On a fast version of a pseudorandom generator

Katalin Gyarmati*

Abstract

In an earlier paper I constructed a large family of pseudorandom sequences by using the discrete logarithm. While the sequences in this construction have strong pseudorandom properties, they can be generated very slowly since no fast algorithm is known to compute ind n. The purpose of this paper is to modify this family slightly so that the members of the new family can be generated much faster, and they have almost as good pseudorandom properties as the sequences in the original family.

1 Introduction

In this work I will continue the work initiated in [5]. C. Mauduit and A. Sárközy [9, pp. 367-370] introduced the following measures of

*Research partially supported by Hungarian Scientific Research Grants OTKA T043631 and T043623.

pseudorandomness:

For a finite binary sequence $E_N = \{e_1, e_2, \ldots, e_N\} \in \{-1, +1\}^N$ write

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

and, for $D = (d_1, \ldots, d_k)$ with non-negative integers $d_1 < \cdots < d_k$,

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

Then the *well-distribution measure* of E_N is defined as

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

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

$$C_k(E_N) = \max_{M,D} |V(E_N, M, D)| = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2}, \ldots e_{n+d_k} \right|,$$

where the maximum is taken over all $D = (d_1, d_2, \ldots, d_k)$ and M such that $M + d_k \leq N$. In [6] I introduced a further measure: Let

$$H(E_N, a, b) = \sum_{j=0}^{[(b-a)/2]-1} e_{a+j} e_{b-j},$$

and then the *symmetry measure* of E_N is defined as

$$S(E_N) = \max_{1 \leq a < b \leq N} |H(E_N, a, b)| = \max_{1 \leq a < b \leq N} \left| \sum_{j=0}^{[(b-a)/2]-1} e_{a+j} e_{b-j} \right|.$$

A sequence E_N is considered as a "good" pseudorandom sequence if each of these measures $W(E_N)$, $C_k(E_N)$ (at least for small k) and

$S(E_N)$ is "small" in terms of N (in particular all are $o(N)$ as $N \longrightarrow \infty$). Indeed, it was proved in [3, Theorem 1, 2] and in [6, Theorem 1, 2] that for a truly random sequence $E_N \subseteq \{-1,+1\}^N$ each of these measures is $\ll \sqrt{N \log N}$ and $\gg \sqrt{N}$.

Throughout the paper we will use the following notations: $\| x \|$ is the distance of x from the closest integer, $e(\alpha) = e^{2\pi i \alpha}$, $\overline{\mathbb{F}_p}$ is the algebraic closured of the field $\mathbb{F}_p$. Finally, if p is a prime, α and m are natural numbers we say that $p^\alpha \parallel m$ if $p^\alpha \mid m$ but $p^{\alpha+1} \nmid m$.

Numerous binary sequences have been tested for pseudorandomness by J. Cassaigne, S. Ferenczi, C. Mauduit, J. Rivat and A. Sárközy. The sequences with the strongest pseudorandom properties have been constructed in [4], [5], [9], [11] and [13]. As concerning the strength of the pseudorandom properties these constructions are nearly equally good. But in the construction given by A. Sárközy in [13] and extended by me in [5], the generation of the sequences in question is much more slowly than in the other constructions. Indeed Sárközy's construction is the following:

Let p be an odd prime, $N = p-1$ and define $E_N = \{e_1, \dots, e_N\} \subseteq \{-1,+1\}^N$ by

$$e_n = \begin{cases} +1 & \text{if } 1 \le \text{ind } n \le \frac{p-1}{2}, \\ -1 & \text{if } \frac{p+1}{2} \le \text{ind } n \le p-1. \end{cases} \tag{1}$$

Here ind n denotes the index or discrete logarithm of n modulo p, defined as the unique integer with

$$g^{\text{ind } n} \equiv n \pmod{p}, \tag{2}$$

and $1 \leq \text{ind } n \leq p-1$, where g is a fixed primitive root modulo p. In [5] I extended this construction to a large family of binary sequences with strong pseudorandom properties by replacing n by a polynomial $f(n)$ in (1) (in the same way as the Legendre symbol construction in [9] was extended in [4].)

Indeed in [5] I proved for the generalized sequence:

Theorem A *For all $f \in \mathbb{F}_p[x]$ with $k = \deg f$ we have*

$$W(E_{p-1}) \leq 38kp^{1/2}(\log p)^2.$$

Moreover if one of the following conditions holds:

a) *f is irreducible;*

b) *If f has the factorization $f = \varphi_1^{\alpha_1}\varphi_2^{\alpha_2}\dots\varphi_u^{\alpha_u}$, where $\alpha_i \in \mathbb{N}$ and the φ_i's are irreducible over $\mathbb{F}_p$, then there exists a β such that exactly one or two φ_i's have the degree β;*

c) *$\ell = 2$;*

d) *$(4\ell)^k < p$ or $(4k)^\ell < p$.*

Then

$$C_\ell(E_{p-1}) < 10k\ell 4^\ell p^{1/2}(\log p)^{\ell+1}.$$

Finally, if $f(x) \not\equiv f(t-x)$ for all $t \in \mathbb{Z}_p$, then

$$S(E_{p-1}) < 88kp^{1/2}(\log p)^3.$$

As we pointed out earlier these constructions are nearly as good as the others, but the problem is that it is slow to compute e_n since

no fast algorithm is known to compute ind n. The Diffie-Hellman key-exchange system utilizes the difficulty of computing ind n.

In this paper my goal is to improve on the construction in Theorem A by replacing the sequence

$$e_n = \begin{cases} +1 & \text{if } 1 \leq \text{ind } f(n) \leq \frac{p-1}{2}, \\ -1 & \text{if } \frac{p+1}{2} \leq \text{ind } f(n) \leq p-1 \text{ or } p \mid f(n) \end{cases} \tag{3}$$

by a sequence which can be generated faster. I will show that this is possible at the price of giving slightly weaker upper bounds for the pseudorandom measures. Throughout this paper we will use the following:

Notation *Let p be an odd prime, g be a primitive root modulo p. Define* ind n *by* (2). *Let $f \in \mathbb{F}_p[x]$ be a polynomial of degree $k \geq 1$, and $f = ch^d$ where $c \in \mathbb{F}_p$ and $h \in \mathbb{F}_p[x]$ is not a perfect power of a polynomial over $\mathbb{F}_p[x]$. Moreover let*

$$m \mid p-1$$

with $m \in \mathbb{N}$, and let x be relative prime to m: $(x, m) = 1$.

