Large families of pseudorandom sequences of k symbols and their complexity, Part I

R. Ahlswede, C. Mauduit and A. Sárközy*

Dedicated to the memory of Levon Khachatrian

*Research partially supported by Hungarian National Foundation for Scientific Research, Grant No. T043623.

1 Introduction

In earlier papers we introduced the measures of pseudorandomness of finite binary sequences [13], constructed large families of binary sequences with strong PR (= pseudorandom) properties [6], [12], introduced the notion of f–complexity of families of binary sequences and we showed that one of the earlier constructions can be modified to obtain families with high f–complexity [4]. In another paper [14] we extended the study of pseudorandomness from binary sequences to sequences of k symbols ("letters"). In [14] we also constructed *one* "good" pseudorandom sequence of a given length of k symbols. However, in the applications we need not only a few good sequences but large families of them, and in certain applications (cryptography) the complexity of the family of these sequences is more important, than the size of it. In this paper our goal is to construct "many" "good" PR sequences of k symbols, to extend the notion of f–complexity to the k symbol case and to study this extended f–complexity concept.

2 A special case

First we will study the important special case when k, the number of symbols (the "size of the alphabet") is a 2–power: $k = 2^r$. We will show that in this case any "good" PR binary sequence

$$E_N = (e_1, e_2, \dots, e_N) \in \{-1, +1\}^N \tag{2.1}$$

defines a sequence of k symbols with "nearly as good" PR properties so that the constructions given in the binary case can be used in the $k = 2^r$ symbol case nearly as effectively.

First we have to recall several definitions from earlier papers. If E_N is a binary sequence of form (2.1), then write

$$U(E_N; t, a, b) = \sum_{j=0}^{t-1} e_{a+jb}$$

and, for $D = (d_1, \dots, d_\ell)$ with non–negative integers $d_1 < \dots < d_\ell$

$$V(E_N, M, D) = \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \dots e_{n+d_\ell}.$$

Then the *well–distribution measure* of E_N is defined

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

where the maximum is taken over all a, b, t such that $a, b, t \in \mathbb{N}$ and $1 \le a \le a+(t-1)b \le N$, while the correlation measure of order ℓ of E_N is defined as

$$C_\ell(E_N) = \max_{M,D} |V(E_N, M, D)| = \max_{M,D} \left| \sum_{n=1}^{M} e_{N+d_1} e_{n+d_2} \dots e_{n+d_\ell} \right|,$$

where the maximum is taken over all $D = (d_1, d_2, \dots, d_\ell)$ and M such that $M + d_\ell \le N$. Then the sequence E_N is considered as a "good" PR sequence if both these measures $W(E_N)$ and $C_\ell(E_N)$ (at least for small ℓ) are "small" in terms of N (in particular, both are $o(N)$ as $N \to \infty$). Indeed, it is shown in [5], [10] that for a "truely random" $E_N \in \{-1, +1\}$ both $W(E_N)$ and, for fixed ℓ, $C_\ell(E_N)$ are around $N^{1/2}$ with "near 1" probability.

In our first paper [13] written on this subject we also introduced a third measure which later we did not use but it will be needed here: the *combined* (well–distribution–correlation) *PR measure of order* ℓ is defined by

$$\begin{aligned} Q_\ell(E_N) &= \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \dots e_{a+jb+d_\ell} \right| \\ &= \max_{a,b,t,D} |Z(a,b,t,D)| \end{aligned} \tag{2.2}$$

where

$$Z(a,b,t,D) = \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \dots e_{a+jb+d_\ell}$$

is defined for all $a, b, t, D = (d_1, d_2, \dots, d_\ell)$ such that all the subscripts $a + jb + d_i$ belong to $\{1, 2, \dots, N\}$ (and the maximum in (2.2) is taken over D's of dimension ℓ).

In [14] we extended these definitions to the case of k symbols. It is not at all clear how to do this extension and, indeed, in [14] we introduced two different ways of extension which are nearly equivalent. Here we will present only one of them which is more suitable for our purpose. Let $k \in \mathbb{N}$, $k \ge 2$, and let $\mathcal{A} = \{a_1, a_2, \dots, a_k\}$ be a finite set ("alphabet") of k symbols ("letters") and consider a sequence $E_N = (e_1, e_2, \dots, e_N) \in \mathcal{A}^N$ of these symbols. Write

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

and for $W = (a_{i_1}, \dots, a_{i_\ell}) \in \mathcal{A}^\ell$ and $D = (d_1, \dots, d_\ell)$ with non–negative integers $d_1 < \dots < d_\ell$,

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

Then the *f–well–distribution* ("*f*" for "frequency") *measure* of E_N is defined as

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

where the maximum is taken over all $a \in \mathcal{A}$ and $u.v.M$ with $u + (M-1)v \le N$, while the *f–correlation measure of order* ℓ of E_N is defined as

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

where the maximum is taken over all $W \in \mathcal{A}^\ell$, and $D = (d_1, \dots, d_\ell)$ and M such that $M + d_\ell \le N$.

We showed in [14] that in the special case $k = 2$, $\mathcal{A} = \{-1,+1\}$ the *f–measures* $\delta(E_N)$, $\gamma_\ell(E_N)$ are between two constant multiples of the binary measures $W(E_N)$, resp. $C_\ell(E_N)$, so that, indeed, the f–measures can be considered as extensions of the binary measures.

