Monatsh Math 153, 217–231 (2008)
DOI 10.1007/s00605-007-0479-z
Printed in The Netherlands

Monatshefte für
Mathematik

Construction of pseudorandom binary lattices by using the multiplicative inverse

By

Christian Mauduit[1] and **András Sárközy**[2]

[1] CNRS, Marseille, France
[2] Eötvös Loránd University, Budapest, Hungary

Communicated by J. Schoißengeier

Dedicated to the memory of Walter Philipp

Received November 23, 2006; accepted in revised form March 27, 2007
Published online June 11, 2007 © Springer-Verlag 2007

Abstract. In an earlier work Hubert and the authors of this paper introduced and studied the notion of pseudorandomness of binary lattices. Later in another paper the authors gave a construction for a large family of "good" binary lattices by using the quadratic characters of finite fields. Here, a further large family of "good" binary lattices is constructed by using finite fields and the notion of multiplicative inverse.

2000 Mathematics Subject Classification: 11K45
Key words: Pseudorandom, binary lattice, finite fields, multiplicative inverse

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 [7] they introduced the measures of pseudorandomness, and they showed that the Legendre symbol sequence $\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \dots, \left(\frac{p-1}{p}\right)$ 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 measures introduced) were also given. In terms of computational time and bounds for the pseudorandom measures, one of the best constructions is, perhaps, the one in [8]. This construction is based on the use of the multiplicative inverse modulo p:

Assume that p is a prime number, $k, \ell \in \mathbb{N}$, $2 \leqslant \ell \leqslant p$,

$$k\ell < \frac{p}{2},$$

and $f(x) \in \mathbb{F}_p[x]$ is of the form

$$f(x) = (x + a_1)(x + a_2) \cdots (x + a_k)$$

Research partially supported by the Hungarian National Foundation for Scientific Research, Grant Nos. T 043623 and T 049693, and by a CNRS–HAS exchange program.

with $a_1,\dots,a_k\in\mathbb{F}_p$ and $a_i\neq a_j$ for $i\neq j$. For $(a,p)=1$, denote the multiplicative inverse of a by a^{-1}:

$$aa^{-1}\equiv 1 \pmod{p}.$$

For $a\in\mathbb{Z}$, denote the least non-negative residue of a modulo p by $r_p(a)$:

$$a\equiv r_p(a) \pmod{p}, \quad 0\leqslant r_p(a)<p.$$

Define the binary sequence $E_p=(e_1,\dots,e_p)\in\{-1,+1\}^p$ by

$$e_n=\begin{cases}+1 & \text{if } (f(n),p)=1,\ r_p(f(n)^{-1})<\frac{p}{2}\\ -1 & \text{if either } (f(n),p)=1,\ r_p(f(n)^{-1})>\frac{p}{2} \text{ or } p|f(n).\end{cases} \tag{1.1}$$

It was proved in [8] (see Theorems 1 and 3) that this sequence E_p has strong pseudorandom properties. (See also [1], [3], [5], [6], [10], [11] and the references in these papers for other results on the connection of the multiplicative inverse and pseudorandomness.)

In [4], 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 all whose coordinates are selected from the set $\{0,1,\dots,N-1\}$:

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

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

Definition 1. A function of the type

$$\eta(\boldsymbol{x}):I_N^n\to\{-1,+1\} \tag{1.2}$$

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

(Note that in the $n=1$ special case these functions are the binary sequences $E_N\in\{-1,+1\}^N$.) In [3], 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 form (1.2), $k\in\mathbb{N}$, 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

$$Q_k(\eta)=\max_{\boldsymbol{b},\boldsymbol{d}_1,\dots,\boldsymbol{d}_k,\boldsymbol{t}}\left|\sum_{j_1=0}^{t_1}\cdots\sum_{j_n=0}^{t_n}\eta(j_1b_1\boldsymbol{u}_1+\cdots+j_nb_n\boldsymbol{u}_n+\boldsymbol{d}_1)\right.$$
$$\left.\dots\eta(j_1b_1\boldsymbol{u}_1+\cdots+j_nb_n\boldsymbol{u}_n+\boldsymbol{d}_k)\right| \tag{1.3}$$

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 $j_1b_1\boldsymbol{u}_1+\cdots+j_nb_n\boldsymbol{u}_n+\boldsymbol{d}_i$ occurring in the multiple sum above 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 η. In the one-dimensional special case $Q_k(\eta)$ is the "combined PR-measure Q_k of order k" which was also introduced in [7]. This one-dimensional PR measure Q_k is called "combined PR measure" since it combines the "well-distribution measure" (which measures the irregularities of the distribution relative to arithmetic progressions) with the "correlation measure of order k". Similarly, in the multi-dimensional case the PR measure of order k combines the estimate of the irregularities relative to "generalized arithmetic progressions" with the estimate of a quantity of correlation type. Note that if $\mathscr{B}$ denotes the box

$$\mathscr{B} = \{j_1 b_1 \boldsymbol{u}_1 + \cdots + j_n b_n \boldsymbol{u}_n :\ 0 \leqslant j_1 \leqslant t_1, \ldots, 0 \leqslant j_n \leqslant t_n\},$$

then (1.3) can be rewritten in the more compact form

$$Q_k(\eta) = \max_{\mathscr{B}, \boldsymbol{d}_1, \ldots, \boldsymbol{d}_k} \left| \sum_{v \in \mathscr{B}} \eta(\mathbf{v} + \boldsymbol{d}_1) \ldots \eta(\mathbf{v} + \boldsymbol{d}_k) \right|.$$

In [4] 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 [4] we gave an example for a "good" n-dimensional binary lattice (for any n) by using quadratic characters of finite fields.

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 [9] we presented a construction of this type which was based again on the use of quadratic characters of finite fields.