The crucial idea of the construction is to reduce ind n modulo m:

Construction 1 *Let* ind$^*n$ *denote the following function: For all* $1 \leq n \leq p-1$

$$\text{ind } n \equiv x \cdot \text{ind}^* n \pmod{m}$$

*(*ind$^*n$ *exists since* $(x, m) = 1$.*)* *Define the sequence* $E_{p-1} =$

$\{e_1, \ldots, e_{p-1}\}$ *by*

$$e_n = \begin{cases} +1 & \text{if } 1 \leq \mathrm{ind}^* f(n) \leq \frac{m}{2}, \\ -1 & \text{if } \frac{m}{2} < \mathrm{ind}^* f(n) \leq m \text{ or } p \mid f(n). \end{cases} \tag{4}$$

Note that this construction also generalizes the Legendre symbol construction described in [4] and [9]. Indeed in the special case $m = 2,\ x = 1$ the sequence e_n defined in (4) becomes

$$e_n = \begin{cases} +1 & \text{if } \left(\frac{f(n)}{p}\right) = -1, \\ -1 & \text{if } \left(\frac{f(n)}{p}\right) = 1 \text{ or } p \mid f(n). \end{cases}$$

(In the special case $m = p-1,\ x = 1$ we obtain the original construction given in (3)).

We will show that the construction presented above has good pseudorandom properties, each of the measures $W(E_{p-1}),\ C_k(E_{p-1})$ is small under certain conditions on the polynomial f. In the case of the well-distribution measure we can control the situation completely.

Theorem 1 *If $m/(m,d)$ is even we have*

$$W(E_{p-1}) \leq 36kp^{1/2} \log p \log(m+1).$$

While in the other case, when $m/(m,d)$ is odd we have:

$$W(E_{p-1}) = \frac{p-1}{m} + O(kp^{1/2} \log p \log(m+1)).$$

In the case of the correlation measures the situation is slightly more difficult. When the order of the correlation measure is odd we have:

Theorem 2 *If $f \in \mathbb{F}_p$, $k = \deg f$ and ℓ are odd integers while m is an even integer, then we have*

$$C_\ell(E_{p-1}) < 9k\ell 4^\ell p^{1/2}(\log p)^{\ell+1}.$$

Otherwise we need the same conditions on the polynomial f as in [5] in the original construction. If the degree of the polynomial is small depending on m, the same upper bound holds as in [5], while in the general case I will prove a slightly weaker result.

Theorem 3 *i) Suppose that m is even or m is odd with $2m \mid p-1$, and at least one of the following 4 conditions holds:*

a) *f is irreducible;*

b) *If f has the factorization $f = \varphi_1^{\alpha_1}\varphi_2^{\alpha_2}\dots\varphi_u^{\alpha_u}$ where $\alpha_i \in \mathbb{N}$ and the φ_i's are irreducible over $\mathbb{F}_p$, then there exists a β such that exactly one or two φ_i's have the degree β;*

c) *$\ell = 2$;*

d) *$(4\ell)^k < p$ or $(4k)^\ell < p$.*

Then

$$C_\ell(E_{p-1}) < 9k\ell 4^\ell p^{1/2}(\log p)^{\ell+1} + \frac{\ell! k^{\ell(\ell+1)}}{m^\ell} p. \tag{5}$$

ii) Moreover if we also have $2^\beta \parallel m$ and $k = \deg f < 2^\beta$ then

$$C_\ell(E_{p-1}) < 9k\ell 4^\ell p^{1/2}(\log p)^{\ell+1}.$$

For fixed m by Heath-Brown's work on Linnik's theorem [7] the least prime number p with $m \mid p-1$ is less than $cm^{5.5}$. Thus the condition $\deg f < 2^\beta \parallel m \mid p-1$ is not too restrictive.

If $m^{2\ell} \gg p$ holds, then the first term majorizes the second term in (5), thus the upper bound becomes $O\left(p^{1/2}(\log p)^{\ell+1}\right)$ where the implied constant factor may depend on k and ℓ.

The study of the symmetry measure also considered in [5] would lead to further complications and I could control it only under the further assumption $\deg f \le 2^{\beta+2}$ where β is defined by $2^\beta \parallel m$. Thus, I do not go into the details of this here.

In applications one should balance between the strength of the upper bounds and the speed of the generation of the sequence depending on our priorities. By the Pohlig-Hellman [12] algorithm we will show in section 3 that the sequence described in (4), in particular $\mathrm{ind}\, {}^*f(n)$, can be computed faster than the original construction. Indeed, if the prime factors of m are smaller than $\log p$ then $\mathrm{ind}^* f(n)$ can be computed by $O((\log p)^6)$ bit operations.

In [2] R. Ahlswede, L.H. Khachatrian, C. Mauduit and A. Sárközy introduced the notion of f-complexity of families of binary sequences as a measure of applicability of the constructions in cryptography.

Definition 1 *The complexity $C(\mathcal{F})$ of a family $\mathcal{F}$ of binary sequence $E_N \in \{-1,+1\}^N$ is defined as the greatest integer j so that for any $1 \le i_1 < i_2 < \cdots < i_j \le N$, and for $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_j$, we have at least one*

$E_N = \{e_1, \ldots, e_N\} \in \mathcal{F}$ *for which*

$$e_{i_1} = \varepsilon_1,\ e_{i_2} = \varepsilon_2, \ldots, e_{i_j} = \varepsilon_j.$$

We will see that the f-complexity of the family constructed in (4) is high.

Theorem 4 *Consider all the polynomials* $f \in \mathbb{F}_p[x]$ *with*

$$0 < \deg f \leq K.$$

For each of these polynomials f*, consider the binary sequence* $E_{p-1} = E_{p-1}(f)$ *defined by* (4)*, and let* $\mathcal{F}$ *denote the family of all binary sequences obtained in this way. Then we have*

$$C(\mathcal{F}) > K.$$

In [10] C. Mauduit and A. Sárközy proved an inequality involving the pseudorandom measures W and C_2. The following is a generalization of their inequality:

Theorem 5 *For all* $E_N \in \{-1, +1\}^N$, $3\ell^2 \leq N$ *we have*

$$W(E_N) \leq 3\ell N^{1-1/(2\ell)} \left(C_{2\ell}(E_N)\right)^{1/(2\ell)}.$$

Here the constant factor 3ℓ could be improved by using a more difficult argument, I will return to this in a subsequent paper.

In section 4 we will prove Theorem 5 and using Theorems 1,2 and 3 we will show that Construction 1 provides a natural example for that the inequality in Theorem 5 is the best possible apart from

a constant factor. Moreover, Construction 1 gives us a sequence for which the correlation measures of small order are small while the well-distribution measure is possibly large.

2 Proofs

2.1 Proof of Theorem 1.

First we note that the sequence defined in (4) by the polynomial $f = h^d$ and the modulus m, remains the same sequence if we replace in Construction 1 the polynomial $f = h^d$ by the polynomial $h^{d/(m,d)}$ and the modulus m by the modulus $m/(m,d)$. Thus in order to prove this theorem it is sufficient to study the case when $(m,d) = 1$.

