

ON THE PSEUDORANDOMNESS OF THE POWER GENERATOR WITH SQUAREFREE COMPOSITE MODULI

MILAN MOLNAR

ABSTRACT. Finite binary sequences with strong pseudorandom properties are essential for secure cryptographic systems. The power generator, defined by a modular exponentiation recurrence, is a widely used method for creating such sequences. While its pseudorandomness has been extensively analysed for prime moduli, real-world cryptographic applications like the RSA and Blum–Blum–Shub generators rely heavily on composite moduli. This paper bridges that gap by investigating the power generator’s behaviour when the modulus is a product of distinct primes. Building upon Gyarmati’s exponential sum estimates for prime moduli, we demonstrate that the generator retains its strong pseudorandom characteristics in the composite case. The approach is based on the Chinese Remainder Theorem, enabling the generalization of character sum bounds. Ultimately, we establish new upper bounds for the pseudorandom measures introduced by Mauduit and Sárközy, specifically the well-distribution and correlation measures.

Communicated by A. Winterhof

1 Introduction

The analysis of pseudorandom properties of finite binary sequences is a fundamental challenge in modern computer science and cryptography. In a seminal paper, Mauduit and Sárközy [11] introduced a rigorous quantitative framework to evaluate these sequences. They defined several pseudorandom measures, such as the well-distribution measure and the correlation measure of order ℓ , which have since become standard tools for determining how closely a sequence mimics true randomness.

Pseudorandom sequences can be constructed using various techniques, one of which is the power generator.

Definition 1.1 (*Power generator*).

Let $k \geq 2$, $m \geq 1$ and ϑ be an integer such that $(\vartheta, m) = 1$. The sequence (u_n) is defined by the following recursion:

$$u_{n+1} \equiv u_n^k \pmod{m}, \quad 0 \leq u_n \leq m-1, \quad n = 0, 1, 2, \dots,$$

with the initial value $u_0 = \vartheta$.

Construction. Let us define the sequence $E_N = (e_1, \dots, e_N) \in \{-1, 1\}^N$ as follows:

$$e_n = \begin{cases} +1, & \text{if } u_n \equiv 0 \pmod{2}, \\ -1, & \text{if } u_n \equiv 1 \pmod{2}. \end{cases}$$

We remark that this is not the only way to define a binary sequence from the sequence (u_n) . For example, the following sequence $A_N = (a_1, \dots, a_N)$ is also studied in the literature, see in [10]:

$$a_n = \begin{cases} +1, & \text{if } u_n < m/2, \\ -1, & \text{otherwise.} \end{cases}$$

The approach of this paper yields the same results for A_N , since one can multiply u_n by 2^{-1} and 2 modulo m , respectively, to get from E_N to A_N and back.

The significance of the power generator lies in its direct connection to key cryptographic primitives. For instance, given a modulus $m = pq$ where p and q are distinct odd primes, the Blum-Blum-Shub (BBS) generator, introduced by Blum, Blum, and Shub [2], is a specific case where the exponent is $k = 2$, or the RSA generator [14] where $(k, \varphi(m)) = 1$ (throughout the paper, we write (a, b) for the greatest common divisor and $[a, b]$ for the least common multiple of two arbitrary integers a, b). Its security is closely tied to the difficulty of integer factorization, making it a cornerstone of theoretical cryptography.

Gyarmati [9] provided strong upper bounds for the pseudorandom measures of these sequences in the prime modulus case, utilizing exponential sum estimates. However, practical applications—such as the RSA generator and the BBS scheme—often rely on composite moduli, a special case of this when m is a product of several distinct primes.

While the distribution of the power generator for squarefree composite moduli has been studied by Friedlander, Pomerance and Shparlinski [6], who proved that for almost all choices of $m = pq$ and for almost all choices of ϑ and k the sequence (u_n) is uniformly distributed, the specific pseudorandom measures (in the sense of Mauduit and Sárközy) remained less explored for the general composite case. Further steps toward understanding sequences with composite moduli were taken by Rivat and Sárközy [13], who studied the construction of pseudorandom sequences using the structure of $\mathbb{Z}_m$.

El-Mahassni [5] studied the distribution of the power generator and obtained bounds for exponential sums containing the terms of the power generator in the general, composite moduli case.

Later Ostafe and Shparlinski [12] proved several results in the prime modulus case, which are similar to those in the paper of Gyarmati [9]. Furthermore, they have given a generalization of the power generator iterating multivariate polynomials.

In a recent paper [1], Bhakta and Shparlinski have given a detailed summary of the distribution of the power generator and exponential sums of the form $\sum_{x \in \mathbb{F}_p} e^{2\pi i f(x)/p}$ with sparse polynomials. We mention that in [9] Gyarmati used a deep theorem of Bourgain [[3], Theorem 1] about these sums, and Bhakta and Shparlinski proved an explicit version of it.

In this paper, we extend the results of Gyarmati [9] by proving that the power generator maintains strong pseudorandom properties when the modulus m is a product of n distinct primes. By applying the Chinese Remainder Theorem and generalizing the character sum estimates used in the prime case, we provide new upper bounds for the pseudorandom measures of these sequences, specifically for the well-distribution and correlation measures. To provide a quantitative assessment of these properties, Mauduit and Sárközy [11] introduced the following definitions.

Definition 1.2 (Mauduit–Sárközy [11]). Let $E_N = (e_1, \dots, e_N) \in \{-1, 1\}^N$ be a finite binary sequence, $\ell \in \mathbb{N}$, $M, N \in \mathbb{N}$, $X = (x_1, \dots, x_\ell) \in \{-1, 1\}^\ell$, $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $D = (d_1, \dots, d_\ell) \in \mathbb{N}^\ell$ with $1 \leq d_1 < \dots < d_\ell$.

$$T(E_N, M, X) = |\{n: 0 \leq n < M, (e_{n+1}, \dots, e_{n+\ell}) = X\}|,$$

where $\ell \leq N$ and $0 < M \leq N + 1 - \ell$.

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

where $1 \leq a + b \leq a + Mb \leq N$.

$$V(E_N, M, D) = \sum_{n=0}^{M-1} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_\ell},$$

where $M + d_\ell \leq N + 1$.

Definition 1.3 (Mauduit–Sárközy [11]).

- 1) Normality measure of order ℓ :

$$\mathcal{N}_\ell(E_N) \stackrel{\text{def}}{=} \max_{X \in \{-1, 1\}^\ell} \max_{0 < M \leq N+1-\ell} |T(E_N, M, X) - M/2^\ell|.$$

- 2) Normality measure:

$$\mathcal{N}(E_N) \stackrel{\text{def}}{=} \max_{\ell \leq \log N / \log 2} \mathcal{N}_\ell(E_N).$$

- 3) Well-distribution measure:

$$\mathcal{W}(E_N) \stackrel{\text{def}}{=} \max_{a, b, M} |U(E_N, M, a, b)| = \max_{a, b, M} \left| \sum_{j=1}^M e_{a+jb} \right|,$$

where the maximum is taken for all a, b and M with $1 \leq a + b \leq a + bM \leq N$ and $b > 0$.

4) Correlation measure of order ℓ :

$$\mathcal{C}_\ell(E_N) \stackrel{\text{def}}{=} \max_{M,D} |V(E_N, M, D)| = \max_{M,D} \left| \sum_{n=0}^{M-1} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_\ell} \right|,$$

where the conditions above hold for M and $D = (d_1, d_2, \dots, d_\ell)$ with $d_1 < d_2 < \cdots < d_\ell < M + d_\ell \leq N + 1$.

5) Correlation measure:

$$\mathcal{C}(E_N) \stackrel{\text{def}}{=} \max_{\ell \leq \log N / \log 2} \mathcal{C}_\ell(E_N).$$

It is immediately seen that after a given index n_0 , the order of $u_n \equiv \vartheta^{k^n}$ modulo m will be the same, let this order be t . Then $(k, t) = 1$, and let us denote the order of k modulo t by T . Thus, the sequence $u_{n_0}, u_{n_0+1}, \dots$ is periodic with period T . Throughout this paper, we will assume that the sequence (u_n) is purely periodic.

We now present the important results from [9], these will form the basis of our proof, we state these steps as lemmas.

Assume that $m = p$ is an arbitrary prime. Let t_p denote the order of ϑ modulo p , and let T_p be the order of k modulo t_p .

To facilitate the handling of exponential sums, we introduce the following notation for $a \in \mathbb{R}$:

$$e_m(a) = e^{2\pi i \frac{a}{m}}.$$

Theorem A. ([9], Theorem 1)

$$\mathcal{W}(E_{T_p}) \ll p^{7/8} (\log p)^2.$$

Theorem B. ([9], Theorem 2) For every real number $\varepsilon > 1/4$, it holds that

$$\mathcal{N}_\ell(E_{T_p}) \ll k^{\varepsilon(\ell-1)} p^{7/8} (\log p)^{\ell+1},$$

where the implied constant depends only on ε .