In this paper our goal is to show that by using finite fields and a principle of Davenport and Lewis [2], construction (1.1) based on the use of the multiplicative inverse also can be adapted and extended to obtain a large family of binary lattices with strong PR properties. It will take slightly more work than in [9] that the given construction possesses strong PR properties but this is more than compensated by the fact that the construction here can be generated at least as fast (note that the multiplicative inverse can be computed fast, in polynomial time) and it can be handled at least as well (perhaps, even slightly better) than the one in [9].

2. The construction and the result

Assume that $q = p^n$ is the power of an odd prime, $\ell \in \mathbb{N}$, $a_1, \ldots, a_\ell$ are distinct elements of $\mathbb{F}_q$, and let

$$f(x) = (x + a_1)(x + a_2) \cdots (x + a_\ell) \quad (\in \mathbb{F}_q[x]) \quad (\text{where } a_i \neq a_j \text{ for } i \neq j).$$

Let $v_1, \ldots, v_n$ be linearly independent elements of $\mathbb{F}_q$ over the prime field $\mathbb{F}_p$ (whose elements we identify with the field of the modulo p residue classes, and we write i for the residue class $\equiv i \pmod{p}$). Define the boxes $B_1, B_2, \ldots, B_n$ by

$$B_1 = \left\{ \sum_{i=1}^{n} u_i v_i :\ 0 \leqslant u_1 \leqslant \frac{p-3}{2},\ u_2, \ldots, u_n \in \mathbb{F}_p \right\},$$

$$B_j = \left\{ \sum_{i=1}^{n} u_i v_i : u_1 = \cdots = u_{j-1} = \frac{p-1}{2}, \right.$$

$$\left. 0 \leqslant u_j \leqslant \frac{p-3}{2}, u_{j+1}, \ldots, u_n \in \mathbb{F}_p \right\} \quad \text{for } j = 2, \ldots, n$$

and write

$$B = \bigcup_{j=1}^{n} B_j. \tag{2.1}$$

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

$$\eta(\boldsymbol{x}) = \eta((x_1, \dots, x_n)) = \begin{cases} +1 & \text{if } f(x_1v_1 + \cdots + x_nv_n) \neq 0 \text{ and} \\ & \quad (f(x_1v_1 + \cdots + x_nv_n))^{-1} \in B \\ -1 & \text{otherwise.} \end{cases} \tag{2.2}$$

We remark that the definition of B is made slightly complicated by the fact that we have to balance between two requirements: the structure of B must be symmetric, easy to handle and, on the other hand, its cardinality must approximate $\frac{q}{2}$ well.

We will show that if k is not very large, then $Q_k(\eta)$ is "small" for this binary lattice η:

Theorem. *If $p, q, n, \ell, f(x), B$ and η are defined as above, $k \in \mathbb{N}$,*

$$k, \ell < p, \quad k + \ell \leqslant p + 1 \tag{2.3}$$

and

$$k\ell < \frac{q}{2}, \tag{2.4}$$

then we have

$$Q_k(\eta) < (2^{k+3} + 1)k\ell n^k q^{1/2}(\log p + 2)^{n+k}. \tag{2.5}$$

3. Proof of the Theorem

We will use the following notations: $\{x\}$ denotes the fractional part of x. $\|x\|$ denotes the distance of x from the nearest integer: $\|x\| = \min(\{x\}, 1 - \{x\})$. We write $e^{2\pi i\alpha} = e(\alpha)$. For p, q defined as in Sect. 2, $\mathbb{F}_q$ denotes the finite field of order q, and we write $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. We denote by ψ_0 the trivial, by ψ_1 the canonical additive character of $\mathbb{F}_q$, and for $h \in \mathbb{F}_q$ we define the additive character ψ_h of $\mathbb{F}_q$ by $\psi_h(n) = \psi_1(hn)$. $v_1, v_2, \dots, v_n$ are linearly independent elements of $\mathbb{F}_q$ over $\mathbb{F}_p$.

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 (1.3):

$$\begin{aligned} &\eta(j_1b_1\boldsymbol{u}_1 + \cdots + j_nb_n\boldsymbol{u}_n + \boldsymbol{d}_1) \dots \eta(j_1b_1\boldsymbol{u}_1 + \cdots + j_nb_n\boldsymbol{u}_n + \boldsymbol{d}_k) \\ &\quad = \eta((j_1b_1 + d_1^{(1)}, \dots, j_nb_n + d_n^{(1)})) \dots \eta((j_1b_1 + d_1^{(k)}, \dots, j_nb_n + d_n^{(k)})). \end{aligned} \tag{3.1}$$

Now write

$$z = j_1(b_1v_1) + \cdots + j_n(b_nv_n)$$

so that z belongs to the box

$$B' = \left\{ \sum_{i=1}^{n} j_i(b_iv_i) : \ 0 \leqslant j_i \leqslant t_i \quad \text{for } i = 1, \dots, n \right\},$$

and set

$$z_i = d_1^{(i)} v_1 + \cdots + d_n^{(i)} v_n \quad (\text{for } i = 1, \dots, k).$$

Then by (2.2), the i-th factor in the product (3.1) is

$$\eta((j_1 b_1 + d_1^{(i)}, \dots, j_n b_n + d_n^{(i)})) \\ = \begin{cases} +1 & \text{if } f(z+z_i) \neq 0 \text{ and } (f(z+z_i))^{-1} \in B \\ -1 & \text{otherwise} \end{cases} \qquad (\text{for } i = 1, \dots, k).$$

Clearly, for all $c \in \mathbb{F}_q$ we have

$$2\left(\frac{1}{q}\sum_{b\,\in\,B}\sum_{h\,\in\,\mathbb{F}_q} \psi_1(h(c-b)) - \frac{1}{2}\right) = \begin{cases} +1 & \text{if } c \in B \\ -1 & \text{if } c \notin B \end{cases}$$

whence, for $f(z+z_i) \neq 0$,

$$2\left(\frac{1}{q}\sum_{b\,\in\,B}\sum_{h\,\in\,\mathbb{F}_q} \psi_1(h((f(z+z_i))^{-1} - b)) - \frac{1}{2}\right) = \begin{cases} +1 & \text{if } (f(z+z_i))^{-1} \in B \\ -1 & \text{if } (f(z+z_i))^{-1} \notin B. \end{cases}$$

