ACTA ARITHMETICA
174.3 (2016)

On the correlation of families of pseudorandom sequences of k symbols

by

Kit-Ho Mak (Hong Kong) and
Alexandru Zaharescu (Bucureşti and Urbana, IL)

1. Introduction. In a series of papers [5–7, 15–18], Mauduit and Sárközy (partly with coauthors) studied finite pseudorandom binary sequences by a constructive approach. Since then, many constructions of pseudorandom binary sequences have been presented. (See for example [11, 12, 14, 20–22], the survey paper [24] and the references therein.) In some situations one may need to extend the binary sequences to pseudorandom sequences of k symbols. To this end, measures of pseudorandomness for sequences of k symbols were developed in [19]. Some constructions of pseudorandom sequences of k symbols can be found in [2, 3, 8, 13, 28].

For many purposes one needs a *large family* of pseudorandom sequences, and it is desirable that the family has a "rich", "complex" structure, and that sequences in the family are "random" or "independent" in some sense. In the binary case, several measures were developed in this direction. This includes the *f-complexity* (here "f" stands for *family*) introduced by Ahlswede, Khachatrian, Mauduit and Sárközy [1], and the *f-correlation* introduced by Gyarmati [9]. The f-complexity was generalized to sequences of k symbols by Ahlswede, Mauduit and Sárközy [2, 3]. In the same spirit, Tóth [25, 26] studied the collision and avalanche effect of pseudorandom sequences, and Gyarmati, Mauduit and Sárközy [10] examined the cross-correlation measure for families of binary sequences.

The aim of this paper is to generalize the f-correlation of [9] to the k-ary case. In particular, we study the f-correlation of k-ary sequences introduced in [2, 3]. It turns out that most properties in the binary case continue to hold in the k-ary case, but some of them require a different treatment.

2010 *Mathematics Subject Classification*: Primary 11K45; Secondary 11A07.
Key words and phrases: pseudorandom sequences, randomness, correlation, concatenation.
Received 29 August 2013; revised 25 March 2016.
Published online 4 July 2016.

DOI: 10.4064/aa7569-4-2016

Along the way we also improve some previous results on pseudorandom k-ary sequences.

1.1. Pseudorandomness of k-ary sequences. We briefly recall the two sets of (nearly equivalent) measures for pseudorandomness of k-ary sequences defined in [19]. Let $k \geq 2$ be an integer, and let $\mathcal{A} = \{a_1, \dots, a_k\}$ be a set of k symbols. For a sequence $E_N = (e_1, \dots, e_N) \in \mathcal{A}^N$ and a given symbol $a \in \mathcal{A}$, let

$$x(E_N, a, M, u, v) = |\{j : 0 \leq j \leq M-1,\, e_{u+jv} = a\}|,$$

and for $w \in \mathcal{A}^\ell$, $D = (d_1, \dots, d_\ell)$ with nonnegative integers $d_1 < \cdots < d_\ell$, let

$$g(E_N, w, M, D) = |\{n : 1 \leq n \leq M,\, (e_{n+d_1}, \dots, e_{n+d_\ell}) = w\}|.$$

The *well-distribution measure* of E_N is defined by

$$\delta(E_N) = \max_{a,M,u,v} \left| x(E_N, a, M, u, v) - \frac{M}{k} \right|, \tag{1.1}$$

and the *correlation measure of order* ℓ of E_N is

$$\gamma_\ell(E_N) = \max_{w,M,D} \left| g(E_N, w, M, D) - \frac{M}{k^\ell} \right|, \tag{1.2}$$

where in both maxima all indices vary between 1 and N.

The other set of measures resembles the case $k = 2$ more closely using the roots of unity. Let $\mathcal{E}$ be the set of kth roots of unity, and let $\mathcal{F}$ be the set of all bijections $\phi : \mathcal{A} \to \mathcal{E}$. Set

$$X(E_N, \phi, M, u, v) = \sum_{j=0}^{M-1} \phi(e_{u+jv}),$$

and for $\phi = (\phi_1, \dots, \phi_\ell) \in \mathcal{F}^\ell$, $D = (d_1, \dots, d_\ell)$ with non-negative integers $d_1 < \cdots < d_\ell$, set

$$G(E_N, \phi, M, D) = \sum_{n=1}^{M} \phi_1(e_{n+d_1}) \dots \phi_\ell(e_{n+d_\ell}).$$

Then the *$\mathcal{E}$-well-distribution measure* of E_N is defined by

$$\Delta(E_N) = \max_{\phi,M,u,v} |X(E_N, \phi, M, u, v)|,$$

and the *$\mathcal{E}$-correlation measure of order* ℓ of E_N is

$$\Gamma_\ell(E_N) = \max_{\phi,M,D} |G(E_N, \phi, M, D)|.$$

Again the maxima are taken over all indices varying from 1 to N.

The two sets of measures are related by the following formulas (see [19, Theorems 1, 2]):

$$\frac{k}{k-1}\delta(E_N) \le \Delta(E_N) \le k\delta(E_N), \tag{1.3}$$

$$\frac{1}{k^\ell}\Gamma_\ell(E_N) \le \gamma_\ell(E_N) \le \sum_{t=1}^{\ell}\binom{\ell}{t}(k-1)^t\Gamma_t(E_N).$$

A sequence E_N is considered to be a"good" pseudorandom sequence if both $\delta(E_N)$ and $\gamma_\ell(E_N)$ are of magnitude $o(N)$ at least for small ℓ, and preferably the orders of $\delta(E_N)$ and $\gamma_\ell(E_N)$ should be close to $O(\sqrt{N}\log N)$, which is the value for the truly random case (see [4] and Theorem 1). By (1.3), similar statements hold for $\Delta(E_N)$ and $\Gamma_\ell(E_N)$.

Note that when $k = 2$, we can recover the well-distribution and correlation measures in the binary case from the $\mathcal{E}$-measures by taking $\mathcal{A} = \{-1, 1\}$ and all maps ϕ to be the identity. More precisely, for a binary sequence $E_N = (e_1, \dots, e_N) \in \{-1, 1\}^N$, the well-distribution measure is

$$W(E_N) = \max_{a,b,t}\Big|\sum_{j=0}^{t-1} e_{a+jb}\Big|,$$

and the correlation measure of order ℓ is

$$C_\ell(E_N) = \max_{M,D}\Big|\sum_{n=1}^{M} e_{n+d_1}\dots e_{n+d_\ell}\Big|.$$

Remark 1.1. In [19], the well-distribution measure (1.1) and the correlation measure (1.2) were called the f-well-distribution measure and f-correlation measure respectively, where "f" stands for *frequency*. To avoid confusion with the f-correlation for families of sequences defined by Gyarmati [9], in this paper "f-correlation" refers exclusively to the "family" notion.

