AIMS Mathematics

https://www.aimspress.com/journal/Math

AIMS Mathematics, 9(8): 21455–21470.
DOI: 10.3934/math.20241042
Received: 16 April 2024
Revised: 20 June 2024
Accepted: 24 June 2024
Published: 04 July 2024

Research article

On the correlation of k symbols

Yixin Ren and Huaning Liu*

Research Center for Number Theory and Its Applications, School of Mathematics, Northwest University, Xi'an 710127, Shaanxi, China

* **Correspondence:** Email: hnliu@nwu.edu.cn.

Abstract: In 2002 Mauduit and Sárközy started to study finite sequences of k symbols

$$E_N = (e_1, e_2, \cdots, e_N) \in \mathcal{A}^N,$$

where

$$\mathcal{A} = \{a_1, a_2, \cdots, a_k\}, \quad (k \in \mathbb{N}, k \geq 2)$$

is a finite set of k symbols. Bérczi estimated the pseudorandom measures for a truly random sequence E_N of k symbol. In this paper, we shall study the minimal values of correlation measures for the sequences of k symbols, developing the methods similar to those introduced by Alon, Anantharam, Gyarmati, and Schmidt, among others.

Keywords: pseudorandom sequence; k symbol; correlation measure
Mathematics Subject Classification: 11K45, 94A55, 94A60

1. Introduction

The need for pseudorandom sequences arises in cryptographic applications and many papers have been written on this subject. In [1], Mauduit and Sárközy introduced the following measures of pseudorandomness for finite pseudorandom binary sequences:

$$E_N = (e_1, e_2, \cdots, e_N) \in \{-1, +1\}^N.$$

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

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

where the maximum is taken over all $a, b, t \in \mathbb{N}$ with

$$1 \leq a \leq a + (t-1)b \leq N.$$

The *correlation measure of order l* of E_N is defined as

$$C_l(E_N) = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} \cdots e_{n+d_l} \right|,$$

where the maximum is taken over all

$$D = (d_1, \cdots, d_l)$$

and M with

$$0 \leq d_1 < \cdots < d_l \leq N - M.$$

The sequence E_N can be considered as a "good" pseudorandom sequence if both $W(E_N)$ and $C_l(E_N)$ (at least for small l) are "small" in terms of N. Cassaigne et al. [2, 3] studied the well-distribution measures and correlation measures for the Liouville function. Fouvry et al. [4] examined pseudorandomness measures of Kloosterman sums' signs. Goubin et al. [5] introduced a construction related to the Legendre symbol for binary sequences. Gyarmati [6] utilized the concept of an index discrete logarithm to construct binary sequences with strong pseudorandom properties. Gyarmati [7] studied the psedorandom properties of the power generator, which includes the RSA generator and the Blum-Blum-Shub generator. Liu et al. [8–10] explored pseudorandom binary sequences via multiplicative inverse, Gowers norm, and the Legendre symbol. Louboutin et al. [11] also obtained the quantitative results on the pseudorandomness of the sequence $(-1)^{n+n*}$. Mauduit et al. [12] presented a new construction utilizing properties of additive characters. Mauduit et al. [1, 13] investigated a Champernowne-type sequence, the Rudin-Shapiro sequence and the Thue-Morse sequence, extending the approach that involved Legendre symbols. The pseudorandomness of binary sequences over elliptic curves was analyzed in [14, 15]. Sárközy et al. [16–18] studied binary sequences with strong pseudorandom properties, and utilized character sum estimates by Eichenauer-Hermann and Niederreiter. Cassaigne et al. [19] estimated $W(E_N)$ and $C_l(E_N)$ for a truly random binary lattice.