It follows that the n-fold sum in (1.3) can be estimated in the following way:

$$\begin{aligned} &\Bigg| \sum_{j_1=0}^{t_1} \cdots \sum_{j_n=0}^{t_n} \eta(j_1 b_1 \boldsymbol{u}_1 + \cdots + j_n b_n \boldsymbol{u}_n + \boldsymbol{d}_1) \cdots \eta(j_1 b_1 \boldsymbol{u}_1 + \cdots + j_n b_n \boldsymbol{u}_n + \boldsymbol{d}_k) \\ &\quad - \sum_{\substack{z\,\in\,B' \\ f(z+z_1)\dots f(z+z_k) \neq 0}} 2^k \prod_{i=1}^{k} \left(\frac{1}{q}\sum_{b\,\in\,B}\sum_{h\,\in\,\mathbb{F}_q} \psi_1(h((f(z+z_i))^{-1} - b)) - \frac{1}{2}\right)\Bigg| \\ &\quad \leqslant \sum_{\substack{z\,\in\,\mathbb{F}_q \\ f(z+z_1)\dots f(z+z_k) = 0}} 1 \leqslant k\ell. \end{aligned} \tag{3.2}$$

Separating the $h = 0$ term in the general factor of the product we get

$$\begin{aligned} &\frac{1}{q}\sum_{b\,\in\,B}\sum_{h\,\in\,\mathbb{F}_q} \psi_1(h((f(z+z_i))^{-1} - b)) - \frac{1}{2} \\ &\quad = \left(\frac{1}{q}\sum_{b\,\in\,B} 1 - \frac{1}{2}\right) + \frac{1}{q}\sum_{b\,\in\,B}\sum_{h\,\in\,\mathbb{F}_q^*} \psi_1(h((f(z+z_i))^{-1} - b)). \end{aligned}$$

Here we have

$$\begin{aligned} \frac{1}{q}\sum_{b\,\in\,B} 1 - \frac{1}{2} &= \frac{1}{q}\sum_{j=1}^{n} |B_j| - \frac{1}{2} = \frac{1}{q}\sum_{j=1}^{n} \frac{p-1}{2} \cdot p^{n-j} - \frac{1}{2} \\ &= \frac{1}{q}\frac{p-1}{2}\frac{p^n-1}{p-1} - \frac{1}{2} = \frac{q-1}{2q} - \frac{1}{2} = -\frac{1}{2q} \end{aligned}$$

so that on the left of (3.2) we have

$$\begin{aligned}
&\Bigg| \sum_{\substack{z\,\in\, B'\\ f(z+z_1)\ldots f(z+z_k)\neq 0}} 2^k \prod_{i=1}^{k} \left(\frac{1}{q} \sum_{b\,\in\, B} \sum_{h\,\in\, \mathbb{F}_q} \psi_1(h((f(z+z_i))^{-1}-b)) - \frac{1}{2} \right) \Bigg| \\
&= \Bigg| \sum_{\substack{z\,\in\, B'\\ f(z+z_1)\ldots f(z+z_k)\neq 0}} 2^k \prod_{i=1}^{k} \left(\frac{1}{q} \sum_{b\,\in\, B} \sum_{h\,\in\, \mathbb{F}_q^*} \psi_1(h((f(z+z_i))^{-1}-b)) - \frac{1}{2q} \right) \Bigg| \\
&= \frac{1}{q^k} \Bigg| \sum_{\substack{z\,\in\, B'\\ f(z+z_1)\ldots f(z+z_k)\neq 0}} \Bigg((-1)^k + \sum_{j=1}^{k} (-1)^{k-j} 2^j \sum_{(b_1,\ldots,b_j)\,\in\, B^j} \; \sum_{(h_1,\ldots,h_j)\,\in\, (\mathbb{F}_q^*)^j} \\
&\qquad \times \sum_{1\,\leqslant\, i_1 < \cdots < i_j \,\leqslant\, k} \psi_1(h_1((f(z+z_{i_1}))^{-1}-b_1) + \cdots + h_j((f(z+z_{i_j}))^{-1}-b_j)) \Bigg) \Bigg| \\
&\leqslant 1 + \frac{1}{q^k} \sum_{j=1}^{k} 2^j \sum_{(h_1,\ldots,h_j)\,\in\, (\mathbb{F}_q^*)^j} \; \sum_{1\,\leqslant\, i_1 < \cdots < i_j \,\leqslant\, k} \\
&\qquad \times \Bigg| \sum_{\substack{z\,\in\, B'\\ f(z+z_1)\ldots f(z+z_k)\neq 0}} \psi_1(h_1(f(z+z_{i_1}))^{-1} + \cdots + h_j(f(z+z_{i_j}))^{-1}) \Bigg| \\
&\qquad \times \Bigg| \sum_{(b_1,\ldots,b_j)\,\in\, B^j} \psi_1(-h_1 b_1 - \cdots - h_j b_j) \Bigg|. \qquad (3.3)
\end{aligned}$$

Consider the penultimate sum. Clearly,

$$\begin{aligned}
&\Bigg| \sum_{\substack{z\,\in\, B'\\ f(z+z_1)\ldots f(z+z_k)\neq 0}} \psi_1(h_1(f(z+z_{i_1}))^{-1} + \cdots + h_j(f(z+z_{i_j}))^{-1}) \Bigg| \\
&\qquad \leqslant \Bigg| \sum_{\substack{z\,\in\, B'\\ f(z+z_{i_1})\ldots f(z+z_{i_j})\neq 0}} \psi_1(h_1(f(z+z_{i_1}))^{-1} + \cdots + h_j(f(z+z_{i_j}))^{-1}) \Bigg| + k\ell. \qquad (3.4)
\end{aligned}$$