The proof of the theorem is very similar to the proof of Theorem 1 in [6]. By the formula

$$\frac{1}{m}\sum_{\chi:\chi^m=1}\overline{\chi}^j(a)\chi(b) = \begin{cases} 1 & \text{if } m \mid \text{ind } a - \text{ind } b, \\ 0 & \text{if } m \nmid \text{ind } a - \text{ind } b, \end{cases}$$

we obtain

$$e_n = 2 \sum_{\substack{1\le j\le m/2 \\ jx\equiv \text{ind } f(n) \pmod m}} 1 - 1 = \frac{2}{m}\sum_{1\le j\le m/2}\sum_{\chi:\chi^m=1}\overline{\chi}(f(n))\chi(g^{jx}) - 1.$$

Thus

$$e_n = \frac{2}{m}\sum_{1\le j\le m/2}\sum_{\chi\neq\chi_0:\chi^m=1}\overline{\chi}(f(n))\chi(g^{xj}) + \frac{(-1)^m - 1}{2m}. \qquad (6)$$

Assume now that $1 \le a \le a + (t-1)b \le N$. Then we have

$$|U(E_{p-1}, t, a, b)| = \left| \frac{2}{m} \sum_{\chi \neq \chi_0 : \chi^m = 1} \left(\sum_{i=0}^{t-1} \overline{\chi}(f(a+ib)) \right) \left(\sum_{j=1}^{[m/2]} \chi^j(g^x) \right) + \frac{((-1)^m - 1)t}{2m} \right|. \quad (7)$$

We will prove the following:

$$S \stackrel{\text{def}}{=} \left| \frac{1}{m} \sum_{\chi \neq \chi_0 : \chi^m = 1} \left(\sum_{i=0}^{t-1} \overline{\chi}(f(a+ib)) \right) \left(\sum_{j=1}^{[m/2]} \chi^j(g^x) \right) \right|$$
$$\le 18kp^{1/2}(\log p)^2. \quad (8)$$

If m is even we obtain the statement of Theorem 1 immediately from (7) and (8). If m is odd using the triangle inequality we get

$$|U(E_{p-1}, t, a, b)| = \frac{t}{m} + O(kp^{1/2}(\log p)^2)$$

which completes the proof of Theorem 1. Thus in order to prove Theorem 1, we have to verify (8).

We will use the following lemma:

Lemma 1 *Suppose that p is a prime, χ is a non-principal character modulo p of order z, $f \in \mathbb{F}_p[x]$ has s distinct roots in $\overline{F}_p$, and it is not a constant multiple of a z-th power of a polynomial over $\mathbb{F}_p$. Let y be a real number with $0 < y \le p$. Then for any $x \in \mathbb{R}$:*

$$\left| \sum_{x < n \le x+y} \chi(f(n)) \right| < 9sp^{1/2} \log p.$$

Poof of Lemma 1

This is a trivial consequence of Lemma 1 in [1]. Indeed, there this result is deduced from Weil theorem, see [14].

Consider $\sum_{i=0}^{t-1} \overline{\chi}(f(a+ib))$ in (7), and here, let the order of χ be z. Since $\chi^m = 1$ we have $z \mid m$. On the other hand $f = ch^d$ is not a constant multiple of a z-th power of a polynomial over $\mathbb{F}_p$, since $1 = (m, d) = (z, d)$ (because of $z \mid m$) and h is not a perfect power of any polynomial over $\mathbb{F}_p$.

Using Lemma 1 we have:

$$\left| \sum_{i=0}^{t-1} \overline{\chi}(f(a+ib)) \right| \leq 9kp^{1/2} \log p$$

and thus by (8)

$$S \leq \frac{9kp^{1/2} \log p}{m} \sum_{\chi \neq \chi_0 : \chi^m = 1} \left| \sum_{j=1}^{[m/2]} \chi^j(g^x) \right|.$$

Lemma 2

$$\sum_{\chi \neq \chi_0 : \chi^m = 1} \left| \sum_{j=1}^{[m/2]} \chi^j(g^x) \right| \leq \sum_{\chi \neq \chi_0 : \chi^m = 1} \frac{2}{|1 - \chi(g^x)|} < 2m \log(m+1).$$

Proof of Lemma 2 This is Lemma 3 in [5] with m in place of d, $m/2$ in place of $(p-1)/2$ and g^x in place of g, respectively, and it can be proved in the same way.

Using Lemma 2 we obtain

$$S < 18kp^{1/2} \log p \log(m+1)$$

which proves (8) and this completes the proof of Theorem 1.

2.2 Proof of Theorem 2 and 3

In this section we may suppose that m is even: In Theorem 2 m cannot be odd. If m is odd in Theorem 3, then considering $2m$ in

place of m and f^2 in place of f in Construction 1 we generate the same sequence; however in this case we have $(2m, 2d) > 1$.

To prove Theorems 2 and 3, consider any $\mathcal{D} = \{d_1, d_2, \ldots, d_\ell\}$ with non-negative integers $d_1 < d_2 < \cdots < d_\ell$ and positive integers M with $M + d_\ell \leq p - 1$. Then arguing as in [13, p. 382] with $f(n + d_j)$ in place of $n + d_j$, m in place of $p - 1$, and g^x in place of g from (6) and since m is even we obtain:

$$|V(E_N, M, D)| \leq \frac{2^\ell}{m^\ell} \sum_{\substack{\chi_1 \neq \chi_0 \\ \chi_1^m = 1}} \cdots \sum_{\substack{\chi_\ell \neq \chi_0 \\ \chi_\ell^m = 1}} \left| \sum_{n=1}^{M} \chi_1(f(n + d_1)) \cdots \chi_\ell(f(n + d_\ell)) \right| \times \prod \left| \sum_{\ell_j = 1}^{m/2} \overline{\chi}_j(g^{x\ell_j}) \right|. \tag{9}$$

Now let χ be a modulo p character of order m; for simplicity we will choose χ as the character uniquely defined by $\chi(g) = e\left(\frac{x^*}{m}\right)$ where $xx^* \equiv 1 \pmod{m}$. Then

$$\chi(g^x) = e\left(\frac{1}{m}\right). \tag{10}$$

Let $\chi_u = \chi^{\delta_u}$ for $u = 1, 2, \ldots, \ell$, whence by $\chi_1 \neq \chi_0, \ldots, \chi_\ell \neq \chi_0$, we may take

$$1 \leq \delta_u < m.$$

Thus in (9) we have

$$\begin{aligned} &\left| \sum_{n=1}^{M} \chi_1(f(n + d_1)) \ldots \chi_\ell(f(n + d_\ell)) \right| \\ &= \left| \sum_{n=1}^{M} \chi^{\delta_1}(f(n + d_1)) \ldots \chi^{\delta_\ell}(f(n + d_\ell)) \right| \\ &= \left| \sum_{n=1}^{M} \chi\left(f^{\delta_1}(n + d_1) \ldots f^{\delta_\ell}(n + d_\ell)\right) \right|. \end{aligned}$$