Now let E_N be the binary sequence in (2.1), and to this binary sequence assign a sequence $\varphi(E_N)$ whose elements are the 2^n letters in the alphabet $\{-1,+1\}^r$, and whose length is $[N/r]$:

$$\varphi(E_N) = \big((e_1,\dots,e_r),(e_{r+1},\dots,e_{2r}),\dots,(e_{([N/r]-1)r+1},\dots,e_{[N/r]r})\big).$$

We will show that if E_N is a "good" PR binary sequence, then $\varphi(E_N)$ is also a "good" PR sequence of the $k = 2^r$ letters in the alphabet $\{-1,+1\}^r$. Indeed, this follows from the inequalities in the following theorem:

Theorem 1. *If E_N and $\varphi(E_N)$ are defined as above, then we have*

$$\delta\big(\varphi(E_N)\big) \le \frac{1}{2^r}\sum_{s=1}^{r}\binom{r}{s}Q_s(E_N) \tag{2.3}$$

and, for $\ell \in \mathbb{N}$

$$\gamma_\ell\big(\varphi(E_N)\big) \le \frac{1}{2^{r\ell}}\sum_{s=1}^{r}\sum_{q=1}^{\ell}\binom{r}{s}\binom{\ell}{q}Q_{qs}(E_N). \tag{2.4}$$

Proof of Theorem 1. Clearly, for all $a = (\varepsilon_1,\dots,\varepsilon_r) \in \{-1,+1\}^r$, M, u and v we have

$$\begin{aligned}
x\big(\varphi(E_N),a,M,u,v\big) &= \big|\big\{j : 0 \le j \le M-1, (e_{(u+jv-1)r+1},\dots,e_{(u+jv)r}) = (\varepsilon_1,\dots,\varepsilon_r)\big\}\big| \\
&= \sum_{j=0}^{M-1}\prod_{i=1}^{r}\frac{e_{(u+jv-1)r+i}\varepsilon_i + 1}{2} \\
&= \frac{M}{2^r} + \frac{1}{2^r}\sum_{s=1}^{r}\sum_{1\le i_1<\dots<i_s\le r}\varepsilon_{i_1}\dots\varepsilon_{i_s}\sum_{j=0}^{M-1}e_{(u+jv-1)r+i_1}\dots e_{(u+jv-1)r+i_s}
\end{aligned}$$

whence

$$\begin{aligned}
&\left|x\big(\varphi(E_N),a,M,u,v\big) - \frac{M}{k}\right| = \left|x\big(\varphi(E_N),a,M,u,v\big) - \frac{M}{2^r}\right| \\
&\le \frac{1}{2^r}\sum_{s=1}^{r}\sum_{1\le i_1<\dots<i_s\le r}\left|\sum_{j=0}^{M-1}e_{(u-1)r+jvr+i_1}\dots e_{(u-1)r+jvr+i_s}\right| \\
&= \frac{1}{2^r}\sum_{s=1}^{r}\sum_{1\le i_1<\dots<i_s\le r}\big|Z\big((u-1)r,vr,M-1,(i_1,\dots,i_s)\big)\big| \\
&\le \frac{1}{2^r}\sum_{s=1}^{r}\sum_{1\le i_1<\dots<i_s\le r}Q_s(E_N) = \frac{1}{2^r}\sum_{s=1}^{r}\binom{r}{s}Q_s(E_N)
\end{aligned} \tag{2.5}$$

which proves (2.3).

Now let $\mathcal{A}=\{-1,+1\}^r$, $w=(a_{i_1},\dots,a_{i_\ell})\in\mathcal{A}^\ell$, $a_{i_j}=(\varepsilon_1^{(j)},\dots,\varepsilon_r^{(j)})$ and $D=(d_1,\dots,d_\ell)$. Then we have

$$\begin{aligned}
&g\big(\varphi(E_N),W,M,D\big)\\
&=\big|\big\{n:1\le n\le M,\ \big((e_{(n+d_1-1)r+1},\dots,e_{(n+d_1)r}),\dots,(e_{(n+d_\ell-1)r+1},\dots,e_{(n+d_\ell)r})\big)\\
&=\big((\varepsilon_1^{(1)},\dots,\varepsilon_r^{(1)}),\dots,(\varepsilon_1^{(\ell)},\dots,\varepsilon_r^{(\ell)})\big)\big\}\big|=\sum_{n=1}^{M}\prod_{i=1}^{r}\prod_{j=1}^{\ell}\frac{e_{(n+d_j-1)+i}\varepsilon_i^{(j)}+1}{2}\\
&=\frac{M}{2^{r\ell}}+\frac{1}{2^{r\ell}}\sum_{s=1}^{r}\sum_{q=1}^{\ell}\sum_{1\le i_1<\dots<i_s\le r}\ \sum_{1\le j_1<\dots<j_q\le\ell}\left(\prod_{\mu=1}^{s}\prod_{\nu=1}^{q}\varepsilon_{i_\mu}^{(j_\nu)}\right)\left(\sum_{n=1}^{M}\prod_{\mu=1}^{s}\prod_{\nu=1}^{q}e_{(n+d_{j_\nu}-1)r+i_\mu}\right)
\end{aligned}$$