Proposition 1.1. [19] *For all $\epsilon > 0$, there are numbers*

$$N_0 = N_0(\epsilon)$$

and

$$\delta = \delta(\epsilon) > 0,$$

such that for $N > N_0$ and a random sequence $E_N \in \{-1, +1\}^N$, we have

$$P\left(W(E_N) > \delta N^{\frac{1}{2}}\right) > 1 - \epsilon, \quad P\left(W(E_N) > 6\,(N \log N)^{\frac{1}{2}}\right) < \epsilon.$$

Proposition 1.2. [19] *For all $l \in \mathbb{N}$, $l \geq 2$ and $\epsilon > 0$, there are numbers*

$$N_0 = N_0(\epsilon, l)$$

and

$$\delta = \delta(\epsilon, l) > 0,$$

such that for $N > N_0$ and a random sequence $E_N \in \{-1, +1\}^N$, we have

$$P\left(C_l(E_N) > \delta N^{\frac{1}{2}}\right) > 1 - \epsilon, \quad P\left(C_l(E_N) > 5\left(lN \log N\right)^{\frac{1}{2}}\right) < \epsilon.$$

Alon et al. extended Propositions 1.1 and 1.2 in [20] and provided the lower bound of $C_{2l}(E_N)$ for general sequence $E_N \in \{-1, +1\}^N$ in [21].

Proposition 1.3. [21] *For any integers l and N such that*

$$1 \le l \le \left\lfloor \frac{N}{2} \right\rfloor$$

and any $E_N \in \{-1, 1\}^N$, we have

$$C_{2l}(E_N) \ge \sqrt{\frac{1}{2}\left\lfloor \frac{N}{2l+1} \right\rfloor}.$$

Proposition 1.4. [21] *There is an absolute constant $c > 0$ such that, for any positive integers m and N with*

$$m \le \left\lfloor \frac{N}{3} \right\rfloor$$

and

$$\max\{C_2(E_N), C_4(E_N), \cdots, C_{2m}(E_N)\} \ge c\sqrt{mN}$$

for all $E_N \in \{-1, +1\}^N$.

Proposition 1.5. [21] *Let l and N be positive integers with*

$$2 \le l \le \sqrt{\frac{N}{6}}.$$

If N is large enough, then

$$\max\{C_{2l-2}(E_N), C_{2l}(E_N)\} \ge \sqrt{\frac{1}{2}\left\lfloor \frac{N}{3} \right\rfloor}$$

for all $E_N \in \{-1, +1\}^N$.

Gyarmati [22] provided lower bound for $C_{2m+1}(E_N)C_{2l}(E_N)$ with $2m + 1 > 2l$.

Proposition 1.6. [22] *If $(m, l) \in \mathbb{N}^2$, $2m + 1 > 2l$, and $N \in \mathbb{N}$, then for any $E_N \in \{-1, +1\}^N$, we have*

$$C_{2m+1}(E_N)C_{2l}(E_N) \gg N^{1-\frac{l}{2m+1}}.$$

Anantharam [23] improved Proposition 1.6 in the case $m = l = 1$.

Proposition 1.7. [23] *For any $N \in \mathbb{N}$ big enough and $E_N \in \{-1, +1\}^N$, we have*

$$C_3(E_N)C_2(E_N) \ge \frac{2}{25}N.$$

Gyarmati and Mauduit [24] generalized the results from [22, 23].

Proposition 1.8. [24] *For any positive integers m, l and N, and any $E_N \in \{-1, 1\}^N$, we have*

$$C_{2m+1}(E_N)C_{2l}(E_N) \gg N^{c(m,l)},$$

where the implied constant depends on m and l, where

$$c(m,l) = \begin{cases} 1, & \text{if } m \geq l, \\ \frac{1}{2} + \frac{2m+1}{4l}, & \text{if } m < l. \end{cases}$$

Additionally, they provided the following example showing that Proposition 1.8 is optimal:

Example 1.1. *For*

$$E_N = \{+1, -1, +1, -1, +1, -1, \cdots\},$$

we have

$$C_{2m+1}(E_N) = 1$$

and

$$C_{2l}(E_N) = N - 2l + 1.$$

Aistleitner [25] provided a tail characterisation of the limiting distribution of $W(E_N)/\sqrt{N}$. Schmidt [26] proved that the limiting distribution of

$$C_l(E_N)/\sqrt{2N \log \binom{N}{l-1}}$$

exists, and provided simple proofs of Propositions 1.3 and 1.4. Moreover, Schmidt [26] obtained explicit constants for Proposition 1.4.