Theorem C. ([9], Theorem 3) Assume that $\ell^2 < p$. Let $N_p = N_p(\vartheta, k, \delta) \leq T_p$ denote the largest positive integer such that for every $1 \leq i < j \leq 2N_p$

$$(k^j - k^i, t_p) \leq t_p \cdot p^{-\delta}.$$

Then there exists a constant $\varepsilon(\ell, \delta) = \varepsilon > 0$, depending only on ℓ and δ , such that for the sequence E_{N_p}

$$\mathcal{C}_\ell(E_{N_p}) \leq p^{1-\varepsilon}.$$

In the following lemmas, Gyarmati gave upper estimates first for complete, and then for incomplete exponential sums containing the terms of the power generator.

Lemma 1.4. ([9], Lemma 4) Suppose that $h_i \in \mathbb{Z}_+$ for $1 \leq i \leq r$, $\vartheta_i = \vartheta^{h_i}$ and $a_i \in \mathbb{F}_p^\times$, where $(h_1, \dots, h_r, p-1) = 1$. Let $N_p(\vartheta_1, \dots, \vartheta_r, k, \delta) = N_p$ denote the largest positive integer such that $N_p \leq T_p$, and for all $0 \leq i \leq N_p$ and $1 \leq j \leq r$

$$(k^i h_j, t_p) \leq t_p \cdot p^{-\delta},$$

and for every pair i_1, j_1, i_2, j_2 with $1 \leq i_1, i_2 \leq N_p$ and $1 \leq j_1, j_2 \leq r$

$$(k^{i_1} h_{j_1} - k^{i_2} h_{j_2}, t_p) \leq t_p \cdot p^{-\delta} \quad \text{or} \quad (k^{i_1} h_{j_1} - k^{i_2} h_{j_2}, t_p) = t_p.$$

If no such N_p exists, then $N_p(\vartheta_1, \dots, \vartheta_r, k, \delta) = N_p = 1$.

Assume that $j \in \mathbb{Z}_{T_p}$. Then there exists a constant $\varepsilon(r, \delta) = \varepsilon_1 > 0$, depending only on r and δ , such that

$$\left| \sum_{x=1}^{T_p} e_p(a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}) e_{T_p}(jx) \right| \ll (t_p T_p)^{1/2} \left(p^{-\varepsilon_1} + \frac{(r+1)^{r/2}}{N_p^{1/2}} \right).$$

If $(h_1, t_p) = 1$ also holds, then $(r+1)^{r/2}$ can be replaced by $(r+1)^{1/2}$:

$$\left| \sum_{x=1}^{T_p} e_p(a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}) e_{T_p}(jx) \right| \ll (t_p T_p)^{1/2} \left(p^{-\varepsilon_1} + \frac{(r+1)^{1/2}}{N_p^{1/2}} \right),$$

where the implied constants are absolute.

In a special case Friedlander, Hansen and Shparlinski gave a bound in [7], which also appears in the paper of Gyarmati [9].

Lemma 1.5. ([7], Theorem 8, [9], Remark 1) If $\vartheta_i = \vartheta^{k^{i-1}}$ for $1 \leq i \leq r$, then assuming that $\eta \geq 1$ is an integer, $\varepsilon_2 > 1/4$, and $t_p > p^{1/2+\nu}$ for a constant $\nu > 0$:

$$\left| \sum_{x=1}^{T_p} e_p(a_1 \vartheta^{k^x} + \dots + a_r \vartheta^{k^{x+r-1}}) e_{T_p}(jx) \right| \ll k^{\varepsilon_2(r-1)} T_p^{1-\frac{2\eta+1}{2\eta(\eta+1)}} t_p^{\frac{1}{2\eta}} p^{\frac{1}{4(\eta+1)}},$$

where the implied constant depends only on ε_2 and ν .

Lemma 1.6. ([9], Lemma 2) Let a_i, ϑ_i for $1 \leq i \leq r$ and N_p be as in Lemma 1.4, and assume that $M, L \in \mathbb{N}$ and $L < T_p$. Then there exists a constant $\varepsilon(r, \delta) = \varepsilon_1 > 0$, depending only on r and δ , such that

$$\left| \sum_{x=M}^{M+L} e_p(a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}) \right| \ll (t_p T_p)^{1/2} \left(p^{-\varepsilon_1} + \frac{(r+1)^{r/2}}{N_p^{1/2}} \right) \log p.$$

If $(h_1, t_p) = 1$ also holds, then $(r+1)^{r/2}$ can be replaced by $(r+1)^{1/2}$:

$$\left| \sum_{x=M}^{M+L} e_p(a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}) \right| \ll (t_p T_p)^{1/2} \left(p^{-\varepsilon_1} + \frac{(r+1)^{1/2}}{N_p^{1/2}} \right) \log p,$$

where the implied constants are absolute.

Lemma 1.7. ([9], Lemma 1, Remark 1) Let $\eta \geq 1$ be an integer, $\varepsilon_2 > 1/4$ and $t_p > p^{1/2+v}$ for a constant $v > 0$. Let $a_i, \vartheta_i = \vartheta^{i-1}$ for $1 \leq i \leq r$ be as in Lemma 1.5, and let $M, L \in \mathbb{N}$ with $L < T_p$. Then

$$\left| \sum_{x=M}^{M+L} e_p(a_1 \vartheta^{k^x} + \dots + a_r \vartheta^{k^{x+r-1}}) \right| \ll k^{\varepsilon_2(r-1)} T_p^{1 - \frac{2\eta+1}{2\eta(\eta+1)}} t_p^{\frac{1}{2\eta}} p^{\frac{1}{4(\eta+1)}} \log p,$$

where the implied constant depends only on ε_2 and v . In the special case where $r = 1$, we obtain the following:

$$\left| \sum_{x=M}^{M+L} e_p(a_1 \vartheta^{k^x}) \right| \ll T_p^{1 - \frac{2\eta+1}{2\eta(\eta+1)}} t_p^{\frac{1}{2\eta}} p^{\frac{1}{4(\eta+1)}} \log p,$$

where the implied constant depends only on v .

2 Theorems

Assume that $m = pq$, where $p < q$ are arbitrary primes. Let us define the numbers t, T, t_p, T_p, t_q, T_q analogously to the definitions above, considering the sequence (u_n) modulo m , modulo p , and modulo q .

Theorem 2.1.

$$\mathcal{W}(E_T) \ll m^{11/12} (\log m)^2.$$

Theorem 2.2. For every real number $\varepsilon > 1/4$, it holds that

$$\mathcal{N}_\ell(E_T) \ll k^{2\varepsilon(\ell-1)} m^{11/12} (\log m)^{\ell+1},$$

where the implied constant depends only on ε .

Theorem 2.3. Assume that $\ell^3 < m$. Let $N_p = N_p(\vartheta, k, \delta) \leq T_p$ denote the largest positive integer such that for every $1 \leq i < j \leq 2N_p$

$$(k^j - k^i, t_p) \leq t_p \cdot p^{-\delta}.$$

Let N_q be defined similarly with respect to q , and let $N := \min N_p, N_q$. Then there exists a constant $\varepsilon(\ell, \delta) = \varepsilon > 0$, depending only on ℓ and δ , such that for the sequence E_N

$$\mathcal{C}_\ell(E_N) \leq m^{1-\varepsilon}.$$

3 Proofs

In [8], Friedlander and Shparlinski gave estimates for exponential sums containing terms of the power generator in the case where the modulus is the product of two distinct primes. To do this, they used the Chinese Remainder Theorem, which allows the reduction of the prime product case to the prime modulus case. We will use this approach to generalize the theorems and lemmas listed in Section 1.

First, we study the case where $(T_p, T_q) = 1$. It follows that $T = [T_p, T_q] = T_p T_q$. By the Chinese Remainder Theorem, there exist α_p, α_q such that:

$$\begin{aligned} \alpha_p &\equiv 1 \pmod{T_p}, & \alpha_q &\equiv 0 \pmod{T_q}, \\ \alpha_p &\equiv 0 \pmod{T_q}, & \alpha_q &\equiv 1 \pmod{T_p}. \end{aligned}$$

As n and k run through the residue classes modulo T_p and T_q , respectively, the values $n\alpha_p + k\alpha_q$ run through all residue classes modulo T .

Lemma 3.1. Suppose that $h_i \in \mathbb{Z}_+$ for $1 \leq i \leq r$, $\vartheta_i = \vartheta^{h_i}$, $a_i \in \mathbb{Z}_{pq}^*$, and assume that $(h_1, \dots, h_r, p-1) = 1$ and $(h_1, \dots, h_r, q-1) = 1$ hold. Then the sequence

$$\{a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}\}$$

is periodic modulo m with period T , its period modulo p is T_p and modulo q is T_q .