so that, as in (2.5),

$$\begin{aligned}
&\left|g\big(\varphi(E_N),W,M,D\big)-\frac{M}{2^{r\ell}}\right|=\left|g\big(\varphi(E_N),W,M,D\big)-\frac{M}{k^\ell}\right|\\
&\le\frac{1}{2^r\ell}\sum_{s=1}^{r}\sum_{q=1}^{\ell}\sum_{1\le i_1<\dots<i_s\le r}\ \sum_{1\le j_1<\dots<j_q\le\ell}\big|Z\big(0,r,M-1,(d_{j_1}r+i_1,d_{j_1}r+i_2,\dots,d_{j_q}r+i_s)\big)\big|\\
&\le\frac{1}{2^{r\ell}}\sum_{s=1}^{r}\sum_{q=1}^{\ell}\sum_{1\le i_1<\dots<i_s\le r}\ \sum_{1\le j_1<\dots<j_q\le\ell}Q_{qs}(E_N)\\
&=\frac{1}{2^{r\ell}}\sum_{s=1}^{r}\sum_{q=1}^{\ell}\binom{r}{s}\binom{\ell}{q}Q_{qs}(E_N)
\end{aligned}$$

whence (2.4) follows and this completes the proof of Theorem 1.

Finally, we will make some comments on the applicability of the construction described at the beginning of this section. First, we remark that in certain applications this simple construction can be used even in the case when k, the number of the given symbols, is not a 2–power; the price paid is a slight data expansion. E.g., consider the following problem in cryptography: assume that a plaintext is given which uses, say, $k=80$ characters, and we want to encrypt it by using a PR sequence of letters taken from an alphabet of appropiate size as key. Then we consider the smallest 2–power $\ge$ the number of characters: $2^7>80$ ($>2^6$). Next to each of the characters we assign one of the 2^7 blocks of bits of length 7 taken from $\{0,1\}^7$, and we replace each character in the plaintext by the corresponding block from $\{0,1\}^7$, so that the plaintext is mapped into a sequence $a_1,a_2,\dots,a_M$ whose elements belong to $\{0,1\}^7$. Now by using the algorithm described above with $r=7$, we construct a PR sequence $b_1,b_2,\dots,b_M$ of letters from the alphabet $\mathcal{A}=\{0,1\}^7$ (whose size is 2–power: $|\mathcal{A}|=2^7$). Then we obtain the ciphertext $c_1,c_2,\dots,c_M$ by taking $c_i\in\{0,1\}^7$ as the residue of a_i+b_i modulo 2^7 (and to decipher $c_1,c_2,\dots,c_M$, we subtract b_i from c_i modulo 2^7).

A further remark on the limits of the applicability of this method: this algorithm can be applied only if N is “much greater”, than $k=2^r$. Indeed, N must grow at least as fast as a large power of k, otherwise the inequalities in Theorem 1 become trivial or say very little.

3 A construction in the general case

We will construct a large family of sequences of k symbols with a given length which has good PR properties (for any $k \in \mathbb{N}$, $k \geq 2$). This construction will be the generalization of the construction given in [6] in the $k = 2$ special case (however, it is much more difficult to control the general case presented here).

We will need three definitions.

Definition 1. A multiset is said to be a k–set if each element occurs with multiplicity less than k in it.

(So that a 2–set is a set whose elements are distinct, each occuring only once; in this case we will also call the set "simple set".)

Definition 2. If $k \in \mathbb{N}$, $k \geq 2$, $m \in \mathbb{N}$, $\mathcal{A}$ and $\mathcal{B}$ are multisets whose elements belong to $\mathbb{Z}_m$ (= the ring of the modulo m residue classes) and $\mathcal{A} + \mathcal{B}$ represents every element of $\mathbb{Z}_m$ with multiplicity divisible by k, i.e., for all $c \in \mathbb{Z}_m$, the number of solutions of

$$a + b = c, \ a \in \mathcal{A}, \ b \in \mathcal{B} \tag{3.1}$$

(the elements of $\mathcal{A}, \mathcal{B}$ counted with their multiplicity) is divisible by k (including the case when there are no solutions), then the sum $\mathcal{A} + \mathcal{B}$ is said to have property P_k.

Definition 3. If $k, h, \ell, m \in \mathbb{N}$, $k \geq 2$ and $h, \ell \leq m$, then (h, ℓ, m) is said to be a k–admissible triple if there is no simple set $\mathcal{A} \subset \mathbb{Z}_m$ and k–set $\mathcal{B}$ with elements from $\mathbb{Z}_m$ such that $|\mathcal{A}| = h$, $|\mathcal{B}| = \ell$ (multiple elements counted with their multiplicity), and $\mathcal{A} + \mathcal{B}$ possesses property P_k.

Definition 4. If $k, h, \ell, m \in \mathbb{N}$, $k \geq 2$ and $h, \ell \leq m$, then (h, ℓ, m) is said to be a (k, k)–admissible triple if there are no k–sets $\mathcal{A}, \mathcal{B}$ with elements from $\mathbb{Z}_m$ such that $|\mathcal{A}| = h$, $|\mathcal{B}| = \ell$ (multiple elements counted with their multiplicity), and $\mathcal{A} + \mathcal{B}$ possesses property P_k.

Note that in the $k = 2$ special case property P_2 is the property P introduced in [6], while both 2–admissibility and (2,2)–admissibility are the admissibility used there.