Example 1.1. Let $\mathcal{A} = \mathcal{E}$ be the set of kth roots of unity. Let p be a prime, and let χ be a (multiplicative) character of order k over the finite field $\mathbb{F}_p$ (hence we have $k \mid p-1$). Let $f(x) \in \mathbb{F}_p[x]$ be a polynomial of degree $h > 0$ that has no multiple zero in the algebraic closure $\overline{\mathbb{F}}_p$. Consider the sequence $E_N = E_N(f) = (e_1, \dots, e_N) \in \mathcal{A}^N$ defined by

$$e_n = \begin{cases} \chi(f(n)) & \text{if } (f(n), p) = 1, \\ 1 & \text{otherwise.} \end{cases}$$

It is shown in [2] that

$$\delta(E_p) < 11hp^{1/2}\log p.$$

If furthermore no combination

$$F(n) = f(n+d_1)^{t_1} \dots f(n+d_\ell)^{t_\ell}$$

is a constant multiple of a complete kth power for any distinct d_i and any $(t_1, \dots, t_\ell) \neq 0$, $0 \leq t_j < k$, then

$$\gamma(E_p) < 10\ell h k p^{1/2} \log p.$$

In other words, for those f, the corresponding sequence $E_N(f)$ is a pseudorandom sequence. It is shown in [3] that f has the above property if any one of the following conditions holds:

(1) $k > 2$, $h < p$ and $\ell = 1$, or $k = 2$, $h < p$ and $\ell = 1, 2$.
(2) $(4h)^{\ell(k-1)} < p$.
(3) For any prime q dividing k, q is a primitive root modulo p.

1.2. f-correlation of binary pseudorandom sequences. We recall that in [9], Gyarmati defined the f-correlation of a family of sequences by considering the concatenation of distinct sequences in the family.

Definition 1.2. Let $\mathcal{F}$ be a family of pseudorandom binary sequences. The *f-correlation measure* of order m is defined by

$$C_m(\mathcal{F}) = \max_{1 \leq \ell \leq m,\, E_N^{(1)}, \dots, E_N^{(\ell)} \in \mathcal{F}} C_m(\{E_N^{(1)}, \dots, E_N^{(\ell)}\}),$$

where $\{E_N^{(1)}, \dots, E_N^{(\ell)}\} \in \{-1, 1\}^{\ell N}$ is the sequence of length ℓN obtained by concatenating the sequences $E_N^{(1)}, \dots, E_N^{(\ell)}$ in that order.

Example 1.3. Consider the case of $k = 2$ in Example 1.1. For a prime p and a polynomial $f(x) \in \mathbb{F}_p[x]$ of degree h that has no multiple zero, define $E_N = E_N(f) = (e_1, \dots, e_N)$ by

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

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. In [9], Gyarmati considered the f-correlation of several families of E_N with different sets of polynomials. For example, if $\mathcal{F}$ is the set of all polynomials of degree at most h that have no multiple zero, then $C_2(\mathcal{F}) \geq p - 1$ is large. However, if $\mathcal{F}_2 \subseteq \mathcal{F}$ is the set of all monic polynomials of degree at most h and of the form

$$f(x) = x^r + a_{r-2}x^{r-2} + \dots + a_1 x + a_0 \tag{1.4}$$

with $1 \leq r \leq h$ and $a_i \in \mathbb{F}_p$, then

$$C_2(\mathcal{F}_2) \leq 80 h p^{1/2} \log p$$

is small, but $C_k(\mathcal{F}_2) \geq p$ is large for all $k \geq 3$. Finally, if we take $\mathcal{F}_3 \subseteq \mathcal{F}_2$ to be the set of all *irreducible* monic polynomials of the form (1.4), then

$$C_k(\mathcal{F}_3) \leq 10hk^2 2^{k-1} p^{1/2} \log p.$$

So $\mathcal{F}_3$ has small f-correlation to a very high order.

To see the applicability of this notion of f-correlation for k-ary sequences, we will study Example 1.1 and find families of polynomials that have small f-correlation of high orders, analogous to that of Example 1.3.

2. f-correlation of k-ary sequences and statements of main results. We start with the definitions for the f-correlation of families of k-ary sequences, which are direct generalizations of Definition 1.2. Since there are two measures for pseudorandomness of k-ary sequences, there are two definitions for the f-correlation. Similar to the case of one pseudorandom sequences, these two definitions are nearly equivalent.

DEFINITION 2.1. Let $\mathcal{F}$ be a family of k-ary sequences.

(1) The *f-correlation measure* of order m is defined by

$$c_m(\mathcal{F}) = \max_{1 \leq \ell \leq m,\, E_N^{(1)}, \ldots, E_N^{(\ell)} \in \mathcal{F}} \gamma_m(\{E_N^{(1)}, \ldots, E_N^{(\ell)}\}),$$

where $\{E_N^{(1)}, \ldots, E_N^{(\ell)}\} \in \mathcal{A}^{\ell N}$ is the sequence of length ℓN obtained by concatenating the sequences $E_N^{(1)}, \ldots, E_N^{(\ell)}$ in that order.

(2) The *$\mathcal{E}$-f-correlation measure* of order m is defined by

$$C_m(\mathcal{F}) = \max_{1 \leq \ell \leq m,\, E_N^{(1)}, \ldots, E_N^{(\ell)} \in \mathcal{F}} \Gamma_m(\{E_N^{(1)}, \ldots, E_N^{(\ell)}\}).$$

Clearly $c_m(\mathcal{F})$ and $C_m(\mathcal{F})$ have the following properties.