To be able to estimate this sum, we will need

Lemma 1. *Assume that $q = p^n$ is a prime power, $j \in \mathbb{N}$, $\ell \in \mathbb{N}$,*

$$j, \ell < p, \quad j + \ell \leqslant p + 1, \tag{3.5}$$

$$j\ell < \frac{q}{2}, \tag{3.6}$$

$a_1, \ldots, a_\ell$ are distinct elements of $\mathbb{F}_q$, $h_1, \ldots, h_j$ are distinct nonzero elements of $\mathbb{F}_q$, and $m_1, \ldots, m_j$ are distinct elements of $\mathbb{F}_q$. Write $f(x) = \prod_{i=1}^{\ell}(x + a_i)$ $(\in \mathbb{F}_q[x])$, and define $Q(x)$, $R(x) \in \mathbb{F}_q[x]$ by

$$Q(x) = \sum_{i=1}^{j} h_i \prod_{\substack{1\,\leqslant\, t \,\leqslant\, j\\ t\neq i}} f(x + m_t),$$

$$R(x) = \prod_{t=1}^{j} f(x + m_t)$$

so that

$$\sum_{i=1}^{j} h_i(f(x+m_i))^{-1} = \frac{Q(x)}{R(x)} \textit{ for every } x \in \mathbb{F}_q \textit{ with } f(x+m_i) \neq 0 \textit{ for } 1 \leqslant i \leqslant j.$$

Then, $Q(x)$ is not the 0 polynomial.

Proof of Lemma 1. If $\frac{u(x)}{v(x)}$ is a rational function over $\mathbb{F}_q$ such that

$$\deg u(x) < \deg v(x)$$

and $v(x)$ is of the form

$$v(x) = (x + a_1) \cdots (x + a_\lambda)$$

with $a_i \in \mathbb{F}_q$,

$$a_i \neq a_j \quad \text{for } 1 \leqslant i < j \leqslant \lambda$$

and

$$1 \leqslant \lambda = \deg v(x) < \frac{q}{2}, \tag{3.7}$$

then $\frac{u(x)}{v(x)}$ has a *unique* partial fraction decomposition of the form

$$\frac{u(x)}{v(x)} = \frac{A_1}{x + a_1} + \cdots + \frac{A_\lambda}{x + a_\lambda} \text{ over } \mathbb{F}_q.$$

Again let $v_1, \ldots, v_n$ denote a basis for the linear vector space $\mathbb{F}_q$ over $\mathbb{F}_p$, and now we take $v_1 = 1$ (which can be done without loss of generality). Then this decomposition can be rewritten as

$$\frac{u(x)}{v(x)} = \sum_{(x_1,\ldots,x_n) \in \{0,\ldots,p-1\}^n} \frac{A_{x_1,\ldots,x_n}}{x + x_1 v_1 + \cdots + x_n v_n} \tag{3.8}$$

where the coefficients $A_{x_1,\ldots,x_n} = A_{x_1,\ldots,x_n}\left(\frac{u(x)}{v(x)}\right)$ with $(x_1, \ldots, x_n) \in \{0, \ldots, p-1\}^n$ are also unique. For such a rational function $\frac{u(x)}{v(x)}$, we define the polynomial P of n variables over $\mathbb{F}_q$ by

$$P\left(\frac{u(x)}{v(x)}; y_1, \ldots, y_n\right) = \sum_{(x_1,\ldots,x_n) \in \{0,\ldots,p-1\}^n} A_{x_1,\ldots,x_n} y_1^{x_1} \ldots y_n^{x_n}.$$

Since $f(x) = \prod_{i=1}^{\ell}(x + a_i)$ with $a_1, \ldots, a_\ell \in \mathbb{F}_p$, thus we have $A_{x_1,\ldots,x_n} = 0$ for $(x_2, \ldots, x_n) \neq (0, \ldots, 0)$ so that $P\left(\frac{1}{f(x)}; y_1, \ldots, y_n\right) \in \mathbb{F}_q[y_1]$. We write

$$P^*(y_1) = P\left(\frac{1}{f(x)}; y_1, \ldots, y_n\right) = \sum_{i=0}^{p-1} \alpha_i y_1^i.$$

We will prove by contradiction: assume that contrary to the conclusion of the lemma $Q(x)$ is the zero polynomial. Then it follows that

$$P\left(\frac{Q(x)}{R(x)};y_1,\dots,y_n\right)=P\left(\sum_{i=1}^{j}\frac{h_i}{f(x+m_i)};y_1,\dots,y_n\right)$$

is the zero polynomial; note that now (3.7) holds with this $R(x)$ in place of $v(x)$ by (3.6) thus the partial fraction decomposition is unique.

On the other hand, if we write $m_i=\mu_1^{(i)}v_1+\dots+\mu_n^{(i)}v_n$ for $i=1,\dots,j$, then we have