Theorem 2. *Assume that $k \in \mathbb{N}$, $k \geq 2$, p is a prime number, χ is a (multiplicative) character modulo p of order k (so that $k|(p-1)$, $f(x) \in F_p[x]$ (F_p being the field of the modulo p residue classes) has degree $h (> 0)$, $f(x)$ has no multiple zero in $\bar{F}_p$ (= the algebraic closure of E_p), and define the sequence $E_p = \{e_1, \dots, e_p\}$ on the k letter alphabet of the k–th (complex) roots of unity by*

$$e_n = \begin{cases} \chi\big(f(n)\big) & \text{for } \big(f(n), p\big) = 1 \\ +1 & \text{for } p \mid f(n). \end{cases}$$

Then

(i) we have

$$\delta(E_p) < 11 h p^{1/2} \log p, \tag{3.2}$$

(ii) if $\ell \in \mathbb{N}$ is such that the triple (r, t, p) is k–admissible for all $1 \le r \le h$, $1 \le t \le \ell(k-1)$, then

$$\gamma_\ell(E_p) < 10\ell hkp^{1/2}\log p. \tag{3.3}$$

Proof of Theorem 2. The proof of both (i) and (ii) will be based on

Lemma 1. *Assume that p is a prime number, χ is a non–principal character modulo p of order k, $f(x) \in F_p[x]$ has degree h and a factorization $f(x) = b(x-x_1)^{r_1}\dots(x-x_s)^{r_s}$ (where $x_i \ne x_j$ for $i \ne j$) in $\bar{F}_p$ with*

$$(k, r_1, \dots, r_s) = 1. \tag{3.4}$$

Let X, Y be real numbers with $0 < Y \le p$. Then

$$\left| \sum_{x<n\le X+Y} \chi\big(f(n)\big) \right| < 9sp^{1/2}\log p (\le 9hp^{1/2}\log p). \tag{3.5}$$

Proof of Lemma 1. With h in the upper bound in (3.5), this is Theorem 2 in [13] where we derived it from $\mathcal{A}$. Weil's theorem [17] (see also Lemma 1 and its proof in [6]). To see that (3.5) also holds in the slightly sharper form with the factor s in place of h, all we have to observe is that in the proof of Theorem 2 in [13], at a certain point (p. 374, line 6 from below) we majorized s by h; skipping this step we obtain (3.5) in the sharper form. (We are indebted to Igor Shparlinski for this observation.)

We will need Lemma 1 in the following slightly modified form:

Lemma 2. *The assertion of Lemma 1 also holds if assumption (3.4) is replaced by*

$$(k, r_1, \dots, r_s) < k \tag{3.6}$$

(i.e., there is an r_i with $k \nmid r_i$).

Note that this lemma is sharper than Lemma 3 in [14] since now $x_1, \dots, x_s \in F_p$ is not assumed.

Proof of Lemma 2. Write $\delta = (k, r_1, \dots, r_s)$ so that

$$\delta < k \tag{3.7}$$

by (3.6), and define the character χ_1 by $\chi_1 = \chi^\delta$; then by (3.7), χ_1 is a non–principal character. Write the polynomial $\varphi(x) = b^{-1}f(x) = (x-x_1)^{r_1}\dots(x-x_s)^{r_s} \in F_p[x]$ as the product of powers of distinct irreducible polynomials over F_p: $\varphi(x) = \big(\pi_1(x)\big)^{u_1}\dots\big(\pi_t(x)\big)^{u_t}$. Since irreducible polynomials cannot have multiple zeros, and distinct irreducible polynomials are coprime and thus cannot have a common zero, thus it follows that the exponents $u_1, \dots, u_t$ are amongst the exponents $r_1, \dots, r_s$ whence, by the definition of δ, we have $\delta \mid (u_1, \dots, u_t)$. Then writing $\psi(x) = \big(\pi(x)\big)^{u_1/\delta}\dots\big(\pi(x)\big)^{u_t/\delta}$, clearly we have $\psi(x) \in F_p[x]$ and

$$f(x) = b\varphi(x) = b\big(\psi(x)\big)^\delta.$$

It follows that

$$\left|\sum_{X<n\le X+Y}\chi\big(f(n)\big)\right| = |\chi(b)|\left|\sum_{X<n\le X+Y}\big(\chi\big(\psi(n)\big)\big)^{\delta}\right| \le \left|\sum_{X<n\le X+Y}\chi_1\big(\psi(n)\big)\right|. \tag{3.8}$$

To estimate this sum, we will apply Lemma 1. Indeed, χ_1 is of order k/δ, and clearly $\psi(x)$ has the factorization $\psi(x) = (x-x_1)^{r_1/\delta}\dots(x-x_s)^{r_s/\delta}$ in $\bar{F}_p$. Thus replacing χ and $f(x)$ in Lemma 1 by χ_1 and $\psi(x)$, condition (3.4) becomes

$$\left(\frac{k}{\delta},\frac{r_1}{\delta},\dots,\frac{r_s}{\delta}\right) = 1$$

which holds trivially by the definition of δ. Thus, indeed, Lemma 1 can be applied to estimate the last sum in (3.8), and applying it, we obtain the desired upper bound.