PROPOSITION 2.2. *Let $\mathcal{F}$, $\mathcal{F}_1$ and $\mathcal{F}_2$ be families of k-ary sequences.*

(1) *If $m_1 \leq m_2$ are two positive integers, then $c_{m_1}(\mathcal{F}) \leq c_{m_2}(\mathcal{F})$ and $C_{m_1}(\mathcal{F}) \leq C_{m_2}(\mathcal{F})$.*
(2) *If $\mathcal{F}_1 \subseteq \mathcal{F}_2$, then $c_m(\mathcal{F}_1) \leq c_m(\mathcal{F}_2)$ and $C_m(\mathcal{F}_1) \leq C_m(\mathcal{F}_2)$.*
(3) *We have*

$$\frac{1}{k^m} C_m(\mathcal{F}) \leq c_m(\mathcal{F}) \leq (k^m - 1) C_m(\mathcal{F}).$$

From (3), we see that $C_m(\mathcal{F})$ and $c_m(\mathcal{F})$ only differ by a constant multiple. So we will focus on $c_m(\mathcal{F})$; the corresponding statements for $C_m(\mathcal{F})$ can be derived similarly.

Before analyzing the f-correlations of the family in Example 1.1, we first give some idea of the situation in the perfectly random case.

THEOREM 1. *Let $E_N^{(1)}, \dots, E_N^{(m)}$ be m randomly chosen k-ary sequences, and let ℓ be a positive integer. For all $\varepsilon > 0$, there is a number $N_0 = N_0(\varepsilon, k, \ell, m)$ such that for all $N > N_0$,*

$$P\big(\gamma_\ell(\{E_N^{(1)}, \dots, E_N^{(m)}\}) > 10k^\ell (2k\ell mN \log mN)^{1/2}\big) < \varepsilon, \tag{2.1}$$

and there is a number $N_1 = N_1(\varepsilon, k, \ell, m)$ such that for all $N > N_1$,

$$P\big(\Gamma_\ell(\{E_N^{(1)}, \dots, E_N^{(m)}\}) > 10k^{2\ell} (2k\ell mN \log mN)^{1/2}\big) < \varepsilon. \tag{2.2}$$

The above theorem complements [4, Theorem 4] (see Lemma 3.2 below). Note also that (2.2) follows from (2.1) by using (1.3).

Next, let $E_N(f)$ be defined as in Example 1.1. We first notice that if $r \in \mathbb{F}_p^*$ is a kth power residue modulo p, and if $g(x) = rf(x)$, then $E_N(f) = E_N(g)$. In general, if $g(x) = rf(x)$ for some $r \in \mathbb{F}_p^*$, it is not difficult to see that

$$\gamma_2(\{E_N(f), E_N(g)\}) \ge N/(2k).$$

Hence, if we want a family with small f-correlation, it is natural to restrict our attention to

$$\mathcal{F} = \{E_N(f) : f(x) \in \mathbb{F}_p[x],\ 0 < \deg(f) \le h, \\ f \text{ monic and without multiple roots}\}, \tag{2.3}$$

where $0 < h < p$.

Our next task is to investigate the f-correlation of $\mathcal{F}$ and some of its subfamilies. In particular, we will construct subfamilies that have small f-correlation close to the random case. First, note that if $g(x) = f(x + a)$ for some $a \in \mathbb{F}_p$ with $|a| < N$, then the ith entry of $E_N(g)$ is the same as the $(i + a)$th entry of $E_N(f)$. So these two sequences are not independent. Indeed,

$$\begin{aligned}
\gamma_2(\{E_N(f), E_N(g)\}) &= \max_{w,M,D} \left| g(\{E_N(f), E_N(g)\}, w, M, D) - \frac{M}{k^2} \right| \\
&\ge \left| \{n : 1 \le n \le N - a, (e_n, e_{n+N+a}) = (1, 1)\} - \frac{N-a}{k^2} \right| \\
&= \left| \{n : 1 \le n \le N - a, e_n = 1\} - \frac{N-a}{k^2} \right| \\
&= \frac{N-a}{k} - \frac{N-a}{k^2} + O(\sqrt{p} \log p).
\end{aligned}$$

Hence, if we want a family with small f-correlation, then we may only take at most one of the $f(x+a)$ into the family. In general, we have the following criterion on the polynomials to guarantee that a subfamily of $\mathcal{F}$ has small f-correlation.

THEOREM 2. *Let $\mathcal{F}$ be defined in* (2.3). *Let $\mathcal{F}_1 \subseteq \mathcal{F}$ be a family of pseudorandom k-ary sequences, and let ℓ be a positive integer. If for any set of m sequences*

$$E_N(f_1), \dots, E_N(f_m) \in \mathcal{F},$$

any $\mathbf{i} = (i_1, \dots, i_\ell)$ with $1 \le i_1 \le \cdots \le i_\ell \le m$, any $a_1 \dots, a_\ell \in \mathbb{F}_p$ such that $a_r \ne a_s$ whenever $i_r = i_s$, and any nonzero $\mathbf{t} = (t_1, \dots, t_m)$ with $0 \le t_i < k$, the combination

$$\prod_{j=1}^{\ell} f_{i_j}(x + a_j)^{t_j}$$

is never a constant multiple of a complete kth power in $\mathbb{F}_p[x]$, then

$$\gamma_\ell(\{E_N(f_1), \dots, E_N(f_m)\}) \le 10\ell m^2 h p^{1/2} \log p.$$

As a consequence,

$$c_m(\mathcal{F}_1) \le 10 m^3 h p^{1/2} \log p.$$

REMARK 2.1. Although we are in the case of k-ary sequences, it is still important that the polynomials f_i have distinct roots. Merely requiring them to be kth power free is not enough to ensure small f-correlation. For example, let $p > 5$ and $k = 3$. Set

$$f_1(x) = (x^2 - 1)^2(x^2 - 4), \qquad f_2(x) = (x^2 - 1)(x^2 - 4)^2.$$

Then both f_1 and f_2 are cube free, and hence $E_N(f_1)$ and $E_N(f_2)$ are both pseudorandom. However, their product $f_1(x)f_2(x) = (x^2 - 1)^3(x^2 - 4)^3$ is a perfect cube. Therefore, $\gamma_2(\{E_N(f_1), E_N(f_2)\})$ is large. Indeed, let $E = \{E_N(f_1), E_N(f_2)\}$ and write $E = (e_1, \dots, e_{2N})$; then $e_i e_{N+i} = 1$ for all $1 \le i \le N$. It is now easy to see that $\gamma_2(E) \ge N/6$.

The condition on the polynomials f_i in Theorem 2 is difficult to check in general (for a discussion of the case $m = 1$, see [3]), but we will improve a condition in [3] for the case $m = 1$, namely (2) in Example 1.3 there.