Proposition 1.9. [26] *There exists a sequence of real numbers c_r, $c_r > \frac{1}{9}$ for each $r \geq 3$ and*

$$c_r \to \frac{1}{\sqrt{6e}} = 0.2476\ldots$$

as $r \to \infty$, such that for all positive integers m and N with

$$m \leq \left\lfloor \frac{N}{3} \right\rfloor,$$

we have

$$\max\{C_2(E_N), C_4(E_N), \cdots, C_{2m}(E_N)\} \geq c_N \sqrt{mN}$$

for all $E_N \in \{-1, +1\}^N$.

In 2002, Mauduit and Sárközy [27] started to study finite sequences of k symbols

$$E_N = (e_1, e_2, \cdots, e_N) \in \mathcal{A}^N,$$

where

$$\mathcal{A} = \{a_1, a_2, \cdots, a_k\}, \quad (k \in \mathbb{N}, k \geq 2)$$

is a finite set of k symbols. Let

$$\mathcal{E} = \{\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k\}$$

be the set of the k-th roots of unity $e^{\frac{2\pi ij}{k}}$, $j = 1, 2, \cdots, k$. Let $\mathcal{F}$ denote the set of bijections φ: $\mathcal{A} \longleftrightarrow \mathcal{E}$. The *$\mathcal{E}$-well-distribution measure* of E_N is defined by

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

where the maximum is taken over all $\varphi \in \mathcal{F}$ and a, b, $t \in \mathbb{N}$ with

$$1 \leq a \leq a + (t-1)b \leq N.$$

The *$\mathcal{E}$-correlation measure of order l* of E_N is defined as

$$\Gamma_l(E_N) = \max_{\phi,M,D} \left| \sum_{n=1}^{M} \varphi_1\left(e_{n+d_1}\right) \cdots \varphi_l\left(e_{n+d_l}\right) \right|,$$

where the maximum is taken over all

$$\phi = (\varphi_1, \cdots, \varphi_l) \in \mathcal{F}^l, \quad D = (d_1, \cdots, d_l)$$

and M with

$$0 \leq d_1 < \cdots < d_l \leq N - M.$$

The sequences of k symbol are considered as "good" pseudorandom sequences if both $\Delta(E_N)$ and $\Gamma_l(E_N)$ (at least for small l) are "small" in terms of N (in particular, both are $o(N)$ as $N \to \infty$, and ideally it is $N^{\frac{1}{2}+\varepsilon}$). Ahlswede et al. [28, 29] devised "many", "good", PR sequences on k symbols by using multiplicative character and irreducible polynomials. Gomez and Winterhof [30] derived results on the pseudorandomness k symbols sequences of the Fermat quotients modulo p. Two families of sequences of k symbols were constructed using the integers modulo pq for distinct odd primes p and q in [31]. Mak [32] utilized rational functions and multiplicative inverses to construct several pseudorandom sequences of k symbols. Mauduit and Sárközy [27] asked us to say something about the "average" size of the measures. Bérczi [33] estimated $\Delta(E_N)$ and $\Gamma_l(E_N)$ for a truly random sequences of k symbol.

Proposition 1.10. [33] *For all $\epsilon > 0$, there are numbers*

$$N_0 = N_0(\epsilon)$$

and

$$\delta = \delta(\epsilon) > 0$$

such that for $N > N_0$ and a random sequence $E_N \in \mathcal{A}^N$, we have

$$P\left(\Delta(E_N) > \delta k^{-\frac{3}{2}} N^{\frac{1}{2}}\right) > 1 - \epsilon, \quad P\left(\Delta(E_N) > 4k^2 (N \log N)^{\frac{1}{2}}\right) < \epsilon.$$

Proposition 1.11. [33] *For all $k \in \mathbb{N}$, $k \geq 2$ and $\epsilon > 0$, there are numbers*

$$N_0 = N_0(\epsilon)$$

and

$$\delta = \delta(\epsilon) > 0$$

such that for $N > N_0$ and a random sequence $E_N \in \mathcal{A}^N$, we have

$$P\left(\Gamma_l(E_N) > \delta k^{-\frac{3}{2}} N^{\frac{1}{2}}\right) > 1 - \epsilon.$$

