{s(m)} y^{s(n)}.$$

Then clearly, for $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_q$, the sum $\mathcal{A} + \mathcal{B}$ possesses property P if and only if

$$\varphi\big(P_{\mathcal{A}}(x, y) P_{\mathcal{B}}(x, y)\big) = 0 \quad \big(\text{in } \mathbb{F}_2[x, y]\big). \tag{4.6}$$

In [2] the analogous statement was sufficient to prove the special case $q = p$ of conjecture (iii) above and also to construct counterexamples. Here in the case of the general q statement (4.6) above is not enough for proving the conjecture but still it helps to find counterexamples.

When looking for counterexamples, we may start out from the observation that if a polynomial $f(x, y)$ is given, then $\varphi(f(x, y))$ can be obtained from $f(x, y)$ by reducing the x powers in $f(x, y)$ modulo $x^p + 1$ in $\mathbb{F}_2[x]$ and reducing the y powers modulo $y^p + 1$ in $\mathbb{F}_2[y]$. Thus as in [2], we use the fact that $x^p + 1$ can be factorized in $\mathbb{F}_2[x]$ in a nontrivial way (nontrivial: the factors are of degree ≥ 2)

if (and only if) 2 is *not* a primitive root modulo p. Thus if p is of this type, then there are $P_1(x)$, $P_2(x)$ with

$$x^p + 1 = P_1(x)P_2(x) \tag{4.7}$$

(and $\deg P_1, \deg P_2 \geq 2$). Then we are looking for polynomials $P_{\mathcal{A}}(x, y)$, $P_{\mathcal{B}}(x, y)$ (which determine $\mathcal{A}$, $\mathcal{B}$ uniquely) satisfying (4.6) by trying to represent the 0 polynomial as

$$\begin{aligned} P_1(y)(x^p + 1) + P_1(x)(y^p + 1) &= P_1(y)P_1(x)P_2(x) + P_1(x)P_1(y)P_2(y) = \\ &= \big(P_1(x)P_1(y)\big)\big(P_2(x) + P_2(y)\big) = 0 \end{aligned}$$

(where P_1, P_2 are the polynomials in (4.7)), and then we take

$$P_{\mathcal{A}}(x, y) = P_1(x)P_1(y) \tag{4.8}$$

and

$$P_{\mathcal{B}}(x, y) = P_2(x) + P_2(y). \tag{4.9}$$

Example 1. We take $q = 7^2$. Then we have

$$x^7 + 1 = (x^3 + x + 1)(x^4 + x^2 + x + 1) \quad (\text{in } \mathbb{F}_2[x])$$

so that now in (4.7) we may choose $P_1(x) = x^3+x+1$ and $P_2(x) = x^4+x^2+x+1$. Then (4.8) and (4.9) become

$$\begin{aligned} P_{\mathcal{A}}(x, y) = P_1(x)P_1(y) &= (x^3 + x + 1)(y^3 + y + 1) = \\ &= x^3y^3 + x^3y + x^3 + xy^3 + xy + x + y^3 + y + 1 \end{aligned}$$

and

$$\begin{aligned} P_{\mathcal{B}}(x, y) = P_2(x)P_2(y) &= (x^4 + x^2 + x + 1)(y^4 + y^2 + y + 1) = \\ &= x^4 + x^2 + x + y^4 + y^2 + y \end{aligned}$$

and, indeed, it is easy to check that for these polynomials (4.6) holds. These polynomials correspond to the subsets

$$\mathcal{A} = \{3 + 3v, 3 + v, 3, 1 + 3v, 1 + v, 1, 3v, v, 0\}$$

and

$$\mathcal{B} = \{4, 2, 1, 4v, 2v, v\},$$

and then the sum $\mathcal{A} + \mathcal{B}$ possesses property P, which proves that the triple $(9, 6, 49)$ is not admissible.

In this example we have $|\mathcal{A}| = 9 > 7 = p$. One also might like to see a construction with $q = p^2$, $|\mathcal{A}|$, $|\mathcal{B}| < p$. For such a construction we have to go higher with p.