Let $N_p(\vartheta_1, \dots, \vartheta_r, k, \delta) = N_p$ be the largest positive integer such that $N_p \leq T_p$ and for every $1 \leq i \leq N_p$ and $1 \leq j \leq r$

$$(k^i h_j, t_p) \leq t_p \cdot p^{-\delta},$$

and for every pair i_1, j_1, i_2, j_2 with $1 \leq i_1, i_2 \leq N_p$ and $1 \leq j_1, j_2 \leq r$

$$(k^{i_1} h_{j_1} - k^{i_2} h_{j_2}, t_p) \leq t_p \cdot p^{-\delta} \quad \text{or} \quad (k^{i_1} h_{j_1} - k^{i_2} h_{j_2}, t_p) = t_p.$$

If no such N_p exists, we set $N_p = 1$. The value N_q is defined analogously for the prime q .

Then there exists a constant $\varepsilon(r, \delta) = \varepsilon_1 > 0$, depending only on r and δ , such that for $j \in \mathbb{Z}_T$

$$|\sum_{x=1}^T e_{pq}(a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}) e_T(jx)| \ll (t_p t_q T_p T_q)^{1/2} \left(p^{-\varepsilon_1} + \frac{(r+1)^{r/2}}{N_p^{1/2}} \right) \left(q^{-\varepsilon_1} + \frac{(r+1)^{r/2}}{N_q^{1/2}} \right).$$

If $(h_1, t_p) = 1$ and $(h_1, t_q) = 1$ also hold, then $(r+1)^{r/2}$ can be replaced by $(r+1)^{1/2}$:

$$|\sum_{x=1}^T e_{pq}(a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}) e_T(jx)| \ll (t_p t_q T_p T_q)^{1/2} \left(p^{-\varepsilon_1} + \frac{(r+1)^{1/2}}{N_p^{1/2}} \right) \left(q^{-\varepsilon_1} + \frac{(r+1)^{1/2}}{N_q^{1/2}} \right),$$

where the implied constants are absolute.

Finally, if $\vartheta_i = \vartheta^{k^{i-1}}$ for $1 \leq i \leq r$, and $t_p > p^{1/2+\nu}$, $t_q > q^{1/2+\mu}$ for some $\nu, \mu > 0$, then for any integer $\eta \geq 2$ and $\varepsilon_2 > 1/4$

$$|\sum_{x=1}^T e_{pq}(a_1 \vartheta^{k^x} + \dots + a_r \vartheta^{k^{x+r-1}}) e_T(jx)| \ll k^{2\varepsilon_2(r-1)} (T_p T_q)^{1-\frac{2\eta+1}{2\eta(\eta+1)}} (t_p t_q)^{\frac{1}{2\eta}} (pq)^{\frac{1}{4(\eta+1)}},$$

where the implied constant depends only on ε_2, ν and μ .

Proof of Lemma 3.1. To prove Lemma 3.1, we will use the statements of Lemma 1.4. and Lemma 1.5. Since $(p, q) = 1$, there exist integers A, B , such that $Ap + Bq = 1$. It follows that $(B, p) = 1$ and $(A, q) = 1$. Similarly, there exist integers A_1, B_1 satisfying $A_1 T_p + B_1 T_q = 1$. We may then write the sum as

$$\begin{aligned} & \left| \sum_{x=1}^T e_{pq}(a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}) e_T(jx) \right| \\ &= \left| \sum_{x=1}^{T_p} \sum_{y=1}^{T_q} e_{pq} \left((Ap + Bq) \left[a_1 \vartheta_1^{k^{x\alpha p + y\alpha q}} + \dots + a_r \vartheta_r^{k^{x\alpha p + y\alpha q}} \right] \right) e_T(j(A_1 T_p + B_1 T_q)[x\alpha p + y\alpha q]) \right| \\ &= \left| \sum_{x=1}^{T_p} \sum_{y=1}^{T_q} e_p \left(B \left[a_1 \vartheta_1^{k^{x\alpha p + y\alpha q}} + \dots + a_r \vartheta_r^{k^{x\alpha p + y\alpha q}} \right] \right) e_{T_p}(jB_1 x) \right. \\ & \quad \cdot \left. e_q \left(A \left[a_1 \vartheta_1^{k^{x\alpha p + y\alpha q}} + \dots + a_r \vartheta_r^{k^{x\alpha p + y\alpha q}} \right] \right) e_{T_q}(jA_1 y) \right| \end{aligned}$$

Since, according to the observation above, the sequence $\{a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}\}$ has period T_p modulo p and period T_q modulo q , it is sufficient to consider the exponents modulo T_p and modulo T_q respectively.

$$\begin{aligned} & \left| \sum_{x=1}^{T_p} \sum_{y=1}^{T_q} e_p(B[a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}]) e_{T_p}(jB_1 x) e_q(A[a_1 \vartheta_1^{k^y} + \dots + a_r \vartheta_r^{k^y}]) e_{T_q}(jA_1 y) \right| \\ &= \left| \sum_{x=1}^{T_p} e_p(B[a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}]) e_{T_p}(jB_1 x) \right| \cdot \left| \sum_{y=1}^{T_q} e_q(A[a_1 \vartheta_1^{k^y} + \dots + a_r \vartheta_r^{k^y}]) e_{T_q}(jA_1 y) \right| \end{aligned}$$

Applying the estimates of Lemma 1.4. and Lemma 1.5. completes the proof of Lemma 3.1.

Lemma 3.2. *Let a_i, ϑ_i for $1 \leq i \leq r$ and N_p, N_q be as in Lemma 3.1, and assume that $M, L \in \mathbb{N}$ with $L < T$. Then there exists a constant $\varepsilon(r, \delta) = \varepsilon_1 > 0$, depending only on r and δ , such that*

$$\left| \sum_{x=M}^{M+L} e_{pq}(a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}) \right| \ll (t_p t_q T_p T_q)^{\frac{1}{2}} \left(p^{-\varepsilon_1} + \frac{(r+1)^{r/2}}{N_p^{1/2}} \right) \left(q^{-\varepsilon_1} + \frac{(r+1)^{r/2}}{N_q^{1/2}} \right) \log pq.$$

Furthermore, if $(h_1, t_p) = 1$ and $(h_1, t_q) = 1$ also hold, then $(r+1)^{r/2}$ can be replaced by $(r+1)^{1/2}$.

$$\left| \sum_{x=M}^{M+L} e_{pq}(a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}) \right| \ll (t_p t_q T_p T_q)^{\frac{1}{2}} \left(p^{-\varepsilon_1} + \frac{(r+1)^{1/2}}{N_p^{1/2}} \right) \left(q^{-\varepsilon_1} + \frac{(r+1)^{1/2}}{N_q^{1/2}} \right) \log pq,$$

where the implied constants are absolute.

Lemma 3.3. *Let $\eta \geq 2$ be an integer, $\varepsilon_2 > 1/4$, and let $t_p > p^{1/2+\nu}$, $t_q > q^{1/2+\mu}$ for some $\nu, \mu > 0$. Let $a_i, \vartheta_i = \vartheta^{k^{i-1}}$ for $1 \leq i \leq r$ be as in Lemma 3.1, and $M, L \in \mathbb{N}$ with $L < T$. Then*

$$\left| \sum_{x=M}^{M+L} e_{pq}(a_1 \vartheta^{k^x} + a_2 \vartheta^{k^{x+1}} \dots + a_r \vartheta^{k^{x+r-1}}) \right| \ll k^{2\varepsilon_2(r-1)} (T_p T_q)^{1 - \frac{2\eta+1}{2\eta(\eta+1)}} (t_p t_q)^{\frac{1}{2\eta}} (pq)^{\frac{1}{4(\eta+1)}} \log pq,$$

where the implied constant depends only on ε_2 , ν and μ . In the special case where $r = 1$, the following holds:

$$\left| \sum_{x=M}^{M+L} e_{pq}(a_1 \vartheta^{k^x}) \right| \ll (T_p T_q)^{1 - \frac{2\eta+1}{2\eta(\eta+1)}} (t_p t_q)^{\frac{1}{2\eta}} (pq)^{\frac{1}{4(\eta+1)}} \log pq,$$

where the implied constant depends only on ν and μ .

Proof of Lemma 3.2. and Lemma 3.3. The proof is essentially the same as those of Lemma 1.6. and Lemma 1.7. in the paper of Gyarmati .