THEOREM 3. *With notation as in Theorem* 2, *for $m = 1$, the condition on the polynomials in Theorem* 2 *is satisfied if $(4h)^\ell < p$.*

We are now ready to construct explicit families of pseudorandom k-ary sequences that have small f-correlation, similar to the binary case. As in the binary case, forcing one coefficient (neither leading nor constant) to be zero is enough to guarantee small f-correlation of order two; for example we have the following.

COROLLARY 4. *Let p be a prime. Let $\mathcal{F}_2$ be the subfamily of $\mathcal{F}$ defined by polynomials of the form*

$$f(x) = x^r + a_{r-2}x^{r-2} + \cdots + a_1 x + a_0,$$

where $0 < r \le h$, $a_i \in \mathbb{F}_p$ and the coefficient of x^{r-1} is zero. Then

$$c_2(\mathcal{F}_2) \le 80hp^{1/2}\log p.$$

REMARK 2.2. Similar to [9, Theorem 3], the family $\mathcal{F}_2$ has small f-correlation of order two, but $c_m(\mathcal{F}_2)$ is large for all $m \ge 3$.

In order to get a family of small f-correlation, we can use irreducible polynomials.

COROLLARY 5. *Let p be a prime. Let $\mathcal{F}_3$ be the subfamily of $\mathcal{F}_2$ consisting of the $E_N(f)$ with $f(x) \in \mathbb{F}_p[x]$ irreducible. Then*

$$c_m(\mathcal{F}_3) \le 10 \cdot 2^{m-1}m^2hp^{1/2}\log p \quad \text{for any } m.$$

3. Lemmas. In this section we collect several lemmas that will be used later. The first one gives an estimate for incomplete character sums, which is of vital importance in our later proofs.

LEMMA 3.1. *Let p be a prime, and let χ be a (multiplicative) character of order d. Let $f(x) \in \mathbb{F}_p[x]$ of degree h be such that $f(x) \ne cg(x)^d$ for any $c \in \mathbb{F}_p$ and $g(x) \in \mathbb{F}_p[x]$. Then for any real numbers X, Y,*

$$\Big|\sum_{X<n<X+Y} \chi(f(n))\Big| < 9hp^{1/2}\log p.$$

Proof. This is [15, Theorem 1], a consequence of Weil's theorem [27]. ∎

The next lemma is about the $\mathcal{E}$-correlation of a randomly chosen k-ary sequence.

LEMMA 3.2. *Suppose k is even. Let E_N be a randomly chosen k-ary sequence of length N. For each positive integer ℓ and each $\varepsilon > 0$, there is an $N_0 = N_0(\varepsilon, k, \ell)$ such that for all $N > N_0$,*

$$P\big(\Gamma_\ell(E_N) > 10(k\ell N\log N)^{1/2}\big) < \varepsilon.$$

Proof. See Bérczi [4, Theorem 4]. ∎

We will also need Minkowski's lattice point theorem, a basic and well-known result in number theory. For a proof, see [23, Theorem I.4.4].

LEMMA 3.3. *Let Γ be a complete lattice in $\mathbb{R}^n$. Let X be a convex subset of $\mathbb{R}^n$, symmetric with respect to the origin, whose volume satisfies*

$$\mathrm{vol}(X) > 2^n \mathrm{vol}(\Gamma).$$

Then X contains at least one nonzero lattice point in Γ.

The final lemma of this section, which is a consequence of Minkowski's theorem, shows that translations of a given set in $\overline{\mathbb{F}}_p$ will always reach new elements, provided that the number of translations is relatively small.

LEMMA 3.4. *Let $r \geq 2$ and let $x_1, \dots, x_\ell \in \mathbb{F}_p$ be distinct. Suppose $\mathcal{M}$ is a nonempty finite subset of $\overline{\mathbb{F}}_p$ with $4|\mathcal{M}| < p^{1/\ell}$. Then there exists a $j \in \{1, \dots, \ell\}$ such that $\mathcal{M} + x_j$ is not contained in $\bigcup_{i \neq j}(\mathcal{M} + x_i)$.*

Proof. Suppose $(x_1, \dots, x_\ell, \mathcal{M})$ provides a counterexample to the statement. Then for any nonzero $t \in \mathbb{F}_p$, the tuple $(tx_1, \dots, tx_\ell, t\mathcal{M})$ is another counterexample.

By Lemma 3.3, there exists a nonzero integer t such that

$$\begin{cases} |t| \leq p-1, \\ \|tx_1/p\| \leq (p-1)^{-1/\ell}, \\ \qquad \vdots \\ \|tx_\ell/p\| \leq (p-1)^{-1/\ell}. \end{cases}$$

Thus there are integers y_j such that

$$\begin{cases} |y_j| \leq p(p-1)^{-1/\ell}, \\ y_j \equiv tx_j \pmod{p}, \end{cases} \tag{3.1}$$

for any $j \in \{1, \dots, \ell\}$, and $(y_1, \dots, y_\ell, t\mathcal{M})$ is a counterexample. Now let j_0 be such that $|y_{j_0}| = \max_{1 \leq j \leq \ell} |y_j|$. Choose $\alpha \in t\mathcal{M}$ and set $\tilde{\mathcal{M}} = t\mathcal{M} \cap (\alpha + \mathbb{F}_p)$. Then $(y_1, \dots, y_\ell, \tilde{\mathcal{M}})$ will also be a counterexample.

Note that $\alpha + \mathbb{F}_p$ can be written as a union of at most $|\tilde{\mathcal{M}}|$ intervals (i.e. subsets of $\mathbb{F}_p$ consisting of consecutive integers, or translates of such subsets in $\overline{\mathbb{F}}_p$) whose endpoints are in $\tilde{\mathcal{M}}$, and which contain no points in $\tilde{\mathcal{M}}$ apart from the endpoints. Let $\mathcal{I} = \{\alpha + a, \alpha + a + 1, \dots, \alpha + b\}$ be the longest of these intervals. Then

$$|b - a| \geq \frac{p}{|\tilde{\mathcal{M}}|} \geq \frac{p}{|\mathcal{M}|}.$$

From this, (3.1) and the hypothesis $4|\mathcal{M}| < p^{1/r}$, we obtain

$$|b - a| > 4p^{1-1/r} > 2|y_{j_0}|.$$

Now if $y_{j_0} > 0$, then $\alpha + a + y_{j_0}$ belongs to $\tilde{\mathcal{M}} + y_{j_0}$ but not to $\bigcup_{i \neq j_0}(\tilde{\mathcal{M}} + y_i)$ (because $\alpha + a + y_{j_0}$ still lies in $\mathcal{I}$, and $|y_{j_0}|$ is maximal among all y_i). Similarly, if $y_{j_0} < 0$, then $\alpha + b + y_{j_0}$ belongs to $\tilde{\mathcal{M}} + y_{j_0} \setminus \bigcup_{i \neq j_0}(\tilde{\mathcal{M}} + y_i)$. This contradicts that $(y_1, \dots, y_r, \tilde{\mathcal{M}})$ is a counterexample, and completes our proof. ∎

4. Proof of Theorem 1. Since, as remarked after the statement of Theorem 1, (2.2) follows from (2.1), it is enough to prove (2.1). By Lemma 3.2 and (1.3), one immediately obtains (2.1) for all even k.