If $f^{\delta_1}(n+d_1)\cdots f^{\delta_\ell}(n+d_\ell)$ is not a perfect m-th power, then this sum can be estimated by Lemma 1, whence

$$\left|\sum_{n=1}^{M}\chi(f^{\delta_1}(n+d_1)\cdots f^{\delta_\ell}(n+d_\ell))\right| \le 9s\ell p^{1/2}\log p.$$

Therefore by (9) and the triangle-inequality we get:

$$\begin{aligned}|V(E_N,M,D)| &\le \frac{2^\ell}{m^\ell}\sum_{\substack{\chi_1\neq\chi_0\\ \chi_1^m=1}}\cdots\sum_{\substack{\chi_\ell\neq\chi_0\\ \chi_\ell^m=1}} 9s\ell p^{1/2}\log p\left|\prod_{j=1}^{\ell}\left(\sum_{l_j=1}^{m/2}\chi^{\delta_j}(g^{x\ell_j})\right)\right| \\ &+ \frac{2^\ell}{m^\ell}\sum_{\substack{1\le\delta_1,\dots,\delta_\ell<m,\\ f^{\delta_1}(n+d_1)\cdots f^{\delta_\ell}(n+d_\ell)\text{ is}\\ \text{a perfect } m\text{-th power}}}(p-1)\left|\prod_{j=1}^{\ell}\left(\sum_{l_j=1}^{m/2}\chi^{\delta_j}(g^{x\ell_j})\right)\right| \\ &= \sum\nolimits_1+\sum\nolimits_2. \end{aligned} \tag{11}$$

From Lemma 2 the same way as in [13, p.384] we have

$$\sum\nolimits_1 \le 9k\ell 4^\ell p^{1/2}(\log p)^{\ell+1}. \tag{12}$$

It remains to estimate $\sum_2$. First we claim that in Theorem 2 and in Theorem 3 (ii) we have $\sum_2 = 0$.

Indeed in these cases I will show that if $f^{\delta_1}(n+d_1)\dots f^{\delta_\ell}(n+d_\ell)$ is a perfect m-th power, then there exists a δ_i which is even. Then, if δ_i is even, by (10) and $m\nmid\delta_i$ $(1\le\delta_i\le m-1)$ we have

$$\sum_{\ell_j=1}^{m/2}\chi^{\delta_i}(g^{x\ell_j}) = \sum_{\ell_j=1}^{m/2} e\left(\frac{\delta_i/2}{m/2}\ell_j\right) = 0,$$

which means that in $\sum_2$ the product is 0, whence $\sum_2 = 0$. From this, (11) and (12) Theorem 2 and 3 (ii) follows.

Let us see the proof of those cases for which all δ_i's are odd. In the case of Theorem 2 if $f^{\delta_1}(n+d_1)\cdots f^{\delta_\ell}(n+d_\ell)$ is a perfect m-th

power, then m divides the degree of $f^{\delta_1}(n+d_1)\cdots f^{\delta_\ell}(n+d_\ell)$ which is $k(\delta_1+\cdots+\delta_\ell)$. If k and ℓ are also odd we get that $k(\delta_1+\cdots+\delta_\ell)$ is odd, which contradicts $2 \mid m \mid k(\delta_1+\cdots+\delta_\ell)$. In the case of Theorem 3 (ii) we will use the following lemma, which is Lemma 5 of [5] with m in place of $p-1$.

Lemma 3 *Suppose that the conditions of Theorem 3 hold. Then if* $1 \le \delta_1, \ldots, \delta_\ell \le m-1$, *and* $f^{\delta_1}(n+d_1)\cdots f^{\delta_\ell}(n+d_\ell)$ *is a perfect* m*-th power, then there is a* δ_i *(*$1 \le i \le \ell$*) and an integer* $1 \le \alpha \le k$ *such that* $m \mid \alpha\delta_i$.

By Lemma 3 we have

$$m \mid \alpha\delta_i,$$
$$\frac{m}{(m,\alpha)} \mid \delta_i.$$

By the conditions of Theorem 3 we have $2^\beta \parallel m$ and $k < 2^\beta$. Thus $(m,\alpha) \le \alpha \le k < 2^\beta$. Therefore $2 \mid \frac{m}{(m,\alpha)}$, whence δ_i is even. This completes the proof of Theorem 2 and Theorem 3 (ii).

In order to prove Theorem 3 (i) we need a generalization of Lemma 3. This is the following:

Lemma 4 *Suppose that the conditions of Theorem 3 (i) hold. If* $1 \le \delta_1, \ldots, \delta_\ell \le m-1$ *and* $f^{\delta_1}(n+d_1)\cdots f^{\delta_\ell}(n+d_\ell)$ *is a perfect* m*-th power, then there is a permutation* $(\rho_1, \ldots, \rho_\ell)$ *of* $(\delta_1, \ldots, \delta_\ell)$ *such that for all* $1 \le i \le \ell$ *there exists an* α_i *with* $1 \le \alpha_i \le k^i$ *and*

$$m \mid \alpha_i\rho_i.$$

We postpone the proof of Lemma 4. Now, from this lemma we verify that $\sum_2 \leq \frac{\ell! k^{\ell(\ell+1)}}{m^\ell} p$. Consider a fixed ℓ-tuple $(\delta_1, \ldots, \delta_\ell)$ for which $f^{\delta_1}(n+d_1)\ldots f^{\delta_\ell}(n+d_\ell)$ is a perfect m-th power. We will prove that

$$\prod_{j=1}^{\ell} \left| \sum_{\ell_j}^{m/2} \chi^{\delta_j}(g^{x\ell_j}) \right| \leq \frac{k^{\ell(\ell+1)/2}}{2^\ell}. \tag{13}$$

Indeed, by Lemma 4 we have a permutation $(\rho_1, \ldots, \rho_\ell)$ of $(\delta_1, \ldots, \delta_\ell)$ such that for all $1 \leq i \leq \ell$ there exists an α_i with $1 \leq \alpha_i \leq k^i$ and

$$m \mid \alpha_i \rho_i.$$

By this, $0 < \alpha_i \rho_i < \alpha_i m$ and $\alpha_i \leq k^i$ we get

$$\begin{aligned} m \leq \alpha_i \rho_i &\leq (\alpha_i - 1)m, \\ \frac{1}{\alpha_i} \leq \frac{\rho_i}{m} &\leq 1 - \frac{1}{\alpha_i}, \\ \frac{1}{k^i} \leq \frac{1}{\alpha_i} &\leq \left|\left| \frac{\rho_i}{m} \right|\right|. \end{aligned}$$

By this, (10) and $|1 - e(\alpha)| \geq 4\,||\alpha||$ we have

$$\left| \sum_{\ell_j=1}^{m/2} \chi^{\rho_j}(g^{x\ell_j}) \right| \leq \frac{2}{|1 - \chi^{\rho_j}(g^x)|} = \frac{2}{|1 - e(\rho_j/m)|} \leq \frac{1}{2\,||\rho_j/m||} \leq \frac{k^j}{2}. \tag{14}$$