Let $S = \left| \sum_{x=M}^{M+L} e_{pq}(a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}) \right|$. We will use the following well-known identity:

$$\sum_{j=1}^T e_T(jn) = \begin{cases} T, & \text{if } T|n, \\ 0, & \text{otherwise.} \end{cases}$$

Using the previous identity, we can write:

$$S = \frac{1}{T} \left| \sum_{y=1}^T e_{pq} (a_1 \vartheta_1^{k^y} + \dots + a_r \vartheta_r^{k^y}) \sum_{x=M}^{M+L} \sum_{j=1}^T e_T(j(y-x)) \right|$$

By rearranging the sums and applying the triangle inequality, we obtain

$$\begin{aligned} & \left| \sum_{x=1}^T e_{pq} (a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}) e_T(jx) \right| \\ & \ll (t_p t_q T_p T_q)^{1/2} \left(p^{-\varepsilon_1} + \frac{(r+1)^{1/2}}{N_p^{1/2}} \right) \left(q^{-\varepsilon_1} + \frac{(r+1)^{1/2}}{N_q^{1/2}} \right). \end{aligned}$$

In the special case where $\vartheta_i = \vartheta^{k^{i-1}}$ for $1 \leq i \leq r$, we can only state the estimate for integers $\eta \geq 2$:

$$\begin{aligned} & \left| \sum_{x=1}^T e_{pq} (a_1 \vartheta^{k^x} + \dots + a_r \vartheta^{k^{x+r-1}}) e_T(jx) \right| \ll \gamma k^{2\varepsilon_2(r-1)} (\hat{T}_p \hat{T}_q)^{1 - \frac{2\eta+1}{2\eta(\eta+1)}} (t_p t_q)^{\frac{1}{2\eta}} (pq)^{\frac{1}{4(\eta+1)}} \\ & \ll \gamma^{\frac{4\eta+2}{2\eta(\eta+1)} - 1} k^{2\varepsilon_2(r-1)} (T_p T_q)^{1 - \frac{2\eta+1}{2\eta(\eta+1)}} (t_p t_q)^{\frac{1}{2\eta}} (pq)^{\frac{1}{4(\eta+1)}}, \end{aligned}$$

where $\frac{4\eta+2}{4\eta(\eta+1)} - 1 \leq 0$ if $\eta \geq 2$.

The results obtained for incomplete sums can be established in an analogous manner.

$$\frac{1}{T} \sum_{j=1}^T \left| \sum_{x=M}^{M+L} e_T(-jx) \right| \left| \sum_{y=1}^T e_{pq} (a_1 \vartheta_1^{k^y} + \dots + a_r \vartheta_r^{k^y}) e_T(jy) \right|$$

Now, let

$$Q := \max_j \left| \sum_{y=1}^T e_{pq} (a_1 \vartheta_1^{k^y} + \dots + a_r \vartheta_r^{k^y}) e_T(jy) \right|.$$

Thus, we obtain:

$$S \leq \frac{1}{T} \sum_{j=1}^T \left| \sum_{x=M}^{M+L} e_T(-jx) \right| Q.$$

By applying the formula for the sum of a geometric series, the triangle inequality, and the standard identity $|1 - e(x)| \geq 4 \|x\|$, we get

$$\sum_{j=1}^T \left| \sum_{x=M}^{M+L} e_T(-jx) \right| \leq \sum_{j=1}^T \frac{2}{|1 - e(\frac{-j}{T})|} \leq \frac{1}{2} \sum_{j=1}^T \frac{1}{||j/T||} = T \sum_{j=1}^T \frac{1}{j} \ll T \log T.$$

Applying the estimates of Lemma 3.1. to Q , Lemma 3.2. and Lemma 3.3. follow. $\square$

It remains to treat the case where $(T_p, T_q) \neq 1$. In this case, we can reduce the calculation to the one described above. For this, we will use a lemma from the paper of Friedlander and Shparlinski [8].

Lemma 3.4. *If the sequence (u_n) is purely periodic with period T , then for integers $\lambda \geq 0$ and $\gamma \geq 1$, the sequence $(u_{\lambda+\gamma n})$ is purely periodic with period $\frac{T}{(T, \gamma)}$.*

Proof of Lemma 3.4.

See [8] Lemma 2.6.

Let $\gamma := (T_p, T_q)$ and let us write the complete sum under investigation as follows:

$$\begin{aligned} \left| \sum_{x=1}^T e_{pq}(a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}) e_T(jx) \right| &= \left| \sum_{\lambda=0}^{\gamma-1} \sum_{n=1}^{T/\gamma} e_{pq}(a_1 \vartheta_1^{k^{\lambda+n\gamma}} + \dots + a_r \vartheta_r^{k^{\lambda+n\gamma}}) e_T(j(\lambda + n\gamma)) \right| \\ &= \left| \sum_{\lambda=0}^{\gamma-1} e_T(j\lambda) \sum_{n=1}^{T/\gamma} e_{pq}(a_1 \vartheta_1^{k^{\lambda+n\gamma}} + \dots + a_r \vartheta_r^{k^{\lambda+n\gamma}}) e_{T/\gamma}(jn) \right| \\ &\leq \sum_{\lambda=0}^{\gamma-1} \left| \sum_{n=1}^{T/\gamma} e_{pq}(a_1 \xi_{\lambda,1}^{k^n} + \dots + a_r \xi_{\lambda,r}^{k^n}) e_{T/\gamma}(jn) \right|, \end{aligned}$$

where $\xi_{\lambda,i} := \vartheta_i^{k^\lambda}$ and $\hat{k} := k^\gamma$.

By Lemma 3.4, the sequence $\{a_1 \xi_1^{\hat{k}^n} + \dots + a_r \xi_r^{\hat{k}^n}\}$ is purely periodic with period T/γ , since the sequence $\{a_1 \vartheta_1^{k^n} + \dots + a_r \vartheta_r^{k^n}\}$ was purely periodic with period T . It is clear that the orders of $\xi_{\lambda,i}$ modulo p and modulo q are t_p and t_q respectively, since these are terms of our original sequence. Furthermore, the periods $\hat{T}_p$ and $\hat{T}_q$ of the new sequence modulo p and modulo q will be coprime, since they are divisors of T_p/γ and T_q/γ respectively. Thus, we can apply the previously established results:

$$\begin{aligned} \left| \sum_{n=1}^{T/\gamma} e_{pq}(a_1 \xi_{\lambda,1}^{\hat{k}^n} + \dots + a_r \xi_{\lambda,r}^{\hat{k}^n}) e_{T/\gamma}(jn) \right| &\ll (t_p t_q \hat{T}_p \hat{T}_q)^{\frac{1}{2}} \left(p^{-\varepsilon_1} + \frac{(r+1)^{r/2}}{\hat{N}_p^{1/2}} \right) \left(q^{-\varepsilon_1} + \frac{(r+1)^{r/2}}{\hat{N}_q^{1/2}} \right) \\ &\ll \left(t_p t_q \cdot \frac{T_p T_q}{\gamma^2} \right)^{1/2} \left(p^{-\varepsilon_1} + \frac{(r+1)^{r/2}}{\hat{N}_p^{1/2}} \right) \left(q^{-\varepsilon_1} + \frac{(r+1)^{r/2}}{\hat{N}_q^{1/2}} \right). \end{aligned}$$

Note that $\widehat{N}_p = N_p$ and $\widehat{N}_q = N_q$ since $(k^i h_j, t_p) = (k^{\gamma_i} h_j k^\lambda, t_p)$, $(k^{i_1} h_{j_1} - k^{i_2} h_{j_2}, t_p) = (k^{\gamma_{i_1}} h_{j_1} k^\lambda - k^{\gamma_{i_2}} h_{j_2} k^\lambda, t_p)$, because $(k, t_p) = 1$. The same argument applies to q . Thus, estimating the original sum, we obtain:

$$\left| \sum_{x=1}^T e_{pq}(a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}) e_T(jx) \right| \ll (t_p t_q T_p T_q)^{1/2} \left(p^{-\varepsilon_1} + \frac{(r+1)^{1/2}}{N_p^{1/2}} \right) \left(q^{-\varepsilon_1} + \frac{(r+1)^{1/2}}{N_q^{1/2}} \right).$$

In the special case where $\vartheta_i = \vartheta^{k^{i-1}}$ for $1 \leq i \leq r$, we can only state the estimate for integers $\eta \geq 2$:

$$\left| \sum_{x=1}^T e_{pq}(a_1 \vartheta^{k^x} + \dots + a_r \vartheta^{k^{x+r-1}}) e_T(jx) \right| \ll \gamma k^{2\varepsilon_2(r-1)} (\widehat{T}_p \widehat{T}_q)^{1 - \frac{2\eta+1}{2\eta(\eta+1)}} (t_p t_q)^{\frac{1}{2\eta}} (pq)^{\frac{1}{4(\eta+1)}} \\ \ll \gamma^{\frac{4\eta+2}{2\eta(\eta+1)} - 1} k^{2\varepsilon_2(r-1)} (T_p T_q)^{1 - \frac{2\eta+1}{2\eta(\eta+1)}} (t_p t_q)^{\frac{1}{2\eta}} (pq)^{\frac{1}{4(\eta+1)}},$$

where $\frac{4\eta+2}{4\eta(\eta+1)} - 1 \leq 0$ if $\eta \geq 2$.