Now, fix an odd k. Write $\mathcal{A}_{2k}$ and $\mathcal{A}_k$ for sets of $2k$ and k symbols respectively. Fix any 2-to-1 map $\varphi : \mathcal{A}_{2k} \to \mathcal{A}_k$ (i.e. for any $a \in \mathcal{A}_k$, $\phi^{-1}(a)$ consists of exactly two elements), and extend φ in the natural way to a

map $\mathcal{A}_{2k}^N \to \mathcal{A}_k^N$. Let $E_N \in \mathcal{A}_k^N$ be a random k-ary sequence. Then there are 2^N sequences $\tilde{E}_N$ such that $\varphi(\tilde{E}_N) = E_N$. Pick one of them, and write $\tilde{E}_N = (\tilde{e}_1, \dots, \tilde{e}_N)$.

Recall that

$$g_k(E_N, w, M, D) = |\{n : 1 \le n \le M,\ (e_{n+d_1}, \dots, e_{n+d_\ell}) = w\}|.$$

Set

$$r_k(E_N, w) = r_k(E_N, w, M, D) := g_k(E_N, w, M, D) - \frac{M}{k^\ell}. \tag{4.1}$$

From the definition of $g_k(E_N, w)$ we have

$$\begin{aligned} g_k(E_N, w) &= |\{n : 1 \le n \le M,\ (e_{n+d_1}, \dots, e_{n+d_\ell}) = w\}| \\ &= |\{n : 1 \le n \le M,\ \varphi(\tilde{e}_{n+d_1}, \dots, \tilde{e}_{n+d_\ell}) = w\}| \\ &= |\{n : 1 \le n \le M,\ (\tilde{e}_{n+d_1}, \dots, \tilde{e}_{n+d_\ell}) \in \varphi^{-1}(w)\}| \\ &= \sum_{\tilde{w} \in \varphi^{-1}(w)} g_k(\tilde{E}_N, \tilde{w}). \end{aligned}$$

Using (4.1), we get

$$\frac{M}{k^\ell} + r_k(E_N, w) = \sum_{\tilde{w} \in \varphi^{-1}(w)} \left(\frac{M}{(2k)^\ell} + r(\tilde{E}_N, \tilde{w}) \right),$$

which simplifies to

$$r_k(E_N, w) = \sum_{\tilde{w} \in \varphi^{-1}(w)} r_k(\tilde{E}_N, \tilde{w})$$

since there are 2^ℓ elements in $\varphi^{-1}(w)$. Taking absolute values on both sides, then take the maximum over all w, D, M and use (1.2) to obtain

$$\gamma_\ell(E_N) \le 2^\ell \gamma_\ell(\tilde{E}_N). \tag{4.2}$$

Let $A > 0$ be a real number. Then (4.2) implies that to one E_N with $\gamma_\ell(E_N) > A$ there correspond at least 2^N of $\tilde{E}_N$ with $\gamma_\ell(\tilde{E}_N) > A/2^\ell$.

Now consider

$$\begin{aligned} P(\gamma_\ell(E_N) > A) &= \frac{|E_N \in \mathcal{A}_k^N : \gamma_\ell(E_N) > A|}{k^N} \\ &\le \frac{2^{-N} |\tilde{E}_N \in \mathcal{A}_{2k}^N : \gamma_\ell(E_N) > A/2^\ell|}{k^N} \\ &= \frac{|\tilde{E}_N \in \mathcal{A}_{2k}^N : \gamma_\ell(E_N) > A/2^\ell|}{(2k)^N} \\ &= P(\gamma_\ell(\tilde{E}_N) > A/2^\ell). \end{aligned}$$

On the other hand, since $2k$ is even, we can apply Lemma 3.2 to obtain

$$P\big(\gamma_\ell(\tilde{E}_N) > 10(2k)^\ell (2k\ell N \log N)^{1/2}\big) < \varepsilon.$$

By the above calculation this implies

$$P\big(\gamma_\ell(E_N) > 10k^\ell(2k\ell N\log N)^{1/2}\big) < \varepsilon. \tag{4.3}$$

Now (2.1) for k odd and general m follows from (4.3), by replacing E_N with $\{E_N^{(1)},\dots,E_N^{(m)}\}$ and N with mN.

5. Proof of Theorem 2. Let $E_N(f_1),\dots,E_N(f_m)\in\mathcal{F}_1$ and set $E=\{E_N(f_1),\dots,E_N(f_m)\}$. Write $E=(e_1,\dots,e_{mN})$. Define $I_{i_1,\dots,i_\ell}$ to be the set of all n with $1\le n\le M$ and such that

$$i_j=\left[\frac{n+d_j-1}{N}\right]+1$$

for all $1\le j\le\ell$. It is easy to see that $I_{\mathbf{i}}$ is an interval (possibly empty) for all $\mathbf{i}$. Write $\mathbf{i}=(i_1,\dots,i_\ell)$. Clearly $I_{\mathbf{i}}$ is empty unless $1\le i_j\le m$ for all j. We also have $I_{\mathbf{i}_1}\cap I_{\mathbf{i}_2}=\emptyset$ if $\mathbf{i}_1\ne\mathbf{i}_2$, and the union of all $I_{\mathbf{i}}$ is the set of integers from 1 to M. Note that if we fix an i_1, then

$$\begin{aligned}
i_1=\left[\frac{n+d_1-1}{N}\right]+1 \Rightarrow\ & i_1-1\le\frac{n+d_1-1}{N}\le i_1\\
\Rightarrow\ & N(i_1-1)\le n+d_1-1\le i_1N\\
\Rightarrow\ & N(i_1-1)+d_j-d_1\le n+d_j-1\le i_1N+d_j-d_1\\
\Rightarrow\ & i_1-1+\frac{d_j-d_1}{N}\le\frac{n+d_j-1}{N}\le i_1+\frac{d_j-d_1}{N}\\
\Rightarrow\ & i_1-1+\left[\frac{d_j-d_1}{N}\right]\le\left[\frac{n+d_j-1}{N}\right]\le i_1+\left[\frac{d_j-d_1}{N}\right].
\end{aligned}$$