Proposition 1.12. [33] *For all even $k \in \mathbb{N}$, $l \in \mathbb{N}$ and $\epsilon > 0$, there are numbers*

$$N_0 = N_0(\epsilon, k, l)$$

such that for $N > N_0$ and a random sequence $E_N \in \mathcal{A}^N$, we have

$$P\left(\Gamma_l(E_N) > 10\,(klN \log N)^{\frac{1}{2}}\right) < \epsilon.$$

In this paper we shall develop the previous research methods to study the correlation measures of sequences of k symbols. Based on the research method of [21, 23, 26], we prove Theorems 1.1–1.4. Inspired by the work of Gyarmati and Mauduit [22, 24], we formulate Problem 1.1. Our results are the following:

Theorem 1.1. *For any integers l and N with*

$$1 \leq l \leq \left\lfloor \frac{N}{2} \right\rfloor$$

and any $E_N \in \mathcal{A}^N$, we have

$$\Gamma_{2l}(E_N) \geq \sqrt{\frac{1}{2} \left\lfloor \frac{N}{2l+1} \right\rfloor}.$$

Theorem 1.2. *Let the sequence $\{c_r\}$ be defined as in Proposition 1.9. Then, for any positive integers m and N with*

$$m \leq \left\lfloor \frac{N}{3} \right\rfloor$$

and for any $E_N \in \mathcal{A}^N$, we have

$$\max\{\Gamma_2(E_N), \Gamma_4(E_N), \cdots, \Gamma_{2m}(E_N)\} \geq c_N \sqrt{mN}.$$

Theorem 1.3. *Let l and N be positive integers with*

$$2 \leq l \leq \sqrt{\frac{N}{6}}.$$

If N is large enough, then for all $E_N \in \mathcal{A}^N$, we have

$$\max\{\Gamma_{2l-2}(E_N), \Gamma_{2l}(E_N)\} \geq \sqrt{\frac{1}{2} \left\lfloor \frac{N}{3} \right\rfloor}.$$

Theorem 1.4. *For any $N \in \mathbb{N}$ large enough and $E_N \in \mathcal{A}^N$, we have*

$$\Gamma_3(E_N)\Gamma_2(E_N) \geq \frac{1}{10}N.$$

Proposition 1.8 and our theorems inspire the following problem:

Problem 1.1. *Let m and l be positive integers. Is it true that for large enough N and every $E_N \in \mathcal{A}^N$, we have*

$$\Gamma_{2m+1}(E_N)\Gamma_{2l}(E_N) \gg_{m,l} N.$$

The rest of this paper is organized as follows. We shall introduce Welch's bound and prove Theorems 1.1–1.3 in Section 2, and we will prove Theorem 1.4 in Section 3.

2. Welch's bound and proof of Theorems 1.1–1.3

Schmidt [26] provided simple proofs for Propositions 1.3 and 1.4 by using Welch's bound on the maximal non-trivial scalar products over a set of vectors.

Lemma 2.1. [34] *Let M and $L \geq 2$ be positive integers, and let $v_1, \cdots, v_L$ be elements of $\mathbb{C}^M$. For*

$$v_i = (v_{i,1}, \cdots, v_{i,M})$$

and

$$v_j = \left(v_{j,1}, \cdots, v_{j,M}\right),$$

we define the scalar product

$$\left\langle v_i, v_j \right\rangle = \sum_{n=1}^{M} v_{i,n}\overline{v_{j,n}},$$

where the bar means complex conjugation. Suppose that

$$\langle v_i, v_i \rangle = M$$

for each i. Then, for all integers $r \geq 1$, we have

$$\max_{i \neq j} \left| \left\langle v_i, v_j \right\rangle \right| \geq \left(\frac{M^{2r}}{L-1} \left(\frac{L}{\binom{M+r-1}{r}} - 1 \right) \right)^{\frac{1}{2r}}.$$

Lemma 2.2. [21, Lemma 2.6] *Let l and n be positive integers with*

$$l \leq \frac{1}{2}\sqrt{n}.$$

If n is large enough, then there is a family $\mathcal{L}$ of l-element subsets of $\{1, 2, \cdots, n\}$ with $|\mathcal{L}| = n$ and such that

$$|L \cap L'| \leq 1$$

for all distinct L and $L' \in \mathcal{L}$.