The results obtained for incomplete sums can be established in an analogous manner.

In the following, we will use additive characters to estimate the pseudorandom measures, following the approach of Rivat and Sárközy [13] as well as Gyarmati .

Lemma 3.5. *For any $n \in \mathbb{N}$, let $r_m(n)$ denote the unique integer $r \in \{0, \dots, m-1\}$ such that $n \equiv r \pmod{m}$. Then for any odd integer m , there exists a function $v_m(a, x): \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{C}$ such that*

$$\frac{1}{m} \sum_{|a| < m/2} v_m(a, x) e_m(an) = \begin{cases} 1, & \text{if } r_m(n) \equiv x \pmod{2}, \\ 0, & \text{if } r_m(n) \not\equiv x \pmod{2}. \end{cases}$$

Furthermore

$$v_m(0, x) = \begin{cases} \frac{m+1}{2}, & \text{if } x \equiv 0 \pmod{2}, \\ \frac{m-1}{2}, & \text{if } x \equiv 1 \pmod{2}, \end{cases}$$

and for $1 \leq |a| < m/2$,

$$|v_m(a, x)| \ll \frac{m}{\min\{|a|, m - 2|a|\}}.$$

Proof of Lemma 3.5.

See [9] Lemma 8.

Using this, the following lemma is easily obtained.

Lemma 3.6. *For any $n \in \mathbb{N}$ and an odd integer m ,*

$$\frac{1}{m} \sum_{|a| < m/2} v_m(a) e_m(an) = \begin{cases} +1, & \text{if } r_m(n) \equiv 0 \pmod{2}, \\ -1, & \text{if } r_m(n) \equiv 1 \pmod{2}, \end{cases}$$

where $v_m(a) = v_m(a, 0) - v_m(a, 1)$, and

$$|v_m(0)| = 1, \quad |v_m(a)| \ll \frac{m}{\min\{|a|, m-2|a|\}} \quad (1 \leq |a| < m/2).$$

Proof of Theorem 2.1. We divide the proof into three cases:

- 1) $t_p \leq p^{11/12}$ and $t_q \leq q^{11/12}$,
- 2) $t_p \leq p^{11/12}$ and $t_q > q^{11/12}$ (or $t_p > p^{11/12}$ and $t_q \leq q^{11/12}$),
- 3) $t_p > p^{11/12}$ and $t_q > q^{11/12}$.

In Case 1, the result is trivial, since any pseudorandom measure is bounded by T , and here $T \leq t \leq t_p t_q \leq m^{11/12}$. For the rest of the proof, $\mathcal{W}(E_T)$ can be expressed as

$$\mathcal{W}(E_T) = \max_{a,b,M} |U(E_T, M, a, b)| = \max_{a,b,M} \left| \sum_{j=1}^M e_{a+jb} \right|,$$

where $a \in \mathbb{Z}$, $b, M \in \mathbb{N}$, and $1 \leq a + b \leq a + Mb \leq T$. Using the triangle inequality and the representation from Lemma 3.6, we obtain:

$$\begin{aligned} \left| \sum_{j=1}^M e_{a+jb} \right| &= \frac{1}{m} \left| \sum_{|a_1| < m/2} v_m(a_1) \sum_{j=1}^M e_m(a_1 u_{a+jb}) \right| \\ &\leq \frac{1}{m} \sum_{|a_1| < m/2} |v_m(a_1)| \cdot \left| \sum_{j=1}^M e_m(a_1 u_{a+jb}) \right| \end{aligned}$$

Separating the terms according to the value of (a_1, m) , the right-hand side can be written as

$$\frac{1}{m} (|v_m(0)|M + S_1 + S_p + S_q),$$

where

$$S_1 = \sum_{\substack{|a_1| < m/2 \\ (a_1, m) = 1}} |v_m(a_1)| \cdot \left| \sum_{j=1}^M e_m(a_1 u_{a+jb}) \right|,$$

$$S_p = \sum_{\substack{|a_1| < p/2 \\ a_1 \neq 0}} |v_m(qa_1)| \cdot \left| \sum_{j=1}^M e_m(qa_1 u_{a+jb}) \right|,$$

and S_q is defined analogously by swapping p and q :

$$S_q = \sum_{\substack{|a_1| < q/2 \\ a_1 \neq 0}} |v_m(pa_1)| \cdot \left| \sum_{j=1}^M e_m(pa_1 u_{a+jb}) \right|.$$

Let $\hat{u}_j = (\vartheta^{k^a})^{(k^b)^j}$ and the period of $\hat{u}_j$ modulo m be $\hat{T} \leq T$, and its periods modulo p and modulo q be $\hat{T}_p$ and $\hat{T}_q$, respectively.

Now let us study Case 2, when $t_p \leq p^{11/12}$ and $t_q > q^{11/12}$. In this case, we cannot apply Lemma 3.3. directly to S_1 , but we can estimate the complete sum similarly to the proof of Lemma 3.1:

$$\begin{aligned} & \left| \sum_{j=1}^{\hat{T}} e_m(a_1 \hat{u}_j) e_{\hat{T}}(\hat{j}x) \right| = \left| \sum_{\lambda=0}^{\gamma-1} \sum_{n=1}^{\hat{T}/\gamma} e_m(a_1 \hat{u}_{\lambda+n\gamma}) e_{\hat{T}}(\hat{j}(\lambda + n\gamma)) \right| \\ &= \left| \sum_{\lambda=0}^{\gamma-1} e_{\hat{T}}(\hat{j}\lambda) \sum_{n=1}^{\hat{T}/\gamma} e_m(a_1 \hat{u}_{\lambda+n\gamma}) e_{\hat{T}/\gamma}(\hat{j}n) \right| \leq \sum_{\lambda=0}^{\gamma-1} \left| \sum_{n=1}^{\hat{T}/\gamma} e_m(a_1 \xi_{\lambda,n}) e_{\hat{T}/\gamma}(\hat{j}n) \right| \\ &= \sum_{\lambda=0}^{\gamma-1} \left| \sum_{x=1}^{\mathcal{T}_{\lambda,p}} e_p(Ba_1 \xi_{\lambda,x}) e_{\mathcal{T}_{\lambda,p}}(\hat{j}B_1 x) \right| \cdot \left| \sum_{y=1}^{\mathcal{T}_{\lambda,q}} e_q(Aa_1 \xi_{\lambda,y}) e_{\mathcal{T}_{\lambda,q}}(\hat{j}A_1 y) \right|, \end{aligned}$$

where $\hat{j} \in \mathbb{Z}_{\hat{T}}$, $\gamma := (\hat{T}_p, \hat{T}_q)$, $\xi_{\lambda,n} := \hat{u}_{\lambda+n\gamma}$, and $\mathcal{T}_{\lambda,p}, \mathcal{T}_{\lambda,q}$ are the periods of the sequence $\xi_{\lambda,n}$ modulo p and modulo q respectively.

Since $\mathcal{T}_{\lambda,p} \leq \hat{T}_p \leq T_p \leq t_p \leq p^{11/12}$ and $t_q > q^{1/2+\mu}$, we use a trivial estimate for the factor related to p . For the factor related to q , we apply Lemma 1.5. with $r = 1$ and $\eta = 2$:

$$\left| \sum_{j=1}^{\hat{T}} e_m(a_1 \hat{u}_j) e_{\hat{T}}(\hat{j}x) \right| \ll \sum_{\lambda=0}^{\gamma-1} \mathcal{T}_{\lambda,p} \cdot \mathcal{T}_{\lambda,q}^{7/12} t_q^{3/12} q^{1/12} \leq p^{11/12} \cdot \hat{T}_q^{7/12} t_q^{3/12} q^{1/12} \ll m^{11/12}.$$

For the incomplete sum, it follows similarly to Lemmas 3.2. and 3.3. that

$$\left| \sum_{j=1}^M e_m(a_1 \hat{u}_j) \right| \ll m^{11/12} \log m.$$

$$S_1 \ll \sum_{\substack{|a_1| < m/2 \\ (a_1, m) = 1}} |\nu_m(a_1)| \cdot m^{11/12} \log m$$