For any fixed i_1, clearly there exists an integer H_j such that

$$\left[\frac{n+d_j-1}{N}\right]=\begin{cases} i_1-1+\left[\frac{d_j-d_1}{N}\right] & \text{if } n<H_j,\\ i_1+\left[\frac{d_j-d_1}{N}\right] & \text{if } n\ge H_j.\end{cases}$$

Define a sequence of integers K_s $(0\le s\le\ell)$ by

$$\{K_0,K_1,\dots,K_\ell\}=\{0,H_2,H_3,\dots,H_\ell,M+1\}.$$

It is clear that $0=K_0\le K_1\le\cdots\le K_\ell=M+1$. From the definitions of the K_s's and H_s's, for any n,n' with $K_s\le n,n'\le K_{s+1}$ we have

$$\left[\frac{n+d_j-1}{N}\right]=\left[\frac{n'+d_j-1}{N}\right].$$

Thus the interval $[K_s,K_{s+1})$ is contained in a single interval $I_{i_1,\dots,i_\ell}$.

Since i_1 may take m different values and for each fixed i_1, the number of intervals $[K_s,K_{s+1})$ constructed above is ℓ and these intervals (for $0\le s\le\ell-1$) cover the whole range $[0,M]$, we have

$$|\{\mathbf{i}:I_{\mathbf{i}}\ne\emptyset\}|\le m\ell. \tag{5.1}$$

Next, consider

$$\begin{aligned} g(E,w,M,D) &= |\{1 \le n \le M : (e_{n+d_1},\dots,e_{n+d_\ell}) = w\}| \\ &= \sum_{\mathbf{i}} |\{n \in I_{\mathbf{i}} : (e_{n+d_1},\dots,e_{n+d_\ell}) = w\}|. \end{aligned}$$

Note that for $n \in I_{\mathbf{i}}$, we have $e_{n+d_j} = \chi(f_{i_j}(n+d_j-(i_j-1)N))$. Write $w = (w_1,\dots,w_\ell)$. By the orthogonality of characters, if $(a,p)=1$, then

$$\frac{1}{k}\sum_{t=0}^{k-1}(\overline{w_j}\chi(a))^t = \begin{cases} 1, & \chi(a) = w_j, \\ 0, & \chi(a) \ne w_j. \end{cases}$$

Hence,

$$\begin{aligned} &g(E,w,M,D) \\ &= \frac{1}{k^\ell}\sum_{\mathbf{i}} \sum_{\substack{n\in I_{\mathbf{i}} \\ p\nmid f_{i_j}(n+d_j-(i_j-1)N)}} \sum_{t_1=0}^{k-1}\cdots\sum_{t_\ell=0}^{k-1}\prod_{j=1}^{\ell}\big(\overline{w_j}\chi(f_{i_j}(n+d_j-(i_j-1)N))\big)^{t_j} \\ &\quad + \sum_{\mathbf{i}} \sum_{\substack{n\in I_{\mathbf{i}} \\ \exists j,\, p\mid f_{i_j}(n+d_j-(i_j-1)N)}} 1, \end{aligned} \tag{5.2}$$

where the sum over $\mathbf{i}$ is taken over all $\mathbf{i}$ with $I_{\mathbf{i}} \ne \emptyset$. By (5.1) we see that the second term on the right-hand side is at most

$$\sum_{\mathbf{i}} \sum_{\substack{n\in I_{\mathbf{i}} \\ \exists j,\, p\mid f_{i_j}(n+d_j-(i_j-1)N)}} 1 \le m^2\ell h. \tag{5.3}$$

Write $\mathbf{t} = (t_1,\dots,t_\ell)$. To estimate the first term on the right-hand side in (5.2), note that the terms corresponding to $\mathbf{t} = \mathbf{0}$ sum to

$$\frac{1}{k^\ell}\sum_{\mathbf{i}} \sum_{\substack{n\in I_{\mathbf{i}} \\ p\nmid f_{i_j}(n+d_j-(i_j-1)N)}} 1 = \frac{M}{k^\ell} - \frac{1}{k^\ell} \sum_{\substack{n\in I_{\mathbf{i}} \\ p\mid f_{i_j}(n+d_j-(i_j-1)N)}} 1.$$

Similar to (5.3), the second term above is at most $m^2\ell h/k^\ell$. Combining this with (5.2) and (5.3), we obtain

$$\begin{aligned} \gamma_\ell(E) \le{}& \frac{1}{k^\ell}\sum_{\mathbf{i}} \sum_{\substack{n\in I_{\mathbf{i}} \\ p\nmid f_{i_j}(n+d_j-(i_j-1)N)}} \sum_{\mathbf{t}\ne\mathbf{0}}\prod_{j=1}^{\ell}\big(\overline{w_j}\chi(f_{i_j}(n+d_j-(i_j-1)N))\big)^{t_j} \\ &+ 2m^2\ell h. \end{aligned}$$

Changing the order of summation yields

(5.4)

$$\gamma_\ell(E) \le \frac{1}{k^\ell} \sum_{\mathbf{i}} \sum_{\mathbf{t}\neq\mathbf{0}} \overline{w_1^{t_1} \dots w_\ell^{t_\ell}} \sum_{\substack{n\in I_{\mathbf{i}} \\ p\nmid f_{i_j}(n+d_j-(i_j-1)N)}} \prod_{j=1}^{\ell} \chi(f_{i_j}(n+d_j-(i_j-1)N))^{t_j} + 2m^2\ell h.$$

A typical polynomial in the character of the above sum is of the form

$$f_{i_1}(n+d_1-(i_1-1)N)^{t_1} \cdots f_{i_\ell}(n+d_\ell-(i_\ell-1)N)^{t_\ell}.$$