$$\begin{aligned}
P&\left(\frac{1}{f(x+m_i)};y_1,\dots,y_n\right)=P\left(\sum_{j=0}^{p-1}\frac{\alpha_j}{x+m_i+j};y_1,\dots,y_n\right)\\
&=P\left(\sum_{j=0}^{p-1}\frac{\alpha_j}{x+(\mu_1^{(i)}+j)v_1+\mu_2^{(i)}v_2+\dots+\mu_n^{(i)}v_n};y_1,\dots,y_n\right)\\
&=P\left(\sum_{j=0}^{p-1-\mu_1^{(i)}}\frac{\alpha_j}{x+(\mu_1^{(i)}+j)v_1+\mu_2^{(i)}v_2+\dots+\mu_n^{(i)}v_n}\right.\\
&\qquad\left.+\sum_{j=p-\mu_1^{(i)}}^{p-1}\frac{\alpha_j}{x+(\mu_1^{(i)}-p+j)v_1+\mu_2^{(i)}v_2+\dots+\mu_n^{(i)}v_n};y_1,\dots,y_n\right)\\
&=\sum_{j=0}^{p-1-\mu_1^{(i)}}\alpha_j y_1^{\mu_1^{(i)}+j}y_2^{\mu_2^{(i)}}\cdots y_n^{\mu_n^{(i)}}+\sum_{j=p-\mu_1^{(i)}}^{p-1}\alpha_j y_1^{\mu_1^{(i)}-p+j}y_2^{\mu_2^{(i)}}\cdots y_n^{\mu_n^{(i)}}\\
&=\left(y_1^{\mu_1^{(i)}}\left(\sum_{j=0}^{p-1-\mu_1^{(i)}}\alpha_j y_1^j\right)+\sum_{j=p-\mu_1^{(i)}}^{p-1}\alpha_j y_1^{\mu_1^{(i)}-p+j}\right)y_2^{\mu_2^{(i)}}\cdots y_n^{\mu_n^{(i)}}\\
&=\left(\left(y_1^{\mu_1^{(i)}}P^*(y_1)-\left(\alpha_{p-\mu_1^{(i)}}y_1^p+\alpha_{p-\mu_1^{(i)}+1}y_1^{p+1}+\dots+\alpha_{p-1}y_1^{p+\mu_1^{(i)}-1}\right)\right)\right.\\
&\qquad\left.+\left(\alpha_{p-\mu_1^{(i)}}+\alpha_{p-\mu_1^{(i)}+1}y_1+\dots+\alpha_{p-1}y_1^{\mu_1^{(i)}-1}\right)\right)y_2^{\mu_2^{(i)}}\cdots y_n^{\mu_n^{(i)}}\\
&=\left(y_1^{\mu_1^{(i)}}P^*(y_1)+\left(\alpha_{p-\mu_1^{(i)}}+\alpha_{p-\mu_1^{(i)}+1}y_1+\dots+\alpha_{p-1}y_1^{\mu_1^{(i)}-1}\right)(1-y_1^p)\right)\\
&\qquad\times y_2^{\mu_2^{(i)}}\cdots y_n^{\mu_n^{(i)}}
\end{aligned}$$

so that

$$\begin{aligned}
0&=P\left(\sum_{i=1}^{j}\frac{h_i}{f(x+m_i)};y_1,\dots,y_n\right)\\
&=\sum_{i=1}^{j}h_i\left(y_1^{\mu_1^{(i)}}P^*(y_1)+\left(\alpha_{p-\mu_1^{(i)}}+\dots+\alpha_{p-1}y_1^{\mu_1^{(i)}-1}\right)(1-y_1^p)\right)y_2^{\mu_2^{(i)}}\dots y_n^{\mu_n^{(i)}}.
\end{aligned}$$

Substituting $y_2 = \cdots = y_n = 1$ and writing

$$H(y_1) = \sum_{i=1}^{j} h_i y_1^{\mu_1^{(i)}},$$

we obtain

$$0 = H(y_1)P^*(y_1) - (y_1^p - 1)\sum_{i=1}^{j} h_i\left(\alpha_{p-\mu_1^{(i)}} + \cdots + \alpha_{p-1}y_1^{\mu_1^{(i)}-1}\right).$$

It follows that

$$(y_1^p - 1)|H(y_1)P^*(y_1) \quad (\text{in } \mathbb{F}_q[y_1]). \tag{3.9}$$

If $g(y_1) \in \mathbb{F}_q[y_1]$ is not the zero polynomial, let $\mathscr{J}(g(y_1))$ denote the greatest nonnegative integer $\mathscr{J}$ such that $(y_1 - 1)^{\mathscr{J}}$ divides $g(y_1)$ in $\mathbb{F}_q[y_1]$. We have

$$(y_1 - 1)^p = y_1^p - 1$$

in $\mathbb{F}_q[y_1]$ (since the characteristic of $\mathbb{F}_q$ is p), thus it follows from (3.9) that

$$\mathscr{J}(H(y_1)P^*(y_1)) \geqslant p. \tag{3.10}$$

Now we will show that it suffices to prove

Lemma 2. *Assume that $t \in \mathbb{N}$ and $L(x) \in \mathbb{F}_q[x]$ is a nonzero polynomial of the form*

$$L(x) = \lambda_1 x^{n_1} + \cdots + \lambda_t x^{n_t} \text{ with } 0 \leqslant n_1 < n_2 < \cdots < n_t \leqslant p - 1. \tag{3.11}$$

Then we have $\mathscr{J}(L(x)) \leqslant t - 1$.

Indeed, assume that Lemma 2 has been proved. The polynomials $H(y_1)$ and $P^*(y_1)$ are polynomials of form (3.11) with j, resp. ℓ in place of t, so that we have $\mathscr{J}(H(y_1)) \leqslant j - 1$ and $\mathscr{J}(P^*(y_1)) \leqslant \ell - 1$. It follows that

$$\mathscr{J}(H(y_1)P^*(y_1)) \leqslant \mathscr{J}(H(y_1)) + \mathscr{J}(P^*(y_1)) \leqslant j + \ell - 2$$

which contradicts (3.5) and (3.10) and this completes the proof of Lemma 1.

It remains to prove Lemma 2.

Proof of Lemma 2. Lemma 2 was proved in the special case $q = p$ in [8]; see Lemma 7 there. Since the polynomials involved in Lemma 2 here have degree $< p$, thus it is easy to check that the proof of Lemma 7 in [8] goes through if we replace $\mathbb{F}_p$ by $\mathbb{F}_q$ and $\mathbb{F}_p[x]$ by $\mathbb{F}_q[x]$; we leave the details to the reader.