In Case 3, Lemma 3.3. can be used, and we obtain the same result. To estimate S_p and S_q , let us divide M by $\hat{T}_p$ and $\hat{T}_q$:

$$\begin{aligned} M &= b_p \hat{T}_p + m_p, & b_p, m_p &\in \mathbb{N} \cup \{0\}, & 0 \leq m_p < \hat{T}_p, \\ M &= b_q \hat{T}_q + m_q, & b_q, m_q &\in \mathbb{N} \cup \{0\}, & 0 \leq m_q < \hat{T}_q. \end{aligned}$$

Obviously $M \leq \frac{T}{b} \leq \frac{T_p T_q}{b} \leq T_p \hat{T}_q$, or $\leq \hat{T}_p T_q$, which implies $b_p \leq T_q$, $b_q \leq T_p$.

$$S_p \ll \sum_{|a_1| < p/2} |\nu_m(qa_1)| \cdot (T_q \left| \sum_{j=1}^{\hat{T}_p} e_p(a_1 \hat{u}_j) \right| + \left| \sum_{j=1}^{m_p} e_p(a_1 \hat{u}_j) \right|)$$

Now we use Lemma 1.5. and Lemma 1.7. with $r = 1$ and $\eta = 2$.

$$\begin{aligned} S_p &\ll \sum_{|a_1| < p/2} |\nu_m(qa_1)| \cdot (\hat{T}_p^{7/12} t_p^{3/12} p^{1/12} q + \hat{T}_p^{7/12} t_p^{3/12} p^{1/12} \log p) \\ &\ll \sum_{|a_1| < p/2} |\nu_m(qa_1)| \cdot p^{11/12} q \log p \end{aligned}$$

Similarly, it can be shown that

$$S_q \ll \sum_{|a_1| < q/2} |\nu_m(pa_1)| \cdot pq^{11/12} \log q.$$

According to Lemma 3.6, $|\nu_m(0)| = 1$ and $|\nu_m(a_1)| \ll \frac{m}{\min\{|a_1|, m-2|a_1|\}}$ if $1 \leq |a_1| < \frac{m}{2}$.

$$\frac{1}{m} (M + S_1 + S_p + S_q)$$

$$\begin{aligned}
&\ll \frac{1}{m} \left(M + \left(\sum_{\substack{|a_1| \leq m/3 \\ a_1 \neq 0}} \frac{m}{|a_1|} + \sum_{\substack{m/3 < |a_1| < m/2 \\ a_1 \neq 0}} \frac{m}{m - 2|a_1|} + 1 \right) \cdot m^{11/12} \log m \right. \\
&\quad + \left(\sum_{\substack{|a_1| \leq p/3 \\ a_1 \neq 0}} \frac{m}{q|a_1|} + \sum_{\substack{p/3 < |a_1| < p/2 \\ a_1 \neq 0}} \frac{m}{m - 2q|a_1|} + 1 \right) \cdot p^{11/12} q \log p \\
&\quad \left. + \left(\sum_{\substack{|a_1| \leq q/3 \\ a_1 \neq 0}} \frac{m}{p|a_1|} + \sum_{\substack{q/3 < |a_1| < q/2 \\ a_1 \neq 0}} \frac{m}{m - 2p|a_1|} + 1 \right) \cdot q^{11/12} p \log q \right) \\
&\ll 1 + m^{11/12} (\log m)^2 + p^{11/12} (\log p)^2 + q^{11/12} (\log q)^2 \ll m^{11/12} (\log m)^2
\end{aligned}$$

Proof of Theorem 2.2. We divide the proof into the same three cases as in Theorem 2.1.

Case 1 is similarly trivial, so we deal with Case 2 and Case 3.

Assume that $\varepsilon > 1/4$, $\ell \leq T$, and $0 < M \leq T + 1 - \ell$. Then, according to Lemma 3.5

$$\begin{aligned}
&T(E_T, M, X) = |\{n: 0 \leq n < M, (e_{n+1}, \dots, e_{n+\ell}) = X\}| \\
&= \frac{1}{m^\ell} \left| \sum_{|a_1| < m/2} \cdots \sum_{|a_\ell| < m/2} v_m(a_1, x_1) v_m(a_2, x_2) \cdots v_m(a_\ell, x_\ell) \sum_{n=0}^{M-1} e_m(a_1 u_{n+1} + \cdots + a_\ell u_{n+\ell}) \right| \\
&\leq \frac{1}{m^\ell} \sum_{|a_1| < m/2} \cdots \sum_{|a_\ell| < m/2} |v_m(a_1, x_1) v_m(a_2, x_2) \cdots v_m(a_\ell, x_\ell)| \\
&\quad \cdot \left| \sum_{n=0}^{M-1} e_m(a_1 u_{n+1} + \cdots + a_\ell u_{n+\ell}) \right|.
\end{aligned}$$

If $(a_1, \dots, a_\ell) = (0, \dots, 0)$, then trivially

$$\left| \sum_{n=0}^{M-1} e_m(a_1 u_{n+1} + \cdots + a_\ell u_{n+\ell}) \right| \leq M.$$

By Lemma 3.5, we get that

$$\frac{(m-1)^\ell}{2^\ell} \leq |v_m(0, x_1) v_m(0, x_2) \cdots v_m(0, x_\ell)| \leq \frac{(m+1)^\ell}{2^\ell}.$$

Next, we decompose the sum:

$$\begin{aligned}
& \frac{1}{m^\ell} \sum_{\substack{|a_i| < m/2 \\ (a_i, m)=1}} |v_m(a_1, x_1) \cdots v_m(a_\ell, x_\ell)| \cdot \left| \sum_{n=0}^{M-1} e_m(a_1 u_{n+1} + \cdots + a_\ell u_{n+\ell}) \right| \\
&= \frac{1}{m^\ell} (|v_m(0, x_1) \cdots v_m(0, x_\ell)| \cdot M + S_1 + S_p + S_q),
\end{aligned}$$

where

$$\begin{aligned}
S_1 &= \sum_{\substack{|a_i| < m/2 \\ (a_i, m)=1}} |v_m(a_1, x_1) \cdots v_m(a_\ell, x_\ell)| \cdot \left| \sum_{n=0}^{N-1} e_m(a_1 u_{n+1} + \cdots + a_\ell u_{n+\ell}) \right|, \\
S_p &= \sum_{\substack{|a_i| < p/2 \\ (a_1, \dots, a_\ell) \neq (0, \dots, 0)}} |v_m(qa_1, x_1) \cdots v_m(qa_\ell, x_\ell)| \cdot \left| \sum_{n=0}^{M-1} e_m(qa_1 u_{n+1} + \cdots + qa_\ell u_{n+\ell}) \right|, \\
S_q &= \sum_{\substack{|a_i| < q/2 \\ (a_1, \dots, a_\ell) \neq (0, \dots, 0)}} |v_m(pa_1, x_1) \cdots v_m(pa_\ell, x_\ell)| \cdot \left| \sum_{n=0}^{M-1} e_m(pa_1 u_{n+1} + \cdots + pa_\ell u_{n+\ell}) \right|.
\end{aligned}$$

Similarly, to Theorem 2.1, we use Lemma 3.3. for estimating S_1 , while using Lemma 1.5. and Lemma 1.7. for estimating S_p and S_q with $\varepsilon_2 = \varepsilon$, $r = \ell$ and $\eta = 2$:

$$\begin{aligned}
S_1 &\ll \sum_{\substack{|a_i| < m/2 \\ (a_i, m)=1}} |v_m(a_1, x_1) \cdots v_m(a_\ell, x_\ell)| \cdot k^{2\varepsilon(\ell-1)} m^{11/12} \log m, \\
S_p &\ll \sum_{|a_i| < p/2} |v_m(qa_1, x_1) \cdots v_m(qa_\ell, x_\ell)| \cdot k^{\varepsilon(\ell-1)} p^{11/12} q \log p, \\
S_q &\ll \sum_{|a_i| < q/2} |v_m(pa_1, x_1) \cdots v_m(pa_\ell, x_\ell)| \cdot k^{\varepsilon(\ell-1)} p q^{11/12} \log q.
\end{aligned}$$