Taking the term-wise product in (14) for $j = 1, \ldots, \ell$ we obtain (13). Thus

$$\sum\nolimits_2 \leq p \frac{k^{\ell(\ell+1)/2}}{m^\ell} \sum_{\substack{1 \leq \delta_1, \ldots, \delta_\ell \leq m, \\ f^{\delta_1}(n+d_1)\cdots f^{\delta_\ell}(n+d_\ell) \text{ is} \\ \text{a perfect } m\text{-th power}}} 1. \tag{15}$$

Next we give an upper bound for

$$r \stackrel{\text{def}}{=} \sum_{\substack{1 \leq \delta_1, \ldots, \delta_\ell \leq m, \\ f^{\delta_1}(n+d_1)\cdots f^{\delta_\ell}(n+d_\ell) \text{ is} \\ \text{a perfect } m\text{-th power}}} 1. \tag{16}$$

The number of different permutations $(\rho_1, \ldots, \rho_\ell)$ of $(\delta_1, \ldots, \delta_\ell)$ is $\ell!$. Consider a fixed permutation $(\rho_1, \ldots, \rho_\ell)$. Then by Lemma 4 we have $m \mid \alpha_i \rho_i$ where $1 \leq \alpha_i \leq k^i$. Thus $\frac{m}{(m,\alpha_i)} \mid \rho_i$. Since $1 \leq \rho_i \leq m$ we have that ρ_i may assume $(m, \alpha_i) \leq \alpha_i \leq k^i$ values. Therefore

$$r \leq \ell! \prod_{i=1}^{\ell} k^i = \ell! k^{\ell(\ell+1)/2}. \tag{17}$$

By (15), (16) and (17) we have

$$\sum\nolimits_2 \leq \ell! \frac{k^{\ell(\ell+1)}}{m^\ell} p$$

which proves Theorem 3 (i). It remains to prove Lemma 4.

Proof of Lemma 4

We will need the following definition and lemma:

Definition 2 *Let $\mathcal{A}$ and $\mathcal{B}$ be multi-sets of the elements of $\mathbb{Z}_p$. If $\mathcal{A}+\mathcal{B}$ represents every element of $\mathbb{Z}_p$ with multiplicity divisible by m, i.e., for all $c \in \mathbb{Z}_p$, the number of solutions of*

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

(the a's and b's are counted with their multiplicities) is divisible by m, then the sum $\mathcal{A}+\mathcal{B}$ is said to have property P.

Lemma 5 *Let $\mathcal{A} = \{a_1, a_2, \ldots, a_r\}$, $\mathcal{D} = \{d_1, d_2, \ldots, d_\ell\} \subseteq \mathbb{Z}_p$. If one of the following two conditions holds*

(i) $\min\{r, \ell\} \leq 2$ *and* $\max\{r, \ell\} \leq p-1$,

(ii) $(4\ell)^r \leq p$ *or* $(4r)^\ell \leq p$,

then there exist $c_1, \ldots, c_\ell \in \mathbb{Z}_p$ *and a permutation* $(q_1, \ldots, q_\ell)$ *of* $(d_1, \ldots, d_\ell)$ *such that for all* $1 \leq i \leq \ell$

$$a + d = c_i \qquad a \in \mathcal{A},\ d \in \mathcal{D}$$

has at least one solution, and the number of solutions is less than i*. Moreover for all solution* $a \in \mathcal{A},\ d \in \mathcal{D}$ *we have* $d \in \{q_1, q_2 \ldots, q_i\}$*, and* $d = q_i$*,* $a = c_i - q_i$ *is always a solution.*

Proof of Lemma 5

We will prove Lemma 5 by induction on i. It was proved in [4, Theorem 2] that for all sets $\mathcal{A}$ and $\mathcal{D}$ with the conditions of Lemma 5, we have a $c \in \mathbb{Z}_p$ such that

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

has exactly one solution.

This proves Lemma 5 in the case $i = 1$. Suppose that Lemma 5 holds for $i = j$. Then we will prove that it also holds for $i = j + 1$. By the induction hypothesis we have $c_1, \ldots, c_j$ and a permutation $(q_1, \ldots, q_j)$ of $(d_1, \ldots, d_j)$ according to Lemma 5. Let $\mathcal{D}' = \mathcal{D} \setminus \{q_1, \ldots q_j\}$. Since Lemma 5 is true for $i = 1$ we have that there exists $c_{j+1} \in \mathbb{Z}_p$ such that

$$a + d = c_{j+1} \qquad a \in \mathcal{A},\ d \in \mathcal{D}'$$

has exactly one solution. Let this unique solution be $\alpha = \alpha_{i+1}$ and $d = q_{j+1}$. Then for the solution of

$$a + d = c_{j+1} \qquad a \in \mathcal{A},\ d \in \mathcal{D}$$

we have $d \in \{q_1, q_2, \ldots, q_{j+1}\}$ which completes the proof of Lemma 5.

Now we return to the proof of Lemma 4. The following equivalence relation was defined in [4] and also used in [5]: We will say that the polynomials $\varphi(x), \psi(x) \in \mathbb{F}_p[x]$ are equivalent, $\varphi \sim \psi$, if there is an $a \in \mathbb{F}_p$ such that $\psi(x) = \varphi(x + a)$. Clearly, this is an equivalence relation.

Write f as the product of irreducible polynomials over $\mathbb{F}_p$. Let us group these factors so that in each group the equivalent irreducible factors are collected. Consider a typical group $\varphi(x+a_1), \ldots, \varphi(x+a_r)$. Then f is of the form $f(x) = \varphi^{\alpha_1}(x+a_1) \ldots \varphi^{\alpha_r}(x+a_r)g(x)$ where $g(x)$ has no irreducible factors equivalent with any $\varphi(x + a_i)$ $(1 \leq i \leq r)$.

Let $h(n) = f^{\delta_1}(n+d_1) \cdots f^{\delta_\ell}(n+d_\ell)$ be a perfect m-th power where $1 \leq \delta_1, \ldots, \delta_\ell < m$. Then writing $h(x)$ as the product of irreducible polynomials over $\mathbb{F}_p$, all the polynomials $\varphi(x+a_i+d_j)$ with $1 \leq i \leq r$, $1 \leq j \leq \ell$ occur amongst the factors. All these polynomials are equivalent, and no other irreducible factor belonging to this equivalence class will occur amongst the irreducible factors of $h(x)$.