We will need a result of Eichenauer-Herrmann and Niederreiter [3]:

Lemma 3. *Assume that $q = p^n$ is a prime power, and let $\frac{Q(x)}{R(x)}$ be a rational function over $\mathbb{F}_q$ which is not of the form $(A(x))^p - A(x)$ with a rational function $A(x)$ over $\mathbb{F}_q$. If ψ is a nontrivial additive character of $\mathbb{F}_q$, then*

$$\left|\sum_{\substack{n \in \mathbb{F}_q \\ R(n) \neq 0}} \psi\left(\frac{Q(n)}{R(n)}\right)\right| < (2\max(\deg Q, \deg R) - 1)q^{1/2} + 1.$$

Proof of Lemma 3. This is a trivial consequence of Lemma 1 in [3] (indeed, our Lemma 3 is a slightly weaker form of Lemma 1 of Eichenauer-Herrmann and Niederreiter).

We will use the incomplete version of this result:

Lemma 4. *Assume that $q = p^n$ is a prime power, $\frac{Q(x)}{R(x)}$ is a nonzero rational function over $\mathbb{F}_q$ such that*

$$\deg Q < \deg R \tag{3.12}$$

and there is no polynomial $L(x) \in \mathbb{F}_q[x]$ with $(L(x))^p | R(x)$ and $\deg L(x) > 0$, ψ is a nontrivial additive character of $\mathbb{F}_q$, and $\overline{B}$ is a box of form

$$\overline{B} = \left\{ \sum_{i=1}^{n} j_i v_i : \ 0 \leqslant j_i \leqslant t_i \quad \text{for } i = 1, 2, \dots, n \right\}$$

(*where $v_1, \dots, v_n$ are linearly independent over the prime field of $\mathbb{F}_q$*). *Then we have*

$$\left| \sum_{\substack{z \in \overline{B} \\ R(z) \neq 0}} \psi\left(\frac{Q(z)}{R(z)} \right) \right| < 3(\deg R + 1) q^{1/2} (2 + \log p)^n.$$

Proof of Lemma 4. This can be derived from Lemma 3 in the same way as Theorem 2 is derived from Lemma 1 in [3] in the special case $n = 1$. Indeed, by $\psi \neq \psi_0$ for any $m, b \in \mathbb{F}_q$ we have

$$\frac{1}{q} \sum_{h \in \mathbb{F}_q} \psi(h(m - b)) = \begin{cases} 1 & \text{if } m = b, \\ 0 & \text{if } m \neq b, \end{cases}$$

and thus

$$\begin{aligned}
\left| \sum_{\substack{z \in \overline{B} \\ R(z) \neq 0}} \psi\left(\frac{Q(z)}{R(z)} \right) \right| &= \left| \sum_{\substack{m \in \mathbb{F}_q \\ R(m) \neq 0}} \psi\left(\frac{Q(m)}{R(m)} \right) \sum_{b \in \overline{B}} \frac{1}{q} \sum_{h \in \mathbb{F}_q} \psi(h(m - b)) \right| \\
&\leqslant \frac{1}{q} \sum_{h \in \mathbb{F}_q} \left| \sum_{\substack{m \in \mathbb{F}_q \\ R(m) \neq 0}} \psi\left(\frac{Q(m) + hmR(m)}{R(m)} \right) \right| \left| \sum_{b \in \overline{B}} \psi(hb) \right| \\
&= \frac{|\overline{B}|}{q} \left| \sum_{\substack{m \in \mathbb{F}_q \\ R(m) \neq 0}} \psi\left(\frac{Q(m)}{R(m)} \right) \right| \\
&\quad + \frac{1}{q} \sum_{h \in \mathbb{F}_q^*} \left| \sum_{\substack{m \in \mathbb{F}_q \\ R(m) \neq 0}} \psi\left(\frac{Q(m) + hmR(m)}{R(m)} \right) \right| \left| \sum_{b \in \overline{B}} \psi(hb) \right|.
\end{aligned} \tag{3.13}$$

Write $Q_h(m) = Q(m) + hmR(m)$. If $h \neq 0$, then by (3.12), $\deg hmR(m) > \deg Q(m)$, thus Q_h is not the zero polynomial:

$$Q_h(m) \neq 0. \tag{3.14}$$

If $h=0$, then

$$Q_0(m)=Q(m)\neq 0$$

by the assumptions of the lemma, so (3.14) holds for every h.

Now we want to use Lemma 3 with $Q_h(m)$ in place of $Q(m)$. In order to ensure the applicability of the lemma we have to show that $\frac{Q_h}{R}$ is not of the form A^p-A. We will prove this by contradiction: assume that there are polynomials $K,L\in\mathbb{F}_q[x]$ with

$$(K,L)=1 \tag{3.15}$$

and

$$\frac{Q_h}{R}=\left(\frac{K}{L}\right)^p-\frac{K}{L} \tag{3.16}$$

hence

$$Q_hL^p=RK(K^{p-1}-L^{p-1}). \tag{3.17}$$

By (3.12), (3.14) and (3.15) it follows from (3.17) that $\deg L>0$ and $L^p|R$ which contradicts our assumption on R. Thus, indeed, Lemma 2 can be applied, and by (3.12) we obtain that

$$\begin{aligned}\left|\sum_{\substack{n\in\mathbb{F}_q\\ R(n)\neq 0}}\psi\left(\frac{Q_h(m)}{R(m)}\right)\right| &< (2\max(\deg Q_h,\deg R)-1)q^{1/2}+1\\ &\leqslant (2\deg R+1)q^{1/2}+1\\ &< 2(\deg R+1)q^{1/2}\quad\text{for all } h\in\mathbb{F}_q. \end{aligned}\tag{3.18}$$