Combining these estimates with Lemma 3.5, we obtain

$$|T(E_T, M, X) - M/2^\ell| \ll \frac{1}{m^\ell} \left| \frac{(m+1)^\ell}{2^\ell} M - \frac{M}{2^\ell} \right|$$

$$\begin{aligned}
& + \frac{1}{m^\ell} \left(\prod_{i=1}^{\ell} \left(\sum_{\substack{|a_i| \leq m/3 \\ a_i \neq 0}} \frac{m}{|a_i|} \right) \cdot k^{2\varepsilon(\ell-1)} m^{11/12} \log m + \prod_{i=1}^{\ell} \left(\sum_{\substack{|a_i| \leq p/3 \\ a_i \neq 0}} \frac{m}{q|a_i|} \right) \cdot k^{\varepsilon(\ell-1)} p^{11/12} q \log p \right. \\
& \quad \left. + \prod_{i=1}^{\ell} \left(\sum_{\substack{|a_i| \leq q/3 \\ a_i \neq 0}} \frac{m}{p|a_i|} \right) \cdot k^{\varepsilon(\ell-1)} p q^{11/12} \log q \right) \\
& \ll 1.5 + k^{2\varepsilon(\ell-1)} m^{11/12} (\log m)^{\ell+1} + k^{\varepsilon(\ell-1)} (p^{11/12} (\log p)^{\ell+1} + q^{11/12} (\log q)^{\ell+1}) \\
& \ll k^{2\varepsilon(\ell-1)} m^{11/12} (\log m)^{\ell+1},
\end{aligned}$$

since $\ell < p$, thus

$$\frac{1}{m^\ell} \left| \frac{(m+1)^\ell}{2^\ell} M - \frac{M}{2^\ell} \right| \leq \left(\frac{(m+1)^\ell}{m^\ell} - 1 \right) \frac{M}{2^\ell} \leq \frac{e\ell M}{m2^\ell} \leq \frac{e\ell}{2^\ell} < 1.5.$$

Proof of Theorem 2.3. Using Lemma 3.6, in the case $M + d_\ell \leq N + 1$, we can express the measure as

$$\begin{aligned}
|V(E_N, M, D)| &= \left| \sum_{n=0}^{M-1} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_\ell} \right| \\
&= \frac{1}{m^\ell} \left| \sum_{|a_1| < m/2} \cdots \sum_{|a_\ell| < m/2} v_m(a_1) \cdots v_m(a_\ell) \sum_{n=0}^{M-1} e_m(a_1 u_{n+d_1} + \cdots a_\ell u_{n+d_\ell}) \right| \\
&\leq \frac{1}{m^\ell} \sum_{|a_1| < m/2} \cdots \sum_{|a_\ell| < m/2} |v_m(a_1) \cdots v_m(a_\ell)| \cdot \left| \sum_{n=0}^{M-1} e_m(a_1 u_{n+d_1} + \cdots + a_\ell u_{n+d_\ell}) \right| \\
&= \frac{1}{m^\ell} (M + S_1 + S_p + S_q),
\end{aligned}$$

where

$$\begin{aligned}
S_1 &= \sum_{\substack{|a_i| < m/2 \\ (a_i, m)=1}} |v_m(a_1) \cdots v_m(a_\ell)| \cdot \left| \sum_{n=0}^{M-1} e_m(a_1 u_{n+d_1} + \cdots + a_\ell u_{n+d_\ell}) \right|, \\
S_p &= \sum_{\substack{|a_i| < p/2 \\ (a_1, \dots, a_\ell) \neq (0, \dots, 0)}} |v_m(qa_1) \cdots v_m(qa_\ell)| \cdot \left| \sum_{n=0}^{M-1} e_m(qa_1 u_{n+d_1} + \cdots + qa_\ell u_{n+d_\ell}) \right|,
\end{aligned}$$

$$S_q = \sum_{\substack{|a_i| < q/2 \\ (a_1, \dots, a_\ell) \neq (0, \dots, 0)}} |v_m(pa_1) \cdots v_m(pa_\ell)| \cdot \left| \sum_{n=0}^{M-1} e_m(pa_1 u_{n+d_1} + \cdots + pa_\ell u_{n+d_\ell}) \right|.$$

We will use Lemma 3.2. for estimating S_1 , and Lemma 1.4. and Lemma 1.6. for estimating S_p and S_q , in the case $h_i = k^{d_i}$, the conditions $(h_1, t_p) = 1$ and $(h_1, t_q) = 1$ hold, thus

$$\begin{aligned} S_1 &\ll \sum_{\substack{|a_i| < m/2 \\ (a_i, m)=1}} |v_m(a_1) \cdots v_m(a_\ell)| \cdot (t_p t_q T_p T_q)^{\frac{1}{2}} \left(p^{-\varepsilon_1} + \frac{(\ell+1)^{1/2}}{N_p^{1/2}} \right) \left(q^{-\varepsilon_1} + \frac{(\ell+1)^{1/2}}{N_q^{1/2}} \right) \log m \\ &\ll \sum_{\substack{|a_i| < m/2 \\ (a_i, m)=1}} |v_m(a_1) \cdots v_m(a_\ell)| \cdot m \left(p^{-\varepsilon_1} + \frac{(\ell+1)^{1/2}}{N^{1/2}} \right) \left(q^{-\varepsilon_1} + \frac{(\ell+1)^{1/2}}{N^{1/2}} \right) \log m, \\ S_p &\ll \sum_{|a_i| < p/2} |v_m(qa_1) \cdots v_m(qa_\ell)| \cdot pq \left(p^{-\varepsilon_1} + \frac{(\ell+1)^{1/2}}{N_p^{1/2}} \right) \log p, \\ S_q &\ll \sum_{|a_i| < q/2} |v_m(pa_1) \cdots v_m(pa_\ell)| \cdot pq \left(q^{-\varepsilon_1} + \frac{(\ell+1)^{1/2}}{N_q^{1/2}} \right) \log q. \end{aligned}$$

If $N \leq m^{1/3}$, the result follows immediately, since any pseudorandom measure is trivially bounded by the length of the sequence, N . Thus we can assume that

$$\min\{N_p, N_q\} = N > m^{1/3}.$$

Since $\ell^3 < m$, we have

$$\begin{aligned} S_1 &\ll \sum_{\substack{|a_i| < m/2 \\ (a_i, m)=1}} |v_m(a_1) \cdots v_m(a_\ell)| \cdot m^{1-\varepsilon_1/2}, \\ S_p &\ll \sum_{|a_i| < p/2} |v_m(qa_1) \cdots v_m(qa_\ell)| \cdot p^{1-\varepsilon_1/2} q, \\ S_q &\ll \sum_{|a_i| < q/2} |v_m(pa_1) \cdots v_m(pa_\ell)| \cdot pq^{1-\varepsilon_1/2}. \end{aligned}$$

Thus

$$\frac{1}{m^\ell} (M + S_1 + S_p + S_q) \ll m^{1-\varepsilon_1/2} (\log m)^\ell + p^{1-\varepsilon_1/2} (\log p)^\ell + q^{1-\varepsilon_1/2} (\log q)^\ell \ll m^{1-\varepsilon_1/4},$$

where the implied constant depends only on ε_1 . This yields the desired bound for sufficiently large p and q . For small primes, the existence of a suitable $\varepsilon > 0$ follows from the assumption $N < m^{1/2}$, ensuring $N < m^{1-\varepsilon}$. $\square$

Remark 1. It can be seen that $N < \min\{p, q\} < m^{1/2}$, thus Theorem 2.3. gives a non-trivial estimate if $\varepsilon > 1/2$.

We mention that there are other measures of pseudorandomness, such as the linear complexity and the maximum order complexity. Recently, Chen, Gómez, Gómez-Pérez and Tirkel [4] studied the connection between the correlation measure and these measures. For example, the maximum order complexity can be estimated in terms of the correlation measure. Roughly speaking, sequences with small correlation measure up to a sufficiently large order must have a high maximum order complexity.

4 Generalization

It is easy to see from our proof that the lemmas and theorems can be generalized to a modulus of the form $m = p_1 p_2 \cdots p_n$, where $p_1 < p_2 < \cdots < p_n$ are primes.

Assume that m is of this form, and let $t, T, t_1, T_1, \dots, t_n, T_n$ denote the values defined above for the sequence (u_n) modulo m , modulo $p_1, \dots$, modulo p_n , respectively. Then the following theorems can be proven:

Theorem 4.1.

$$\mathcal{W}(E_T) \ll m^{11/12} (\log m)^2.$$

Theorem 4.2. For every real number $\varepsilon > 1/4$, it holds that

$$\mathcal{N}_\ell(E_T) \ll k^{n\varepsilon(\ell-1)} m^{11/12} (\log m)^{\ell+1},$$

where the implied constant depends only on ε .

Theorem 4.3. Assume that $\ell^{n+1} < m$. For $1 \leq l \leq n$, let $N_l = N_l(\vartheta, k, \delta) \leq T_l$ denote the largest positive integer such that for every $1 \leq i < j \leq 2N_l$

$$(k^j - k^i, t_l) \leq t_l \cdot p_l^{-\delta}.$$

Let $N := \min\{N_1, N_2, \dots, N_n\}$. Then there exists a constant $\varepsilon(\ell, \delta) = \varepsilon > 0$, depending only on ℓ and δ , such that for the sequence E_N

$$\mathcal{C}_\ell(E_N) \leq m^{1-\varepsilon}.$$

The general results can be established by induction on n , following the same arguments as in the proofs of Theorems 2.1–2.3. Since the transition from $n = 2$ to the general case is straightforward and relies on an analogous decomposition of the exponential sums, we omit the repetitive details.