Since distinct irreducible polynomials cannot have a common zero, each of the zeros of h is of multiplicity divisible by m, if and only if in each group, formed by equivalent irreducible factors $\varphi(x + a_i + d_j)$ of $h(x)$, every polynomial of form $\varphi(x + c)$ occurs with multiplicity divisible by m. In other words writing $\mathcal{A} = \{a_1, \ldots, a_1, \ldots, a_r, \ldots, a_r\}$, $\mathcal{D} = \{d_1, \ldots, d_1, \ldots, d_\ell, \ldots, d_\ell\}$ where a_i has the multiplicity α_i in $\mathcal{A}$ (α_i is the exponent of $\varphi(x + a_i)$ in the factorization of $f(x)$) and d_i

has the multiplicity δ_i in $\mathcal{D}$ (where $h(n) = f^{\delta_1}(n+d_1)\cdots f^{\delta_\ell}(n+d_\ell)$ is a perfect m-th power), then for each group $\mathcal{A}+\mathcal{D}$ must possess property P.

Let $\mathcal{A}'$ and $\mathcal{D}'$ be the simple set version of $\mathcal{A}$ and $\mathcal{D}$, more exactly, let $\mathcal{A}' = \{a_1, \ldots, a_r\}$ and $\mathcal{D}' = \{d_1, \ldots, d_\ell\}$. $\mathcal{A}'$ and $\mathcal{D}'$ satisfy the conditions of Lemma 5. So by Lemma 5 for the sets $\mathcal{A}$ and $\mathcal{D}$ we have the following: There exist $c_1, \ldots, c_\ell \in \mathbb{Z}_p$ and a permutation $(q_1, \ldots, q_\ell) = (d_{j_1}, \ldots, d_{j_\ell})$ of $(d_1, \ldots, d_\ell)$ such that if

$$a + d = c_i \qquad a \in \mathcal{A}',\ d \in \mathcal{D}',$$

then we have

$$d \in \{q_1, \ldots, q_i\} = \{d_{j_1}, \ldots, d_{j_i}\}$$

and $d = q_i$, $a = c_i - q_i$ is a solution. Here $(j_1, \ldots, j_\ell)$ is a permutation of $(1, \ldots, \ell)$. Define ρ_i's by $\rho_i = \delta_{j_i}$ (so $(\rho_1, \ldots, \rho_\ell) = (\delta_{j_1}, \ldots, \delta_{j_\ell})$ is the same permutation of $(\delta_1, \ldots, \delta_\ell)$ as the permutation $(q_1, \ldots, q_\ell) = (d_{j_1}, \ldots, d_{j_\ell})$ of $(d_1, \ldots, d_\ell)$). Returning to the multi-set case, using these notation we get that the number of the solutions

$$a + d = c_i \qquad a \in \mathcal{A},\ d \in \mathcal{D}$$

is of the form

$$\epsilon_{i,1}\alpha_{i,1}\rho_1 + \epsilon_{i,2}\alpha_{i,2}\rho_2 + \cdots + \epsilon_{i,i}\alpha_{i,i}\rho_i$$

where $\epsilon_{i,j} \in \{0,1\}$, $\alpha_{i,j} \in \{\alpha_1, \ldots, \alpha_r\}$ for $1 \le j \le i$ and $\epsilon_{i,i} = 1$. (We study the number of the solutions by multiplicity since $\mathcal{A}$ and $\mathcal{D}$ are multi-sets).

Since $\mathcal{A}+\mathcal{D}$ posses property $\mathcal{P}$ we have that for all $1 \leq i \leq \ell$

$$m \mid \epsilon_{i,1}\alpha_{i,1}\rho_1 + \epsilon_{i,2}\alpha_{i,2}\rho_2 + \cdots + \epsilon_{i,i}\alpha_{i,i}\rho_i. \tag{18}$$

By induction on i we will prove that

$$m \mid \alpha_{1,1}\alpha_{2,2}, \ldots, \alpha_{i,i}\rho_i. \tag{19}$$

Indeed, for $i = 1$ by (18) and $\epsilon_{1,1} = 1$ we get $m \mid \alpha_{1,1}\rho_1$. We will prove that if (19) holds for $i \leq j-1$, then it also holds for $i = j$.

By the induction hypothesis we have

$$m \mid \alpha_{1,1}\rho_1,\ m \mid \alpha_{1,1}\alpha_{2,2}\rho_2,\ \ldots,\ m \mid \alpha_{1,1}\alpha_{2,2}\ldots, \alpha_{j-1,j-1}\rho_{j-1}. \tag{20}$$

Multiplying (18) for $i = j$ by $\alpha_{1,1}\ldots\alpha_{j-1,j-1}$ we get:

$$\begin{aligned} m \mid & \epsilon_{j,1}\alpha_{j,1}\alpha_{1,1}\ldots\alpha_{j-1,j-1}\rho_1 + \epsilon_{j,2}\alpha_{j,2}\alpha_{1,1}\ldots\alpha_{j-1,j-1}\rho_2 + \ldots \\ & + \epsilon_{j,j}\alpha_{j,j}\alpha_{1,1}\ldots\alpha_{j-1,j-1}\rho_i. \end{aligned}$$

From this using (20) and $\epsilon_{j,j} = 1$ we get

$$m \mid \alpha_{1,1}\ldots\alpha_{j,j}\rho_j$$

which was to be proved.

$\alpha_{1,1}, \ldots, \alpha_{i,i} \in \{\alpha_1, \ldots, \alpha_r\}$ where α_i's are exponents of irreducible factors of f, thus $1 \leq \alpha_{i,i} \leq \deg f = k$. Therefore $\alpha_{1,1}\alpha_{2,2}\ldots\alpha_{i,i} \leq k^i$ and by (19) this completes the proof of Lemma 4.

2.3 Proof of Theorem 4

The proof is exactly the same as in [2, Theorem 1], the only difference is in the definitions of q and r: now we choose q, r as integers with $(q,p) = (r,p) = 1$ and $1 \leq \mathrm{ind}^* q \leq \frac{m}{2}$, $\frac{m}{2} < \mathrm{ind}^* r \leq m$.

3 Time analysis

Construction 1 depends on the key g^x where g is a primitive root and $(x, m) = 1$. We only need g^x, it is not necessary to know the value of g or x. First we prove that it is easy to find a key g^x.

Suppose that the factorization of m is known: $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ where $p_1, \dots, p_r$ are primes. The condition $(x, m) = 1$ is equivalent with that $y = g^x$ is not a perfect p_i-th power for any $1 \leq i \leq r$ in $\mathbb{F}_p$. In other words, using Fermat's theorem we have that

$$y^{(p-1)/p_i} \equiv 1 \pmod{p} \tag{21}$$

does not hold for all $1 \leq i \leq r$. By using the iterated squaring method to check (21), it takes $O\left((\log p)^3\right)$ bit operations (see e.g. in [8]).

We will choose a random $y \in \mathbb{Z}_p$, and by (21) we check that $y = g^x$ weather satisfies $(x, m) = 1$ or not. For a fix primitive root g, the number of x's with this property is $\varphi(m)\frac{p-1}{m} \gg \frac{p}{\log\log p}$. Thus after $c \log\log p$ attempts we will find a suitable key g^x with high probability.