The condition in Theorem 2 implies that no such term is a complete kth power (take $a_j = d_j - (i_j-1)N$). By Lemma 3.1, we get

$$\sum_{\substack{n\in I_{\mathbf{i}} \\ p\nmid f_{i_j}(n+d_j-(i_j-1)N)}} \prod_{j=1}^{\ell} \chi\big(f_{i_j}(n+d_j-(i_j-1)N)\big)^{t_j} \le 9h\ell p^{1/2}\log p.$$

Putting this into (5.4) and using (5.1), we obtain

$$\gamma_\ell(E) \le 9\ell m h p^{1/2}\log p + 2m^2\ell h \le 10\ell m^2 h p^{1/2}\log p.$$

6. Proof of Theorem 3. Theorem 3 follows directly from the following proposition, which is slightly more general.

PROPOSITION 6.1. *Let $k \ge 2$ be an integer with $(k,p)=1$. Let $P(x) \in \mathbb{F}_p[x]$ be a monic polynomial of degree h which is not of the form $cg(x)^{k'}$ for any k' with $\mathrm{GCD}(k',k) > 1$, $c \in \mathbb{F}_p$ and $g \in \mathbb{F}_p[x]$. Let $b_1,\dots,b_\ell$ be distinct elements in $\mathbb{F}_p$ with*

$$\ell < \frac{\log p}{\log(4h)}.$$

Then for any $a \in \mathbb{F}_p$ and $\mathbf{e} = (e_1,\dots,e_\ell)$ with $0 \le e_j \le k-1$, $\mathbf{e} \neq 0$, the polynomial

$$Q(x) = \prod_{j=1}^{\ell} P(ax+b_j)^{e_j}$$

is not a complete kth power.

Proof. The proposition is clearly true for all k when $\ell = 1$. Suppose the proposition is not true; then there is a least $\ell > 1$ (satisfying our assumption $\ell < (\log p)/\log(4h)$) such that a counterexample exists. Let $\tilde{k}$ be the least k such that a counterexample occurs for the above ℓ. Then

$$Q(x) = \tilde{P}(x)^{\tilde{k}} = \prod_{j=1}^{\ell} P(ax+b_j)^{\tilde{e}_j}, \tag{6.1}$$

where $1 \le \tilde{e_j} < \tilde{k}$ (if $e_j = 0$ for some j we would have a smaller counterexample) and $\tilde{P}(x) \in \mathbb{F}_p[x]$ since $(k, p) = 1$.

Let $\alpha_1, \dots, \alpha_s$ be all the *distinct* zeros of $P(x)$ in $\overline{\mathbb{F}}_p$ whose multiplicities are not a multiple of $\tilde{k}$. Clearly $1 \le s \le h$. Let $\mathcal{M} = \{a^{-1}\alpha_1, \dots, a^{-1}\alpha_s\}$ and $x_j = -a^{-1}b_j$ for all $1 \le j \le \ell$. Note that $\mathcal{M} + x_j$ is the set of zeros of $P(ax + b_j)$. Since $4|\mathcal{M}| = 4s \le 4h < p^{1/\ell}$, we can apply Lemma 3.4 to obtain a j_0 such that at least one of the roots of $P(ax + b_{j_0})$ is distinct from the roots of all other $P(ax + b_i)$ for $i \ne j_0$. By permuting the x_j and α_j we may assume that the above occurs for $j_0 = \ell$, and the distinguished root is α_s, of multiplicity m_s.

If m_s is relatively prime to $\tilde{k}$, then $\tilde{e}_\ell m_s$ cannot be a multiple of $\tilde{k}$. This means the combination $Q(x)$ cannot be a complete $\tilde{k}$th power, contradicting (6.1). On the other hand, if $\mathrm{GCD}(m_s, \tilde{k}) = \tilde{k}/d > 1$, then (6.1) implies that $\tilde{e}_\ell$ must be a multiple of d. Since $1 < d < \tilde{k}$ (that $d > 1$ follows from the fact that m_s is not a multiple of $\tilde{k}$), we see that

$$\frac{Q(x)}{P(ax + b_\ell)^{\tilde{e}_\ell}} = \left(\frac{\tilde{P}(x)^{\tilde{k}/d}}{P(ax + b_\ell)^{\tilde{e}_\ell/d}}\right)^d = \prod_{j=1}^{\ell-1} P(ax + b_j)^{\tilde{e}_j} \tag{6.2}$$

is a complete dth power. Thus either there exists some $\tilde{e}_j$ which is not a multiple of d, so (6.2) is a counterexample with smaller ℓ, or each $\tilde{e}_j$ is a multiple of d, and then

$$Q(x)^{1/d} = \tilde{P}(x)^{\tilde{k}/d} = \prod_{j=1}^{\ell} P(ax + b_j)^{\tilde{e}_j/d}$$

is a counterexample with the same ℓ but a power smaller than $\tilde{k}$. In both cases we obtain a contradiction. ∎

7. Proof of the corollaries. It suffices to show that the families $\mathcal{F}_2$ and $\mathcal{F}_3$ satisfy the condition in Theorem 2. For Corollary 4, we need to show that for any $E_N(f_1), E_N(f_2) \in \mathcal{F}_2$ (with the possibility of $f_1 = f_2$), and for any $a_1, a_2 \in \mathbb{F}_p$ (with the restriction that $a_1 \ne a_2$ if $f_1 = f_2$), the product

$$Q(x) = f_1(x + a_1)^{t_1} f_2(x + a_2)^{t_2} \tag{7.1}$$

is not a complete kth power for any $0 \le t_1, t_2 < k$, not both zero.

When $f_1 = f_2$ this is a direct consequence of Theorem 3. When $f_1 \ne f_2$, suppose on the contrary that the $Q(x)$ defined in (7.1) is a complete kth power for some a_1, a_2, t_1, t_2. If there is a root $\alpha \in \overline{\mathbb{F}}_p$ of $f_1(x + a_1)$ that is not a root of $f_2(x + a_2)$, then $(x - \alpha)^{t_1}$ divides $Q(x)$ exactly (i.e. $(x - \alpha)^{t_1+1}$ does not divide $Q(x)$). Since $0 \le t_1 < k$ and $Q(x)$ is a complete kth power, this implies $t_1 = 0$. Thus

$$Q(x) = f_2(x + a_2)^{t_2},$$

which is also impossible since f_2 has no multiple roots and $0 < t_2 < k$. Hence $f_1(x+a_1)$ and $f_2(x+a_2)$ must share the same set of roots. As neither has multiple roots, this gives $f_1(x+a_1) = f_2(x+a_2)$, which is impossible by the construction of $\mathcal{F}_2$. This shows that the condition in Theorem 2 holds for $\mathcal{F}_2$.