Thus it follows from (3.13) that

$$\begin{aligned}\left|\sum_{\substack{z\in\overline{B}\\ R(z)\neq 0}}\psi\left(\frac{Q(z)}{R(z)}\right)\right| &\leqslant 2(\deg R+1)q^{1/2}\left(\frac{|\overline{B}|}{q}+\frac{l}{q}\sum_{h\in\mathbb{F}_q^*}\left|\sum_{b\in\overline{B}}\psi(hb)\right|\right)\\ &\leqslant 2(\deg R+1)q^{1/2}\left(1+\frac{l}{q}\sum_{h\in\mathbb{F}_q}\left|\sum_{b\in\overline{B}}\psi(hb)\right|\right)\end{aligned}\tag{3.19}$$

since we have $\overline{B}\subseteq\mathbb{F}_q$ whence $|\overline{B}|\leqslant|\mathbb{F}_q|=q$. If we write $\psi(hm)=\psi_h^*(m)$, then as h runs over the elements of $\mathbb{F}_q$, ψ_h^* runs over the additive characters of $\mathbb{F}_q$. Thus using the definition of $\overline{B}$ the last double sum in (3.19) can be rewritten as

$$\begin{aligned}\sum_{h\in\mathbb{F}_q}\left|\sum_{b\in\overline{B}}\psi(hb)\right| &= \sum_{\psi_h^*}\left|\sum_{j_1=0}^{t_1}\cdots\sum_{j_n=0}^{t_n}\psi_h^*(j_1v_1+\cdots+j_nv_n)\right|\\ &= \sum_{\psi_h^*}\left|\prod_{r=1}^{n}\sum_{j_r=0}^{t_r}\psi_h^*(j_rv_r)\right| = \sum_{\psi_h^*}\prod_{r=1}^{n}\left|\sum_{j_r=0}^{t_r}(\psi_h^*(v_r))^{j_r}\right|.\end{aligned}\tag{3.20}$$

For every $h \in \mathbb{F}_q$ and $1 \leqslant r \leqslant n$, $\psi_h^*(v_r)$ is a p-th root of unity, say, $\psi_h^*(v_r) = e(\frac{s}{p})$ with $0 \leqslant s < p$. If $s = 0$, then we have

$$\left|\sum_{j_r=0}^{t_r} (\psi_h^*(v_r))^{j_r}\right| = \left|\sum_{j_r=0}^{t_r} 1\right| = t_r + 1 \leqslant p \quad (\text{for } s = 0),$$

while for $0 < s < p$,

$$\left|\sum_{j_r=0}^{t_r} (\psi_h^*(v_r))^{j_r}\right| = \left|\sum_{j_r=0}^{t_r} e\left(j_r \frac{s}{p}\right)\right| \leqslant \frac{2}{\left|1 - e\left(\frac{s}{p}\right)\right|} \leqslant \frac{1}{2\|\frac{s}{p}\|} \quad (\text{for } 0 < s < p).$$

Moreover, as ψ_h^* runs over the additive characters of $\mathbb{F}_q$, the n-tuple $(\psi_h^*(v_1), \dots, \psi_h^*(v_n))$ runs over the n-tuples $\left(e\left(\frac{s_1}{p}\right), \dots, e\left(\frac{s_n}{p}\right)\right)$ of the p-th roots of unity, each of the latter n-tuples is assumed exactly once. It follows from these considerations that the double sum in (3.20) is

$$\sum_{h \in \mathbb{F}_q} \left|\sum_{b \in \overline{B}} \psi(hb)\right| \leqslant \left(p + \sum_{s=1}^{p-1} \frac{1}{2\|\frac{s}{p}\|}\right)^n$$

$$= \left(p + \sum_{s=1}^{\frac{p-1}{2}} \frac{p}{s}\right)^n < p^n(2 + \log p)^n = q(2 + \log p)^n. \quad (3.21)$$

It follows from (3.19) and (3.21) that

$$\left|\sum_{\substack{z \in \overline{B} \\ R(z) \neq 0}} \psi\left(\frac{Q(z)}{R(z)}\right)\right| \leqslant 2(\deg R + 1)q^{1/2}(1 + (2 + \log p)^n)$$

$$< 3(\deg R + 1)q^{1/2}(2 + \log p)^n$$

which completes the proof of Lemma 4.

By Lemma 1 and the assumptions of our theorem, the numerator of the rational function in the general term in the last sum in (3.4) is nonzero, thus we may use Lemma 4 to estimate this sum provided that the rational function

$$\frac{Q(z)}{R(z)} = \sum_{r=1}^{j} h_r (f(z + z_{i_r}))^{-1}$$

is such that

$$\deg Q < \deg R \quad (3.22)$$

and

$$\text{there is no } L(x) \in \mathbb{F}_q(x) \text{ with } \deg L > 0 \text{ and } L^p | R. \quad (3.23)$$

(3.22) is trivial, while (3.23) follows from the facts that

$$R(z) = \prod_{r=1}^{j} f(z + z_{i_r}),$$

and the zeros of $f(z)$ are distinct elements of $\mathbb{F}_q$, thus the multiplicity of every zero of $R(z)$ is at most $j \leqslant k$ which is less than p by (2.3). Thus, indeed, we may use Lemma 4 and we obtain that the sum in (3.4) is

$$\begin{aligned}\Bigg| \sum_{\substack{z \in B' \\ f(z+z_1)\ldots f(z+z_k) \neq 0}} & \psi_1(h_1(f(z+z_{i_1}))^{-1} + \cdots + h_j(f(z+z_{i_j}))^{-1})\Bigg| \\ & < 3(\deg R + 1)q^{1/2}(2 + \log p)^n + k\ell \\ & \leqslant 3(j\ell + 1)q^{1/2}(2 + \log p)^n + k\ell \\ & \leqslant 7k\ell q^{1/2}(2 + \log p)^n. \qquad (3.24)\end{aligned}$$

It follows from (3.3) and (3.24) that

$$\begin{aligned}\Bigg| \sum_{\substack{z \in B' \\ f(z+z_1)\ldots f(z+z_k) \neq 0}} & 2^k \prod_{i=1}^{k} \left(\frac{1}{q} \sum_{b \in B} \sum_{h \in \mathbb{F}_q} \psi_1(h((f(z+z_i))^{-1} - b)) - \frac{1}{2} \right) \Bigg| \\ & \leqslant 1 + \frac{1}{q^k} \sum_{j=1}^{k} 2^j \binom{k}{j} 7k\ell q^{1/2} (2 + \log p)^n \left(\sum_{h \in \mathbb{F}_q^*} \Bigg| \sum_{b \in B} \psi_1(hb) \Bigg| \right)^j. \qquad (3.25)\end{aligned}$$