(i) If a is a k–th root of unity, then writing

$$S(a,m) = \frac{1}{k}\sum_{t=1}^{k}\big(\bar{a}\chi(m)\big)^{t}, \tag{3.9}$$

clearly we have

$$S(a,m) = \begin{cases} 1, & \text{if } \chi(m) = a \\ 0, & \text{if } \chi(m) \ne a. \end{cases} \tag{3.10}$$

If a is a k–th roof of unity, $u, v, M \in \mathbb{N}$ and

$$1 \le u \le u + (M-1)v \le p, \tag{3.11}$$

then we have

$$x(E_p, a, M, u, v) = \sum_{\substack{0\le j\le M-1 \\ e_{u+jv}=a}} 1 \tag{3.12}$$

where

$$\left|\sum_{\substack{0\le j\le M-1 \\ e_{u+jv}=a}} 1 - \sum_{\substack{0\le j\le M-1 \\ \chi(f(u+jv))=a}} 1\right| \le \sum_{\substack{0\le j\le M-1 \\ p\mid f(u+jv)}} 1. \tag{3.13}$$

By (3.9) and (3.10),

$$\sum_{\substack{0\le j\le M-1\\ \chi(f(u+jv))=a}} 1=\sum_{j=0}^{M-1} S\big(a,f(u+jv)\big)=\sum_{j=0}^{M-1}\frac{1}{k}\sum_{t=1}^{k}\big(\bar a\chi\big(f(u+jv)\big)\big)^t$$

$$=\frac{1}{k}\sum_{\substack{0\le j\le M-1\\ (f(u+jv),p)=1}} 1+\frac{1}{k}\sum_{t=1}^{k-1}\bar a^t\sum_{j=0}^{M-1}\chi^t\big(f(u+jv)\big)$$

$$=\frac{M}{k}-\frac{1}{k}\sum_{\substack{0\le j\le M-1\\ p\mid f(u+jv)}} 1+\frac{1}{k}\sum_{t=1}^{k-1}\bar a^t\sum_{j=0}^{M-1}\chi^t\big(f(u+jv)\big)$$

whence

$$\left|\sum_{\substack{0\le j\le M-1\\ \chi(f(u+jv))=a}} 1-\frac{M}{k}\right|\le\frac{1}{k}\sum_{t=1}^{k-1}\left|\sum_{j=0}^{M-1}\chi^t\big(f(u+jv)\big)\right|+\frac{1}{k}\sum_{\substack{0\le j\le M-1\\ p\mid f(u+jv)}} 1. \tag{3.14}$$

Writing $g(x)=f(u+xv)$, it follows from (3.12), (3.13) and (3.14) that

$$\left|x(E_p,a,M,u,v)-\frac{M}{k}\right|\le\frac{1}{k}\sum_{t=1}^{k-1}\left|\sum_{j=0}^{M-1}\chi^t\big(g(j)\big)\right|+2\sum_{\substack{0\le j\le M-1\\ p\mid g(j)}} 1. \tag{3.15}$$

The case $M=1$ is trivial, thus we may assume that $M>1$. Then by $v\ge 1$ and (3.11) we have $1\le v<p$ so that $(v,p)=1$. It follows that the polynomials $f(x),g(x)\in F_p[x]$ have the same degree, and since $f(x)$ does not have multiple zeros, thus $g(x)$ does not have multiple zeros either. Moreover, $\chi_1=\chi^t$ is also a character modulo p, and for $1\le t\le k-1$ the character χ_1 is different from the principal character χ_0. Thus by Lemma 1 we have

$$\left|\sum_{j=0}^{M-1}\chi^t\big(g(j)\big)\right|=\left|\sum_{j=0}^{M-1}\chi_1\big(g(j)\big)\right|<9hp^{1/2}\log p \text{ for } 1\le t\le k-1. \tag{3.16}$$

Since f and g are of the same degree thus

$$\sum_{\substack{0\le j\le M-1\\ p\mid g(j)}} 1\le\sum_{\substack{0\le j<p\\ p\mid g(j)}} 1\le h. \tag{3.17}$$

It follows from (3.15), (3.16) and (3.17) that

$$\left|x(E_p,a,M,u,v)-\frac{M}{k}\right|\le\frac{k-1}{k}\cdot 9hp^{1/2}\log p+2h<11hp^{1/2}\log p$$

which completes the proof of (3.2).

(ii) In order to prove (3.3), assume that $\ell \in \mathbb{N}$, $\ell \le N$, $b_1, \dots, b_\ell$ are k–th roots of unity, $w = (b_1, \dots, b_\ell)$, $D = (d_1, \dots, d_\ell)$, $0 \le d_1 < \dots < d_\ell$, $M \in \mathbb{N}$ and $M + d_\ell \le N$. Then

$$\begin{aligned} g(E_n, w, M, D) &= \big|\big\{n : 1 \le n \le M, (e_{n+d_1}, \dots, e_{n+d_\ell}) = w\big\}\big| \\ &= \big|\big\{n : 1 \le n \le M, e_{n+d_1} = b_1, \dots, e_{n+d_\ell} = b_\ell\big\}\big|. \end{aligned} \tag{3.18}$$

Here we have

$$e_{n+d_1} = \chi\big(f(n+d_1)\big), \dots, e_{n+d_\ell} = \chi\big(f(n+d_\ell)\big) \tag{3.19}$$

except for the n values such that

$$f(n+d_i) \equiv 0 \pmod p \text{ for some } 1 \le i \le \ell. \tag{3.20}$$

For fixed i, this congruence may have at most h solutions, and i may assume at most ℓ values. Thus the total number of solutions of (3.20) is $\le h\ell$. If n is not a solution of (3.20), then (3.19) holds, so that by (3.10), for all these n we have

$$\prod_{i=1}^{\ell} S\big(b_i, f(n+d_i)\big) = \begin{cases} 1 & \text{if } e_{n+d_1} = b_1, \dots, e_{n+d_\ell} = b_\ell \\ 0 & \text{otherwise.} \end{cases} \tag{3.21}$$