Lemma 4.4. Let $h_i \in \mathbb{Z}_+$ and $\vartheta_i = \vartheta^{h_i}$ for $1 \leq i \leq r$, and let $a_i \in \mathbb{Z}_m^\times$, where $(h_1, \dots, h_r, p_l - 1) = 1$ holds for every $1 \leq l \leq n$. Then the sequence

$$\{a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}\}$$

is periodic modulo m with period T , and its period modulo p_l is T_l . For $1 \leq l \leq n$, let

$$N_l(\vartheta_1, \dots, \vartheta_r, k, \delta) = N_l$$

be the largest integer such that $N_l \leq T_l$, and for all $1 \leq i \leq N_l$ and $1 \leq j \leq r$

$$(k^i h_j, t_l) \leq t_l \cdot p_l^{-\delta},$$

and for every pair $\{i_1, j_1\}, \{i_2, j_2\}$ where $1 \leq i_1, i_2 \leq N_l$ and $1 \leq j_1, j_2 \leq r$

$$(k^{i_1} h_{j_1} - k^{i_2} h_{j_2}, t_l) \leq t_l \cdot p_l^{-\delta} \quad \text{or} \quad (k^{i_1} h_{j_1} - k^{i_2} h_{j_2}, t_l) = t_l.$$

If no such N_l exists, then let $N_l = 1$.

Then there exists $\varepsilon(r, \delta) = \varepsilon_1 > 0$, depending only on r and δ , such that for $j \in \mathbb{Z}_T$

$$|\sum_{x=1}^T e_m(a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}) e_T(jx)| \ll (\prod_{l=1}^n t_l T_l)^{\frac{1}{2}} \prod_{l=1}^n \left(p_l^{-\varepsilon_1} + \frac{(r+1)^{r/2}}{N_l^{1/2}} \right). \text{ If } (h_1, t_l) = 1$$

also holds for every $1 \leq l \leq n$, then $(r+1)^{r/2}$ can be replaced by $(r+1)^{1/2}$:

$$|\sum_{x=1}^T e_m(a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}) e_T(jx)| \ll (\prod_{l=1}^n t_l T_l)^{\frac{1}{2}} \prod_{l=1}^n \left(p_l^{-\varepsilon_1} + \frac{(r+1)^{1/2}}{N_l^{1/2}} \right),$$

where the implied constants are absolute.

If $\vartheta_i = \vartheta^{k^{i-1}}$ for $1 \leq i \leq r$, and $t_l > p_l^{1/2+v_l}$ for some numbers $v_l > 0$ for every $1 \leq l \leq n$, then for any integer $\eta \geq 2$ and $\varepsilon_2 > 1/4$

$$\left| \sum_{x=1}^T e_m(a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x}) e_T(jx) \right| \ll k^{n\varepsilon_2(r-1)} \left(\prod_{l=1}^n T_l \right)^{1 - \frac{2\eta+1}{2\eta(\eta+1)}} \left(\prod_{l=1}^n t_l \right)^{\frac{1}{2\eta}} m^{\frac{1}{4(\eta+1)}},$$

where the implied constant depends only on $\varepsilon_2, v_1, \dots, v_n$.

Lemma 4.5. Let a_i, ϑ_i for $1 \leq i \leq r$ and N_l for $1 \leq l \leq n$ be as in Lemma 4.4, and assume that $M, L \in \mathbb{N}$ and $L < T$. Then there exists a constant $\varepsilon(r, \delta) = \varepsilon_1 > 0$, depending only on r and δ , such that

$$|\sum_{x=M}^{M+L} e_m(a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x})| \ll (\prod_{l=1}^n t_l T_l)^{\frac{1}{2}} \prod_{l=1}^n \left(p_l^{-\varepsilon_1} + \frac{(r+1)^{r/2}}{N_l^{1/2}} \right) \log m.$$

If $(h_1, t_l) = 1$ also holds for every $1 \leq l \leq n$, then $(r+1)^{r/2}$ can be replaced by $(r+1)^{1/2}$:

$$|\sum_{x=M}^{M+L} e_m(a_1 \vartheta_1^{k^x} + \dots + a_r \vartheta_r^{k^x})| \ll (\prod_{l=1}^n t_l T_l)^{\frac{1}{2}} \prod_{l=1}^n \left(p_l^{-\varepsilon_1} + \frac{(r+1)^{1/2}}{N_l^{1/2}} \right) \log m.$$

where the implied constants are absolute.

Lemma 4.6. Let $\eta \geq 2$ be an integer, $\varepsilon_2 > 1/4$, and let $t_l > p_l^{1/2+v_l}$ for some numbers $v_l > 0$ for every $1 \leq l \leq n$. Let $a_i, \vartheta_i = \vartheta^{i-1}$ for $1 \leq i \leq r$ be as in Lemma 4.4, and $M, L \in \mathbb{N}$ with $L < T$. Then

$$\left| \sum_{x=M}^{M+L} e_m(a_1 \vartheta^{k^x} + a_2 \vartheta^{k^{x+1}} \dots + a_r \vartheta^{k^{x+r-1}}) \right| \ll k^{n\varepsilon_2(r-1)} \left(\prod_{l=1}^n T_l \right)^{1 - \frac{2\eta+1}{2\eta(\eta+1)}} \left(\prod_{l=1}^n t_l \right)^{\frac{1}{2\eta}} m^{\frac{1}{4(\eta+1)}} \log m,$$

where the implied constant depends only on $\varepsilon_2, v_1, \dots, v_n$.

In the special case where $r = 1$, the following can be stated:

$$|\sum_{x=M}^{M+L} e_m(a_1 \vartheta^{k^x})| \ll (\prod_{l=1}^n T_l)^{1 - \frac{2\eta+1}{2\eta(\eta+1)}} (\prod_{l=1}^n t_l)^{\frac{1}{2\eta}} m^{\frac{1}{4(\eta+1)}} \log m,$$

where the implied constant depends only on $v_1, \dots, v_n$.

Acknowledgement

I would like to thank Katalin Gyarmati for her valuable guidance and insightful comments.

REFERENCES

- [1] S. Bhakta and I. E. Shparlinski. Exponential sums with sparse polynomials and distribution of the power generator, 2024. URL: <https://arxiv.org/abs/2412.07989>, arXiv: 2412.07989.
- [2] L. Blum, M. Blum, and M. Shub. A Simple Unpredictable Pseudo-Random Number Generator. SIAM Journal on Computing, 15(2):364–383, 1986.
- [3] J. Bourgain. Mordell’s exponential sum estimate revisited. J. Amer. Math. Soc., 18:477–499, 2005.
- [4] Z. Chen, Ana Isabel Gómez, Domingo Gómez-Pérez, and Andrew Tirkel. Correlation measure, linear complexity and maximum order complexity for families of binary sequences. Finite Fields Appl., 78:101977, 2022.
- [5] E. D. El-Mahassni. On the distribution of the power generator over a residue ring for parts of the period. Rev. Mat. Complut., 21(2):319–325, 2008.

- [6] J. B. Friedlander, C. Pomerance, and I. E. Shparlinski. Period of the power generator and small values of Carmichael's function. *Math Comp.*, 70(236):1591–1605, 2001.
- [7] J. B. Friedlander, J. Hansen, and I. E. Shparlinski. Character sums with exponential functions. *Mathematika*, 47:75–85, 2000.
- [8] J. B. Friedlander and I. E. Shparlinski. On the distribution of the power generator. *Math Comp.*, 70(236):1575–1589, 2001.
- [9] K. Gyarmati. Pseudorandom sequences constructed by the power generator. *Period. Math. Hung.*, 52:9–26, 2006.
- [10] C. Mauduit, H. Niederreiter, and A. Sárközy. On pseudorandom $[0,1)$ and binary sequences. *Publ. Math. Debrecen*, 71(3-4):305–324, 2007.
- [11] C. Mauduit and A. Sárközy. On finite pseudorandom binary sequences I: Measures of pseudorandomness, the Legendre symbol. *Acta Arith.*, 82:365–377, 1997.
- [12] A. Ostafe and I. E. Shparlinski. On the power generator and its multivariate analogue. *J. Complexity*, 28(2):238–249, 2012.
- [13] J. Rivat and A. Sárközy. Modular constructions of pseudorandom binary sequences with composite moduli. *Period. Math. Hung.*, 51:75–107, 2005.
- [14] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21:120–126, 1978.

Milan Molnar

Department of Algebra and Number Theory
 Eötvös Loránd University
 Pázmány Péter sétány 1/C
 1117 Budapest
 HUNGARY

Mmilan070709@gmail.com

Received June 3, 2026

Accepted July 22, 2026

Published October 28, 2026