The proof of Corollary 5 is similar. Let $1 \le \ell \le m$. Suppose

$$Q(x) = f_{i_1}(x+a_1)^{t_1} \dots f_{i_\ell}(x+a_\ell)^{t_\ell}.$$

Suppose $i_1 = \dots = i_s$ and the other i_j's are different. Write $f := f_{i_1} = \dots = f_{i_s}$. The combination

$$R(x) := f(x+a_1)^{t_1} \dots f(x+a_s)^{t_s}$$

is not a complete kth power since f is irreducible and $\deg f < p$. In particular, there is an $\alpha \in \overline{\mathbb{F}}_p$ such that $(x-\alpha)^t$ exactly divides $R(x)$, with $0 < t < k$. By the construction of the family $\mathcal{F}_3$, the roots of other f_{i_j} are linearly independent of the roots of $f(x)$, and so α is not a root of any of the $f_{i_j}(x+a_j)$ for any $i_j \ne i_1$. This means $(x-\alpha)^t$ exactly divides $Q(x)$, and $Q(x)$ cannot be a complete kth power.

Acknowledgments. We thank the referees for carefully reading the manuscript and for many valuable suggestions, in particular an argument that led to a considerable improvement on the estimate (5.1), and hence on Theorem 2.

References

[1] R. Ahlswede, L. H. Khachatrian, C. Mauduit, and A. Sárközy, *A complexity measure for families of binary sequences*, Period. Math. Hungar. 46 (2003), 107–118.

[2] R. Ahlswede, C. Mauduit, and A. Sárközy, *Large families of pseudorandom sequences of k symbols and their complexity. I*, in: General Theory of Information Transfer and Combinatorics, Lecture Notes in Comput. Sci. 4123, Springer, Berlin, 2006, 293–307.

[3] R. Ahlswede, C. Mauduit, and A. Sárközy, *Large families of pseudorandom sequences of k symbols and their complexity. II*, in: General Theory of Information Transfer and Combinatorics, Lecture Notes in Comput. Sci. 4123, Springer, Berlin, 2006, 308–325.

[4] G. Bérczi, *On finite pseudorandom sequences of k symbols*, Period. Math. Hungar. 47 (2003), 29–44.

[5] J. Cassaigne, S. Ferenczi, C. Mauduit, J. Rivat, and A. Sárközy, *On finite pseudorandom binary sequences. III. The Liouville function. I*, Acta Arith. 87 (1999), 367–390.

[6] J. Cassaigne, S. Ferenczi, C. Mauduit, J. Rivat, and A. Sárközy, *On finite pseudorandom binary sequences. IV. The Liouville function. II*, Acta Arith. 95 (2000), 343–359.

[7] J. Cassaigne, C. Mauduit, and A. Sárközy, *On finite pseudorandom binary sequences. VII. The measures of pseudorandomness*, Acta Arith. 103 (2002), 97–118.

[8] D. Gomez and A. Winterhof, *Multiplicative character sums of Fermat quotients and pseudorandom sequences*, Period. Math. Hungar. 64 (2012), 161–168.

[9] K. Gyarmati, *Concatenation of pseudorandom binary sequences*, Period. Math. Hungar. 58 (2009), 99–120.

[10] K. Gyarmati, C. Mauduit, and A. Sárközy, *The cross-correlation measure for families of binary sequences*, in: Applied Algebra and Number Theory, G. Larcher et al. (eds.), Cambridge Univ. Press, 2014, 126–143.

[11] H. Liu, *A family of pseudorandom binary sequences constructed by the multiplicative inverse*, Acta Arith. 130 (2007), 167–180.

[12] H. Liu and C. Yang, *On a problem of D. H. Lehmer and pseudorandom binary sequences*, Bull. Braz. Math. Soc. (N.S.) 39 (2008), 387–399.

[13] K.-H. Mak, *More constructions of pseudorandom sequences of k symbols*, Finite Fields Appl. 25 (2014), 222–233.

[14] C. Mauduit, J. Rivat, and A. Sárközy, *Construction of pseudorandom binary sequences using additive characters*, Monatsh. Math. 141 (2004), 197–208.

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

[16] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences. II. The Champernowne, Rudin–Shapiro, and Thue–Morse sequences, a further construction*, J. Number Theory 73 (1998), 256–276.

[17] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences. V. On* $(n\alpha)$ *and* $(n^2\alpha)$ *sequences*, Monatsh. Math. 129 (2000), 197–216.

[18] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences. VI. On* $(n^k\alpha)$ *sequences*, Monatsh. Math. 130 (2000), 281–298.

[19] C. Mauduit and A. Sárközy, *On finite pseudorandom sequences of k symbols*, Indag. Math. (N.S.) 13 (2002), 89–101.

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

[21] L. Mérai, *A construction of pseudorandom binary sequences using rational functions*, Unif. Distrib. Theory 4 (2009), 35–49.

[22] L. Mérai, *Construction of pseudorandom binary sequences over elliptic curves using multiplicative characters*, Publ. Math. Debrecen 80 (2012), 199–213.

[23] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, Berlin, 1999.

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

[25] V. Tóth, *Collision and avalanche effect in families of pseudorandom binary sequences*, Period. Math. Hungar. 55 (2007), 185–196.

[26] V. Tóth, *Extension of the notion of collision and avalanche effect to sequences of k symbols*, Period. Math. Hungar. 65 (2012), 229–238.

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

[28] C. Wu, X. Weng, and Z. Chen, *Construction of k-ary pseudorandom elliptic curve sequences*, Wuhan Univ. J. Nat. Sci. 16 (2011), 452–456.

Kit-Ho Mak
Department of Mathematics
The Chinese University of Hong Kong
Shatin, NT, Hong Kong
E-mail: khmak@math.cuhk.edu.hk

Alexandru Zaharescu
Simion Stoilow Institute of Mathematics
of the Romanian Academy
P.O. Box 1-764
RO-014700 Bucureşti, Romania
and
Department of Mathematics
University of Illinois at Urbana-Champaign
1409 W. Green Street
Urbana, IL 61801, U.S.A.
E-mail: zaharesc@illinois.edu