Next by the Pohlig-Hellman [12] we prove that $\mathrm{ind}^* n$ can be computed fast. Indeed, first we determine $\mathrm{ind}^* n$ modulo prime power divisor q^α of m by $O\left(\alpha q (\log p)^3\right)$ bit operations. If we know $\mathrm{ind}^* n$ modulo $p_i^{\alpha_i}$ for all $1 \leq \alpha_i \leq r$ where $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, then using the Chinese Remainder theorem we have determined the value $\mathrm{ind}^* n$ modulo m, which gives $\mathrm{ind}^* n$ because of $1 \leq \mathrm{ind}^* n \leq m$. Thus to compute $\mathrm{ind}^* n$ we use $O((\log m)^4 + (\log p)^3(\alpha_1 p_1 + \dots + \alpha_r p_r)) \leq O((\log m)^4 + (\log p)^3(\alpha_1 + \dots + \alpha_r) \max\limits_{1 \leq i \leq r} p_i) \leq O((\log p)^4 \max\limits_{1 \leq i \leq r} p_i)$ bit operations.

Let us see the proof of that $\mathrm{ind}^* n$ can be computed modulo prime power divisors q^α of m by $O(\alpha q(\log p)^3)$ bit operations. We will prove this by induction on α. When $\alpha = 0$ the statement is trivial. Suppose that we already know $\mathrm{ind}^* n$ modulo q^i:

$$\mathrm{ind}^* n \equiv s \pmod{q^i}.$$

From this we compute $\mathrm{ind}^* n$ modulo q^{i+1} by $O(q(\log p)^3)$ bit operations if $q^{i+1} \mid m$. In order to prove this statement we will use the following lemma, which is a trivial consequence of the properties of the primitive roots and Fermat's theorem.

Lemma 6 *$q^\alpha \mid m$. Then*

$$\mathrm{ind}^* n \equiv s \pmod{q^\alpha}$$

holds if and only if

$$n/g^{sx} \textit{ is a perfect } q^\alpha\textit{-th power modulo } p$$

which is equivalent with

$$(n/g^{sx})^{(p-1)/q^\alpha} \equiv 1 \pmod{p}. \tag{22}$$

By Lemma 6 we have that n/g^{sx} is a perfect q^i-th power. By Lemma 6, using (22), we check that which of the numbers

$$n/g^{sx},\ n/g^{(s+q^i)x},\ n/g^{(s+2q^i)x}, \ldots,\ n/g^{s+(q-1)q^i x}$$

is a perfect q^{i+1}-th power. This takes $O\left(q(\log p)^3\right)$ bit operations. There is surely one which is a perfect q^{i+1}-th power, because $s,\ s +$

$q^i, \ldots, \ s+(q-1)q^i$ run over the residue classes modulo q^{i+1} which are congruent to s modulo q^i. By Lemma 6, n/g^{s+jp^ix} is a perfect p^{i+1}-th power if and only if $\mathrm{ind}^* n \equiv s + jq^i x \pmod{q^{i+1}}$. This completes the proof of the statement.

4 An extension of an inequality of Mauduit and Sárközy

C. Mauduit and A. Sárközy [10] expressed the connection between the well-distribution measure and the correlation measure of order 2 in a quantitative form: For all $E_N \in \{-1,+1\}^N$

$$W(E_N) \le 3\sqrt{NC_2(E_N)}. \tag{23}$$

They also gave a construction for which $W(E_N) \gg \sqrt{NC_2(E_N)}$. Their result shows that (23) is sharp apart from a constant factor. The following theorem generalizes (23) for the correlation measures of higher order:

Theorem 5 *For all $E_N \in \{-1,+1\}^N$, $3\ell^2 \le N$ we have*

$$W(E_N) \le 3\ell N^{1-1/(2\ell)} \left(C_{2\ell}(E_N)\right)^{1/(2\ell)}.$$

By Theorem 3 we get for $N = p-1$:

$$C_\ell(E_N) \ll_\ell k^{\ell(\ell+1)} \frac{p}{m^\ell} \tag{24}$$

if $m < \frac{p^{1/(2\ell)}}{(\log p)^{1+1/\ell}}$. We will see that if ℓ is even, m is odd and small enough, then by Theorem 5 and Theorem 1 we have that the upper

bound in (24) is sharp apart from a constant factor. Thus in case of even ℓ and odd m Construction 1 provides a natural example for a sequence whose correlation measures of small orders are small while the well-distribution measure is possibly large. Indeed, by Theorem 1 if $m < \frac{1}{2k} p^{1/2}/(\log p)^2$ we have

$$W(E_{p-1}) \gg \frac{p}{m}.$$

By Theorem 5 we fixed

$$\frac{p}{m} \ll W(E_N) \ll \ell p^{1-1/(2\ell)} \left(C_{2\ell}(E_N)\right)^{1/(2\ell)},$$

which implies

$$\frac{1}{\ell^{2\ell}} \frac{p}{m^{2\ell}} \ll C_{2\ell}(E_N).$$

Comparing this with (24) we get that Theorem 5 is sharp apart from a constant factor. While the construction of A. Sárközy and C. Mauduit [10] showing that (23) is sharp used probabilistic methods, Construction 1 is explicit.

Proof of Theorem 5

The proof is nearly the same as in [10], however we have to handle larger product of e_i's than in [10].

Let

$$W(E_N) = \sum_{j=0}^{t-1} e_{a+jb} = \sum_{\substack{a \le i < m \\ i \equiv a \pmod b}} e_i$$

where $m = a + tb \le N + b$. If $N < i \le N + b$, let $e_i = 1$. Then

$$(W(E_N))^{2\ell} = \Big(\sum_{\substack{a \le i < m \\ i \equiv a \pmod b}} e_i \Big)^{2\ell} \le \sum_{h=0}^{b-1} \Big(\sum_{\substack{a \le i < m \\ i \equiv h \pmod b}} e_i \Big)^{2\ell}$$

$$= \sum_{\substack{r \le 2\ell,\ a \le i_1 < i_2 < \cdots < i_r < m \\ i_1 \equiv i_2 \equiv \cdots \equiv i_r \pmod b}} X_r \cdot e_{i_1} e_{i_2} \dots e_{i_r}$$

$$= \sum_{\substack{j \le \ell,\ a \le i_1 < i_2 < \cdots < i_{2j} < m \\ i_1 \equiv i_2 \equiv \cdots \equiv i_{2j} \pmod b}} X_{2j} \cdot e_{i_1} e_{i_2} \dots e_{i_{2j}}. \tag{25}$$

Here $r \le 2\ell$ because originally all the products are in the form of $e_1^{\alpha_1} \dots e_{m-1}^{\alpha_{m-1}}$ (where $\alpha_1 + \cdots + \alpha_{m-1} = 2\ell$) but $e_i^{\alpha_i} = 1$ if α_i is even and $e_i^{\alpha_i} = e_i$ if α_i is odd. The sum $\alpha_1 + \cdots + \alpha_{m-1} = 2\ell$ is even, so the number of odd α_i's is even. Thus in (25) we may suppose that $r = 2j$ where $j \in \mathbb{N}$.