Now we use Lemma 2.1 to prove Theorems 1.1–1.3. Let

$$E_N = (e_1, e_2, \cdots, e_N) \in \mathcal{A}^N$$

be given and let M be an integer with

$$1 \le M \le N - 1.$$

We write

$$N' = N - M.$$

Next, we fix a family $\mathcal{L}$ of subsets of the set $\{1, 2, \cdots, N'\}$. Let φ be a bijection in $\mathcal{F}$. For

$$1 \le i \le |\mathcal{L}|$$

and $L_i \in \mathcal{L}, L_i \ne \emptyset$, we define the vector

$$v_i = (v_{i,1}, \cdots, v_{i,M})$$

by

$$v_{i,n} = \prod_{x \in L_i} \varphi\left(e_{n+x}\right).$$

Clearly

$$\langle v_i, v_i \rangle = M$$

and for $i \ne j$, we have

$$\left\langle v_i, v_j \right\rangle = \sum_{n=1}^{M} \prod_{x \in L_i \setminus \left(L_i \cap L_j\right)} \varphi(e_{n+x}) \prod_{y \in L_j \setminus \left(L_i \cap L_j\right)} \overline{\varphi(e_{n+y})}.$$

Let $L\Theta L'$ be the symmetric difference of the sets L and L', and let

$$\mathcal{L}^{\Theta} = \{L\Theta L' :\ L, L' \in \mathcal{L}, L \ne L'\},$$
$$K = \left\{|S| :\ S \in \mathcal{L}^{\Theta}\right\}.$$

We get

$$\max\{\Gamma_l(E_N) :\ l \in K\} \ge \max\left\{\left|\left\langle v_i, v_j \right\rangle\right| :\ L_i, L_j \in \mathcal{L}, i \ne j\right\}.$$

Then, from Lemma 2.1, we have for all integers $r \ge 1$,

$$\max\{\Gamma_l(E_N) :\ l \in K\} \ge \left(\frac{M^{2r}}{|\mathcal{L}| - 1}\left(\frac{|\mathcal{L}|}{\binom{M+r-1}{r}} - 1\right)\right)^{\frac{1}{2r}}. \tag{2.1}$$

2.1. *Proof of Theorem 1.1*

We write

$$M = \left\lfloor \frac{N}{2l+1} \right\rfloor, \quad N' = N - M \quad \text{and} \quad t = \left\lfloor \frac{N'}{l} \right\rfloor.$$

Clearly, $1 \leq N' \leq N - 1$ and

$$\begin{aligned} t = \left\lfloor \frac{N'}{l} \right\rfloor &= \left\lfloor \frac{N-M}{l} \right\rfloor \\ &\geq \left\lfloor \frac{N - \frac{N}{2l+1}}{l} \right\rfloor \\ &= \left\lfloor \frac{2N}{2l+1} \right\rfloor \\ &\geq 2\left\lfloor \frac{N}{2l+1} \right\rfloor \\ &= 2M. \end{aligned} \tag{2.2}$$

We take for $\mathcal{L}$ a set system of

$$t = \left\lfloor \frac{N'}{l} \right\rfloor$$

pairwise disjoint l-element subsets $L_1, \cdots, L_t$ of $\{1, 2, \cdots, N'\}$. Noting that $L_i \cap L_j$ is empty for $i \neq j$, and $K = \{2l\}$. By (2.1) and (2.2), we get

$$\begin{aligned} \Gamma_{2l}(E_N) &\geq \left(\frac{M^2}{t-1} \left(\frac{t}{M} - 1 \right) \right)^{\frac{1}{2}} \\ &> \sqrt{M - \frac{M^2}{t}} \geq \sqrt{\frac{M}{2}} \\ &= \sqrt{\frac{1}{2} \left\lfloor \frac{N}{2l+1} \right\rfloor}. \end{aligned}$$

This proves Theorem 1.1.