Here we have

$$\begin{aligned}\sum_{h \in \mathbb{F}_q^*} \Bigg| \sum_{b \in B} \psi_1(hb) \Bigg| &= \sum_{\psi \neq \psi_0} \Bigg| \sum_{b \in B} \psi(b) \Bigg| \\ &= \sum_{\psi \neq \psi_0} \Bigg| \sum_{i=1}^{n} \sum_{b \in B_i} \psi(b) \Bigg| \leqslant \sum_{\psi \neq \psi_0} \sum_{i=1}^{n} \Bigg| \sum_{b \in B_i} \psi(b) \Bigg|. \qquad (3.26)\end{aligned}$$

For $i = 1, 2, \ldots, n$ we have

$$\sum_{\psi \neq \psi_0} \Bigg| \sum_{b \in B_i} \psi(b) \Bigg| = \sum_{\psi \neq \psi_0} \Bigg| \sum_{u_i=0}^{\frac{p-3}{2}} (\psi(v_i))^{u_i} \Bigg| \prod_{t=i+1}^{n} \Bigg| \sum_{u_t=0}^{p-1} (\psi(v_t))^{u_t} \Bigg|. \qquad (3.27)$$

If $\psi(v_t) \neq 1$ for some $i + 1 \leqslant t \leqslant n$, then we have

$$\sum_{u_t=0}^{p-1} (\psi(v_t))^{u_t} = 0,$$

so that the contribution of these terms is 0. Thus we may restrict ourselves to the characters ψ with

$$\psi(v_{i+1}) = \cdots = \psi(v_n) = 1,$$

when each of the innermost sums in (3.27) is p. In the penultimate sum in (3.27) we have

$$\psi(v_i) = e\left(\frac{k}{p}\right) \quad \text{with some } k \in \{0, 1, \ldots, p-1\}; \qquad (3.28)$$

if $k=0$, then the sum is

$$\sum_{u_i=0}^{\frac{p-3}{2}} (\psi(v_i))^{u_i} = \frac{p-1}{2} \quad (\text{for } k=0),$$

while for $1 \leqslant k \leqslant p-1$ we have

$$\left| \sum_{u_i=0}^{\frac{p-3}{2}} (\psi(v_i))^{u_i} \right| \leqslant \frac{2}{|1-\psi(v_i)|} = \frac{2}{|1-e(k/p)|} \leqslant \frac{2}{4\|k/p\|} = \frac{1}{2\|k/p\|}.$$

If $\psi(v_i), \dots, \psi(v_t)$ are fixed, then the values of the $i-1$ p-th roots of unity $\psi(v_1), \dots, \psi(v_{i-1})$ can be chosen in atmost p^{i-1} ways (in exactly p^{i-1} ways if $k \neq 0$ in (3.28) but only $p^{i-1}-1$ ways if $k=0$ since now ψ_0 is excluded). It follows that the double sum in (3.27) is

$$\begin{aligned}\sum_{\psi \neq \psi_0} \left| \sum_{b \in B_i} \psi(b) \right| &\leqslant p^{i-1} \left(\frac{p-1}{2} + \sum_{k=1}^{p-1} \frac{1}{2\|k/p\|} \right) p^{n-i} \\ &= p^{n-1} \left(\frac{p-1}{2} + \sum_{k=1}^{\frac{p-1}{2}} \frac{p}{k} \right) < q \left(\log p + \frac{3}{2} \right) \quad (\text{for } i = 1, 2, \dots, n).\end{aligned} \tag{3.29}$$

By (3.25), (3.26) and (3.29) the upper bound in (3.3) is

$$\begin{aligned}&< 1 + \frac{1}{q^k} \sum_{j=1}^{k} 2^j \binom{k}{j} 7k\ell q^{1/2} (2 + \log p)^n \left(nq \left(\log p + \frac{3}{2} \right) \right)^j \\ &= 1 + \frac{1}{q^k} 7k\ell q^{1/2} (2 + \log p)^n \sum_{j=1}^{k} \binom{k}{j} \left(2nq \left(\log p + \frac{3}{2} \right) \right)^j \\ &< 1 + \frac{7k\ell}{q^k} q^{1/2} (2 + \log p)^n \left(1 + 2nq \left(\log p + \frac{3}{2} \right) \right)^k \\ &< 1 + 7k\ell q^{1/2} (2 + \log p)^n (2n(\log p + 2))^k \\ &< 2^{k+3} k\ell n^k q^{1/2} (\log p + 2)^{n+k}.\end{aligned} \tag{3.30}$$

(2.5) follows from (1.3), (3.2), (3.3) and (3.30), and this completes the proof of the theorem.

References

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

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

[3] Eichenauer-Herrmann J, Niederreiter H (1994) Bounds for exponential sums and their applications to pseudorandom numbers. Acta Arith **67**: 269–281

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

[5] Kodila DG (2005) Time-analysis of pseudorandom bit generators. Ann Univ Sci Budapest Eötvös **48**: 31–43

[6] Liu H (2007) New pseudorandom sequences constructed by multiplicative inverses. Acta Arith **125**: 11–19

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

[8] Mauduit C, Sárközy A (2005) Construction of pseudorandom binary sequences by using the multiplicative inverse. Acta Math Hungar **108**: 239–252

[9] Mauduit C, Sárközy A (2007) A On large families of pseudorandom binary lattices. Uniform distribution theory **2**: 23–37

[10] Niederreiter H, Shparlinski JE (2000) Exponential sums and the distribution of inverse congruential pseudorandom numbers with prime-power modulus. Acta Arith **92**: 89–98

[11] Niederreiter H, Winterhof A (2005) Exponential sums and the distribution of inversive congruential pseudorandom numbers with power of two modulus. Int J Number Theory **1**: 431–438

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