For the exceptional n values satisfying (3.20) (whose number is $\le h\ell$) again by (3.10) we have

$$\prod_{i=1}^{\ell} S\big(b_i, f(n+d_i)\big) = 0 \text{ or } 1. \tag{3.22}$$

It follows from (3.18), (3.21) and (3.22) that

$$\left| g(E_N, w, M, D) - \sum_{n=1}^{M} \prod_{i=1}^{\ell} S\big(b_i, f(n+d_i)\big) \right| \le h\ell \tag{3.23}$$

where we have

$$\begin{aligned} \sum_{n=1}^{M} \prod_{i=1}^{\ell} S\big(b_i, f(n+d_i)\big) &= \sum_{n=1}^{M} \prod_{i=1}^{\ell} \frac{1}{k} \sum_{t_i=1}^{k} \big(\bar{b}_i \chi\big(f(n+d_i)\big)^{t_i} \\ &= \frac{1}{k^\ell} \sum_{t_1=1}^{k} \cdots \sum_{t_\ell=1}^{k} \overline{b_1^{t_1} \dots b_\ell^{t_\ell}} \sum_{n=1}^{M} \chi\big(\big(f(n+d_1)^{t_1} \dots \big(f(n+d_\ell)\big)^{t_\ell}\big) \\ &= \frac{M}{k^\ell} + \frac{1}{k^\ell} \sum_{\substack{0 \le t_1, \dots, t_\ell \le k-1 \\ (t_1, \dots, t_\ell) \ne (0, \dots, 0)}} \cdots \sum \overline{b_1^{t_1} \dots b_\ell^{t_\ell}} \sum_{n=1}^{M} \chi\big(\big(f(n+d_1)\big)^{t_1} \dots \big(f(n+d_\ell)\big)^{t_\ell}\big). \end{aligned} \tag{3.24}$$

It follows from (3.23) and (3.24) that

$$\left| g(E_N, w, M, D) - \frac{M}{k^\ell} \right| \le \frac{1}{k^\ell} \sum_{\substack{0 \le t_1, \dots, t_\ell \le k-1 \\ (t_1, \dots, t_\ell) \ne (0, \dots, 0)}} \cdots \sum \left| \sum_{n=1}^{M} \chi\big(\big(f(n+d_1)\big)^{t_1} \dots \big(f(n+d_\ell)\big)^{t_\ell}\big) \right| + h\ell. \tag{3.25}$$

Write $f(x) = Bf_1(x)$ where $B \in \mathbb{Z}_p$ and $f_1(x) \in \mathbb{Z}_p[x]$ is a unitary polynomial, and set $G(x) = f_1(x+d_1)^{t_1} \dots f_1(x+d_\ell)^{t_\ell}$. Then the innermost sum in (3.25) can be rewritten in the following way:

$$\left| \sum_{n=1}^{M} \chi\big((f(n+d_1))^{t_1} \dots (f(n+d_\ell))^{t_\ell} \big) \right| = \left| \chi(B^{t_1+\dots+t_\ell}) \right| \left| \sum_{n=1}^{M} \chi\big(G(n)\big) \right| \le \left| \sum_{n=1}^{M} \chi\big(G(n)\big) \right|. \tag{3.26}$$

It suffices to show:

Lemma 3. *If k, f, h, ℓ are defined as in Theorem 2, then $G(x)$ has at least one zero (in $\bar{F}_p$) whose multiplicity is not divisible by k.*

Indeed, assuming that Lemma 3 has been proved, the proof of (3.3) can be completed in the following way: by Lemma 3, we may apply Lemma 2 with $G(x)$ in place of $f(x)$ (since then (3.6) holds by Lemma 3). The degree of $G(x)$ is clearly

$$ht_1 + \dots + ht_\ell \le \ell h(k-1) < \ell hk,$$

thus applying Lemma 2 we obtain

$$\left| \sum_{n=1}^{M} \chi\big(G(n)\big) \right| < 9\ell hkp^{1/2} \log p.$$

Each of the innermost sums in (3.25) can be estimated in this way. Thus it follows from (3.25) that

$$\left| g(E_N, w, M, D) - \frac{M}{k^\ell} \right| \le \frac{1}{k^\ell} \sum_{\substack{0 \le t_1, \dots, t_\ell \le k-1 \\ (t_1, \dots, t_\ell) \ne (0, \dots, 0)}} \cdots \sum 9\ell hkp^{1/2} \log p + h\ell < 10\ell hkp^{1/2} \log p$$

for all w, M, D which proves (3.3). Thus it remains to prove the lemma:

Proof of Lemma 3: We will say that the polynomials $\varphi(x), \psi(x) \in F_p[x]$ are equivalent: $\varphi \sim \psi$ if there is an $a \in F_p$ such that $\psi(x) = \varphi(x+a)$. Clearly, this is an equivalence relation.