Let s denote the number of i's with $a \le i < m$ and for which i belongs to a fixed residue class modulo b (here s is the number of the terms in $\sum_{\substack{a \le i < m \\ i \equiv h \pmod b}} e_i$ for any h, s does not depend on h on the value of the fixed residue class). Using the multinomial theorem:

$$X_{2j} = \sum_{\substack{\alpha_1 + \cdots + \alpha_s = 2\ell \\ \alpha_1, \dots, \alpha_{2j} \text{ are odd} \\ \alpha_{2j+1}, \dots, \alpha_s \text{ are even}}} \frac{(2\ell)!}{\alpha_1! \dots \alpha_s!} \le \sum_{\substack{\alpha_1 + \cdots + \alpha_s = 2\ell \\ \alpha_1, \dots, \alpha_{2j} \text{ are odd} \\ \alpha_{2j+1}, \dots, \alpha_s \text{ are even}}} (2\ell)!.$$

For $1 \le i \le 2j$ let $\alpha_i = 2\beta_i - 1$ and for $2j + 1 \le i \le s$ let $\alpha_i = 2\beta_i - 2$. Then

$$X_{2j} \le (2\ell)! \sum_{\substack{\beta_1 + \cdots + \beta_s = s + \ell - j \\ \forall i:\ \beta_i > 0}} 1 = (2\ell)! \binom{s + \ell - j - 1}{s - 1}$$

$$\le \frac{(2\ell)!}{(\ell - j)!} (s + \ell - j - 1)^{\ell - j} \le (2\ell)^{\ell + j} (s + \ell - j - 1)^{\ell - j}$$

$$\le (2\ell)^{\ell + j} (N + \ell)^{\ell - j} = 2^{\ell + j} \ell^{\ell + j} (N + \ell)^{\ell - j}. \tag{26}$$

By (25) and the triangle-inequality we have

$$(W(E_N))^{2\ell} \le \sum_{j=0}^{\ell} |X_{2j}| \sum_{\substack{1\le d_1<d_2<\cdots<d_{2j-1}<m-a \\ 0\equiv d_1\equiv d_2\equiv\cdots\equiv d_{2j-1} \pmod b}} \left| \sum_{i=a}^{m-1-d_{2j-1}} e_i e_{i+d_1}\dots e_{i+d_{2j-1}} \right|. \tag{27}$$

By the definition of the correlation measure we have:

$$\left| \sum_{i=a}^{m-1-d_{2j-1}} e_i e_{i+d_1}\dots e_{i+d_{2j-1}} \right| \le C_{2\ell}(E_N) + 1.$$

Thus from (26) and (27) we obtain

$$\begin{aligned}(W(E_N))^{2\ell} &\le \sum_{j=0}^{\ell} 2^{\ell+j}\ell^{\ell+j}(N+\ell)^{\ell-j} \sum_{\substack{1\le d_1<d_2<\cdots<d_{2j-1}<m-a \\ 0\equiv d_1\equiv d_2\equiv\cdots\equiv d_{2j-1} \pmod b}} (C_{2j}(E_N)+1) \\ &= \sum_{j=0}^{\ell} 2^{\ell+j}\ell^{\ell+j}(N+\ell)^{\ell-j}N^{2j-1}(C_{2j}(E_N)+1)\end{aligned}$$

where by definition $C_0(E_N) = N$. Using that for $1 \le j \le \ell-1$ $C_{2j}(E_N) \le N$ we obtain

$$(W(E_N))^{2\ell} \le \sum_{j=0}^{\ell-1} 2^{\ell+j}\ell^{\ell+j}(N+\ell)^{\ell+j} + 4^{\ell}\ell^{2\ell}N^{2\ell-1}(C_{2\ell}(E_N)+1). \tag{28}$$

By $1+x \le e^x$ we have

$$\begin{aligned}\sum_{j=0}^{\ell-1} 2^{\ell+j}\ell^{\ell+j}(N+\ell)^{\ell+j} &= 2^{\ell}\ell^{\ell}(N+\ell)^{\ell}\sum_{j=0}^{\ell-1} 2^{j}\ell^{j}(N+\ell)^{j} \\ &= 2^{\ell}\ell^{\ell}(N+\ell)^{\ell}(1+2\ell(N+\ell))^{\ell-1} \\ &= 2^{2\ell-1}\ell^{2\ell-1}N^{2\ell-1}\left(1+\frac{\ell}{N}\right)^{\ell}\left(1+\frac{2\ell^2+1}{2\ell N}\right)^{\ell-1} \\ &\le 2^{2\ell-1}\ell^{2\ell-1}N^{2\ell-1}e^{2\ell^2/N} \le 4^{\ell}\ell^{2\ell-1}N^{2\ell-1}.\end{aligned}$$

From this and (28) we obtain

$$(W(E_N))^{2\ell} \le 4^\ell \ell^{2\ell} N^{2\ell-1}(C_{2\ell}(E_N) + 1 + \frac{1}{\ell}) \le 9^\ell \ell^{2\ell} N^{2\ell-1} C_{2\ell}(E_N),$$

which proves Theorem 5.

I would like to thank to Professor András Sárközy for the valuable discussions and to the referee Christian Elsholtz for his careful reading and constructive comments.

References

[1] R. Ahlswede, C. Mauduit, A. Sárközy, *Large families of pseudorandom sequences of k symbols and their complexity, Part I, Part II.*, Proceedings on General Theory of Information Transfer and Combinatorics, to appear.

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

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

[4] L. Goubin, C. Mauduit, A. Sárközy, *Construction of large families of pseudorandom binary sequences*, J. Number Theory, to appear.

[5] K. Gyarmati, *On a family of pseudorandom binary sequences*, Periodica Math. Hungar., to appear.

[6] K. Gyarmati, *On a pseudorandom property of binary sequences*, The Ramanujan Journal, to appear.

[7] D. R. Heath-Brown, *Zero-Free Regions for Dirichlet L-Functions and the Least Prime in an Arithmetic Progression*, Proc. London Math. Soc. 64, (1992), 265-338.

[8] N. Koblitz, *A course in number theory and cryptography*, Graduate Texts in Mathematics 114, Springer-Verlag, New-York, 1994.

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

[10] C. Mauduit, A. Sárközy, *On the measures of pseudorandomness of binary sequences*, Discrete Math. 271 (2003), 195-207.

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

[12] S. C. Pohlig, M. E. Hellman, *An improved algorithm for computing logarithms over* GF(p) *and its cryptographic significance*, IEEE Trans. Information Theory 24 (1978), 106-110.

[13] A. Sárközy, *A finite pseudorandom binary sequence*, Studia Sci. Math. Hungar. 38 (2001), 377-384.

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