2.2. *Proof of Theorem 1.2*

Proof. Let m and N with

$$m \leq \frac{N}{3}.$$

Write

$$M = \left\lfloor \frac{N}{3} \right\rfloor \quad \text{and} \quad N' = N - M,$$

we get

$$N' \geq \frac{2}{3} N.$$

We take for $\mathcal{L}$ the set system of all m-element subsets of $\{0, 1, \cdots, N'\}$. Hence,

$$K = \left\{ |S| : \ S \in \mathcal{L}^{\Theta} \right\} = \{2, 4, \cdots, 2m\}.$$

By (2.1) we get

$$\max\{\Gamma_2(E_N),\Gamma_4(E_N),\cdots,\Gamma_{2m}(E_N)\}\geq\left(\frac{M^{2m}}{|\mathcal{L}|-1}\left(\frac{|\mathcal{L}|}{\binom{M+m-1}{m}}-1\right)\right)^{\frac{1}{2m}}.$$

Then, repeating the proof of Theorem 1.3 in [26]. Write

$$N=3M+\delta$$

for some $\delta\in\{0,1,2\}$,

$$\begin{aligned}\left(\frac{M^{2m}}{|\mathcal{L}|-1}\right)^{\frac{1}{2m}}&\geq\left(\frac{M^{2m}}{|\mathcal{L}|}\right)^{\frac{1}{2m}}\\&=\frac{\frac{N-\delta}{3}}{\binom{(2N+\delta+3)/3}{m}^{\frac{1}{2m}}}\\&>\left(\frac{mN}{9^2}\right)^{\frac{1}{2}}.\end{aligned}$$

Define f: $\{1,2,\cdots,\left\lfloor\frac{N}{3}\right\rfloor\}\to\mathbb{Q}$ by

$$f(m)=\frac{\binom{N-M+1}{m}}{\binom{M+m-1}{m}}.$$

A standard calculation shows that f is monotonically increasing for

$$m\leq(N-2M+2)/2,$$

and is monotonically decreasing for

$$m\geq(N-2M+2)/2.$$

Therefore, the minimum value of $f(m)$ is either $f(1)$ or

$$f(\left\lfloor\frac{N}{3}\right\rfloor)=f(m).$$

Moreover, we readily verify that $f(1)>2$ and

$$f(M)\geq\frac{\binom{2M+1}{M}}{\binom{2M-1}{M}}=\frac{2(2M+1)}{M+1}\geq3.$$

Hence,

$$\left(\frac{|\mathcal{L}|}{\binom{M+m-1}{m}}-1\right)^{\frac{1}{2m}}>2^{\frac{1}{2m}}.$$

Finally,

$$\max\{\Gamma_2(E_N),\Gamma_4(E_N),\cdots,\Gamma_{2m}(E_N)\}\geq c_N\sqrt{mN}.$$

This completes the proof of Theorem 1.2. □

2.3. Proof of Theorem 1.3

Proof. Let l and N be positive integers with

$$2 \le l \le \sqrt{\frac{N}{6}}.$$

Write

$$M = \left\lfloor \frac{N}{3} \right\rfloor \quad \text{and} \quad N' = N - M,$$

we get

$$N' = N - M \ge \frac{2}{3}N \ge 2M$$

and

$$l \le \sqrt{\frac{N}{6}} = \frac{1}{2}\sqrt{\frac{2N}{3}} \le \frac{1}{2}\sqrt{N'}.$$