Example 2. Take $q = 31^2$ so that now

$$x^p + 1 = x^{31} + 1 = (x^5 + x^2 + 1)\big(x^{26} + x^{23} + x^{21} + x^{20} + x^{17} + x^{16} + \\ + x^{15} + x^{14} + x^{13} + x^9 + x^8 + x^6 + x^5 + x^4 + x^2 + 1\big)$$

whence

$$P_1(x) = x^5 + x^2 + 1$$

and

$$P_2(x) = x^{26} + x^{23} + x^{21} + x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^9 + x^8 + x^6 + x^5 + x^4 + x^2 + 1.$$

Then we have

$$P_{\mathcal{A}}(x, y) = P_1(x)P_1(y) = (x^5 + x^2 + 1)(y^5 + y^2 + 1) = \\ = x^5y^5 + x^5y^2 + x^5 + x^2y^5 + x^2y^2 + x^2 + y^5 + y^2 + 1$$

and

$$P_{\mathcal{B}}(x, y) = P_2(x) + P_2(y) = \\ = x^{26} + x^{23} + x^{21} + x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + \\ + x^9 + x^8 + x^6 + x^5 + x^4 + x^2 + y^{26} + y^{23} + y^{21} + y^{20} + \\ + y^{17} + y^{16} + y^{15} + y^{14} + y^{13} + y^9 + y^8 + y^6 + y^5 + y^4 + y^2.$$

Again (4.6) holds, and these polynomials define the subsets

$$\mathcal{A} = \{5 + 5v, 5 + 2y, 5, 2 + 5v, 2 + 2v, 2, 5v, 2v, 1\}$$

and

$$\mathcal{B} = \{26, 23, 21, 20, 17, 16, 15, 14, 13, 9, 8, 6, 5, 4, 2, 26v, 23v, 21v, \\ 20v, 17v, 16v, 15v, 14v, 13v, 9v, 8v, 6v, 5v, 4v, 2v\}$$

whose sum $\mathcal{A}+\mathcal{B}$ possesses property P, which proves that the triple $(9,\ 30,\ 31^2 = 961)$ is not admissible.

REFERENCES

[1] AHLSWEDE, R. – CASSAIGNE, J. – SÁRKÖZY, A.: *On the correlation of binary sequences*, Applied Discrete Math. (to appear).

[2] GOUBIN, L. – MAUDUIT, C. – SÁRKÖZY, A.: *Construction of large families of pseudorandom binary sequences*, J. Number Theory **106** (2004), 56–69.

[3] GYARMATI, K.: *On a family of pseudo-random binary sequences*, Periodica Math. Hungar. **49** (2004), 45–63.

[4] GYARMATI, K. – SÁRKÖZY, A.: *Equations in finite fields with restricted solution sets, I. (Character sums)*, Finite Fields Appl. (to appear).
[5] HUBERT, P. – MAUDUIT, C. – SÁRKÖZY, A.: *On pseudorandom binary lattices*, Acta Arith. (to appear).
[6] MAUDUIT, C. – SÁRKÖZY, A.: *On finite pseudorandom binary sequences, I: Measure of pseudorandomness, the Legendre symbol*, Acta Arith. **82** (1997), 365–377.
[7] MAUDUIT, C. – SÁRKÖZY, A.: *Construction of pseudorandom binary sequences by using the multiplicative inverse*, Acta Math. Hungar. **108** (2005), 239–252.
[8] SÁRKÖZY, A. – STEWART, C.L.: *On pseudorandomness in families of sequences derived from the Legendre symbol*, Periodica Math. Hungar. (to appear).
[9] WEIL, A.: *Sur les courbes algébriques et les variétés qui s'en déduissent*, Act. Sci. Ind. 1041, Hermann, Paris, 1948.
[10] WINTERHOF, A.: *Some estimates for character sums and applications*, Des. Codes Cryptogr. **22** (2001), 123–131.

Received November 23, 2006
Revised March 20, 2007
Accepted

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

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