Write $f_1(x)$ as the product of irreducible polynomials over F_p. It follows from our assumption on $f(x)$ that these irreducible factors are distinct. Let us group these factors so that in each group the equivalent irreducible factors are collected. Consider a typical group $\varphi(x+a_1), \dots, \varphi(x+a_r)$.

Then writing $G(x)$ as the product of irreducible polynomials over F_p, all the polynomials $\varphi(x+a_i+d_j)$ with $1 \le i \le r$, $1 \le j \le \ell$ occur amongst the factors, and for fixed i, j such a factor occurs t_j times. All these polynomials are equivalent, and no other irreducible factor belonging to this equivalence class will occur amongst the irreducible factors of $G(x)$.

Since irreducible polynomials have no multiple zeros and distinct irreducible polynomials cannot have a common zero, thus the conclusion of Lemma 3 fails, i.e., the multiplicity of each of the zeros of $G(x)$ is divisible by k, if and only if in each group, formed by equivalent irreducible factors $\varphi(x+a_i+d_j)$ of $G(x)$ each taken t_j times, every polynomial of form $\varphi(x+c)$ with $c \in F_p$ occurs with multiplicity divisible by k, i.e., the number of representation of c in the form a_i+d_j, counting this representation with multiplicity t_j, is divisible by k. In other words, if we write $\mathcal{A}=\{a_1,\dots,a_r\}$ and $\mathcal{B}$ denotes the k–set whose elements are $d_1,\dots,d_\ell$, each d_j taken with multiplicity $t_j \le k-1$, for each group $\mathcal{A}+\mathcal{B}$ must posses property P_k. Now consider any of these groups by $\deg f>0$ there is at least one such group). Since $\mathcal{A}+\mathcal{B}$ possesses property P_k, thus $(|\mathcal{A}|,|\mathcal{B}|,p)$ is **not** a k–admissible triple. Clearly here we have

$$|\mathcal{A}|=r\le \deg f_1=\deg f=h$$

and

$$|\mathcal{B}|=\sum_{j=1}^{\ell} t_j \le \ell(k-1)$$

which contradicts our assumption on ℓ. Thus the conclusion of Lemma 3 cannot fail, and this completes the proof.

4 The necessity of the k–admissibility

Upper bound (3.3) in Theorem 2 is proved assuming certain k–admissibility, and the study of k–admissibility is a difficult problem (we will return to it in the next sections). Thus Theorem 2 could be applied more easily without this assumption, so that one might like to know whether this assumption is really necessary, or it can be dropped? Next we will show that, subject to certain mild conditions on the parameters involved, any negative example with a sum $\mathcal{A}+\mathcal{B}$ ($\mathcal{A}$ simple set, $\mathcal{B}$ k–set) having property P_k induces a construction of the type described in Theorem 2 with the property that conclusion (3.3) fails, i.e., certain correlation is large. (Sums $\mathcal{A}+\mathcal{B}$ of this type will be constructed later in Section 6.)

Assume that $k\in\mathbb{N}$, $k\ge 2$, p is a prime, $\mathcal{A}=\{a_1,\dots,a_r\}\subset\{0,1,\dots,p-1\}$, $\mathcal{B}$ is a k–set with elements from $\{0,1,\dots,p-1\}$, $|\mathcal{A}|=r<p$, $|\mathcal{B}|=t<p$, the distinct elements of $\mathcal{B}$ are $d_1,\dots,d_\ell$, their multiplicities are $t_1,\dots,t_\ell$ ($1\le t_i\le k-1$), and $\mathcal{A}+\mathcal{B}$ has property P_k. Set $f(n)=(n+a_1)\dots(n+a_r)$, and define the sequence $E_p=\{e_1,\dots,e_p\}$ in the same way as in Theorem 2. Set $M=p-d_\ell$. We claim that assuming also

$$p\to\infty,$$

$$M=p-d_\ell \gg p \tag{4.1}$$

and

$$r\ell=o(p), \tag{4.2}$$

γ_ℓ cannot be "small":

$$|\gamma_\ell(E_p)|\ne o\left(\frac{p}{k^\ell}\right). \tag{4.3}$$

Consider the sum

$$S_M = \sum_{n=1}^{M} e_{n+d_1}^{t_1} \dots e_{n+d_\ell}^{t_\ell}.$$

Here we have

$$e_{n+d_j}^{t_j} = \big(\chi\big(f(n+d_j)\big)\big)^{t_j} = \chi\left(\prod_{i=1}^{r}(n+a_i+d_j)^{t_j}\right)$$

except for n, j such that

$$n + a_i + d_j \equiv 0 (\mathrm{mod}\ p) \text{ for some } 1 \le i \le r. \tag{4.4}$$

If n is such that there are no i (with $1 \le i \le r$), j satisfying (4.4), then we have

$$e_{n+d_1}^{t_1} \dots e_{n+d_\ell}^{t_\ell} = \chi\left(\prod_{j=1}^{\ell}\prod_{i=1}^{r}(n+a_i+d_j)^{t_j}\right) = \chi\left(\prod_{c\in\mathcal{A}+\mathcal{B}}(n+c)\right). \tag{4.5}$$

Here every $c \in \mathcal{A}+\mathcal{B}$ is counted as many times as the number of solutions of

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

where the d's are counted with their multiplicity; for fixed $c \in \mathbb{Z}_p$, denote the number of solutions of this equation by $\varphi(c)$ (for $c \notin \mathcal{A}+\mathcal{B}$ we set $\varphi(c) = 0$). Then (4.5) can be rewritten as

$$e_{n+d_1}^{t_1} \dots e_{n+d_\ell}^{t_\ell} = \prod_{\substack{c\in\mathbb{Z}_p \\ f(c)\neq 0}} \big(\chi(n+c)\big)^{\varphi(c)}.$$

Since $\mathcal{A}+\mathcal{B}$ possesses property P_k, thus $k \mid \varphi(c)$ for all $c \in \mathbb{Z}_p$, and we assumed that $n+c \neq 0$ if $\varphi(c) \neq 0$. Since χ is a character of order k, it follows that

$$e_{n+d_1}^{t_1} \dots e_{n+d_\ell}^{t_\ell} = \prod_{\substack{c\in\mathbb{Z}_p \\ \varphi(c)\neq 0}} \big(\chi^k(n+c)\big)^{\varphi(c)/k} = \prod_{\substack{c\in\mathbb{Z}_p \\ \varphi(c)\neq 0}} 1 = 1$$

for every n for which (4.4) has no solution in i, j. In (4.4) the pair (i, j) can be chosen in $r\ell$ ways, and (i, j) determine n uniquely. Thus we have

$$|S_M - M| < r\ell. \tag{4.6}$$

On the other hand, assume that contrary to (4.3), we have

$$|\gamma_\ell(E_p)| = o\left(\frac{p}{k^\ell}\right)$$

so that, denoting the set of the k–th roots of unity by $\mathcal{A}$, for every ℓ–tuple $w = (\varepsilon_1, \dots, \varepsilon_\ell) \in \mathcal{A}^\ell$ we have

$$g(E_p, w, M, D) = \frac{M}{k^\ell} + o\left(\frac{p}{k^\ell}\right).$$

It follows that

$$\begin{aligned} S_M &= \sum_{(\varepsilon_1,\dots,\varepsilon_\ell)\in\mathcal{A}^\ell} g\big(E_p,(\varepsilon_1,\dots,\varepsilon_\ell),M,(d_1,\dots,d_\ell)\big)\varepsilon_1^{t_1}\dots\varepsilon_\ell^{t_\ell} \\ &= \frac{M}{k^\ell}\sum_{(\varepsilon_1,\dots,\varepsilon_\ell)\in\mathcal{A}^\ell} \varepsilon_1^{t_1}\dots\varepsilon_\ell^{t_\ell} + o\left(\frac{p}{k^\ell}\sum_{(\varepsilon_1,\dots,\varepsilon_\ell)\in\mathcal{A}^\ell} 1\right). \end{aligned}$$

By $1 \le t_i \le k-1$, the first sum is 0. Thus we have

$$S_M = o(p)$$

which contradicts (4.1), (4.2) and (4.6), and this completes the proof of our claim.

5 Concluding remarks

We have just shown that the assumption on the k–admissibility in Theorem 2 cannot be dropped. Thus in order to be able to use the construction in Theorem 2, we need criteria for a triple (r,t,p) being k–admissible. We will present sufficient criteria of this type in Part II. The complexity of the family constructed by us will be also studied there. Finally we estimate the cardinality of a smallest family achieving a prescribed f–complexity by extending the result of [4] from binary to k–ary alphabets. Somewhat surprisingly we also improve the earlier results by establishing a uniformity property.

References

[1] R. Ahlswede, Coloring hypergraphs: A new approach to multi–user source coding, Part I, J. Combinatorics, Information and System Sciences 4(1), 76–115, 1979; Part II, J. Combinatorics, Information and System Sciences 5(3), 220–268, 1980.

[2] R. Ahlswede, On concepts of performance parameters for channels, to appear in this book.

[3] R. Ahlswede and A. Winter, Strong converse for identification via quantum channels, IEEE Trans. on Inf. Theory, Vol. 48, No. 3, 569–579, 2002.

[4] R. Ahlswede, L.H. Khachatrian, C. Mauduit and A. Sárközy, A complexity measure for families of binary sequences, Periodica Math. Hungar., to appear.

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

[6] L. Goubin, C. Mauduit and A. Sárközy, Construction of large families of pseudo–random binary sequences, J. Number Theory, to appear.

[7] H. Halberstam and H.-E. Richert, Sieve Methods, Academic Press, London, 1974.

[8] D.R. Heath–Brown, Artin's conjecture for primitive roots, Quarterly J. Math. 37, 27–38, 1986.

[9] C. Hooley, On Artin's conjecture, J. reine angew. Math. 226, 209–220, 1967.

[10] Y. Kohayakawa, C. Mauduit, C.G. Moreira and V. Rödl, Measures of pseudorandomness for random sequences, preprint.

[11] R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications, revised edition, Cambridge University Press, 1994.

[12] C. Mauduit, J. Rivat and A. Sárközy, Construction of pseudorandom binary sequences using additive characters, Monatshefte Math., to appear.

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

[14] C. Mauduit and A. Sárközy, On finite pseudorandom sequences of k symbols, Indag. Mathem. 13, 89–101, 2002.

[15] A. Schinzel, Remarks on the paper "Sur certaines hypothéses concernant les nombres premiers", Acta Arith. 7, 1–8, 1961/1962.

[16] A. Schinzel and W. Sierpiński, Sur certaines hypothéses concernant les nombres premiers, ibid. 4, 185–208, 1958; Corrigendum ibid. 5, 259, 1959.

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