By Lemma 2.2, we obtain a family $\mathcal{L}$ of l-element subsets of $\{1, 2, \cdots, N'\}$ with

$$|\mathcal{L}| = N' \quad \text{and} \quad |L \cap L'| \le 1$$

for any two distinct $L, L' \in \mathcal{L}$. Then, from (2.1), we have

$$\begin{aligned}
\max\{\Gamma_{2l-2}(E_N), \Gamma_{2l}(E_N)\} &\ge \left(\frac{M^2}{|\mathcal{L}|-1}\left(\frac{|\mathcal{L}|}{M} - 1\right)\right)^{\frac{1}{2}} \\
&> \sqrt{M - \frac{M^2}{|\mathcal{L}|}} \\
&\ge \sqrt{\frac{M}{2}} \\
&= \sqrt{\frac{1}{2}\left\lfloor \frac{N}{3} \right\rfloor},
\end{aligned}$$

which proves Theorem 1.3. □

3. Proof of Theorem 1.4

Proof. Let $E_N \in \mathcal{A}^N$ be given and let φ be a bijection in $\mathcal{F}$. Let $L, M \in \mathbb{N}$ with $L + M \le N$. We get

$$\begin{aligned}
&\sum_{n_1=1}^{L}\sum_{n_2=1}^{L}\sum_{n_3=1}^{L}\left|\sum_{d=1}^{M}\varphi\left(e_{n_1+d}\right)\varphi\left(e_{n_2+d}\right)\varphi\left(e_{n_3+d}\right)\right|^2 \\
&= \sum_{n_1=1}^{L}\sum_{n_2=1}^{L}\sum_{n_3=1}^{L}\sum_{d_1=1}^{M}\sum_{d_2=1}^{M}\varphi\left(e_{n_1+d_1}\right)\varphi\left(e_{n_2+d_1}\right)\varphi\left(e_{n_3+d_1}\right)\overline{\varphi\left(e_{n_1+d_2}\right)\varphi\left(e_{n_2+d_2}\right)\varphi\left(e_{n_3+d_2}\right)} \\
&= \sum_{d_1=1}^{M}\sum_{d_2=1}^{M}\left(\sum_{n=1}^{L}\varphi\left(e_{n+d_1}\right)\overline{\varphi\left(e_{n+d_2}\right)}\right)^3
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{d=1}^{M}\left(\sum_{n=1}^{L}\varphi\left(e_{n+d}\right)\overline{\varphi\left(e_{n+d}\right)}\right)^3 + \sum_{\substack{d_1=1\\ d_1\neq d_2}}^{M}\sum_{d_2=1}^{M}\left(\sum_{n=1}^{L}\varphi\left(e_{n+d_1}\right)\overline{\varphi\left(e_{n+d_2}\right)}\right)^3\\
&= ML^3 + \sum_{\substack{d_1=1\\ d_1\neq d_2}}^{M}\sum_{d_2=1}^{M}\left(\sum_{n=1}^{L}\varphi\left(e_{n+d_1}\right)\overline{\varphi\left(e_{n+d_2}\right)}\right)^3\\
&\geq ML^3 - M(M-1)\Gamma_2\left(E_N\right)^3. \qquad (3.1)
\end{aligned}
$$

On the other hand, we also get

$$
\begin{aligned}
&\sum_{n_1=1}^{L}\sum_{n_2=1}^{L}\sum_{n_3=1}^{L}\left|\sum_{d=1}^{M}\varphi\left(e_{n_1+d}\right)\varphi\left(e_{n_2+d}\right)\varphi\left(e_{n_3+d}\right)\right|^2\\
&= 6\sum_{1\leq n_1<n_2<n_3\leq L}\left|\sum_{d=1}^{M}\varphi\left(e_{n_1+d}\right)\varphi\left(e_{n_2+d}\right)\varphi\left(e_{n_3+d}\right)\right|^2\\
&\quad + \sum_{\substack{1\leq n_1,n_2,n_3\leq L\\ \text{except for } n_1<n_2<n_3,\cdots,n_3<n_2<n_1}}\left|\sum_{d=1}^{M}\varphi\left(e_{n_1+d}\right)\varphi\left(e_{n_2+d}\right)\varphi\left(e_{n_3+d}\right)\right|^2\\
&\leq L(L-1)(L-2)\Gamma_3\left(E_N\right)^2 + \left(L^3 - L(L-1)(L-2)\right)\left|\sum_{d=1}^{M}\varphi\left(e_{n_1+d}\right)\varphi\left(e_{n_2+d}\right)\varphi\left(e_{n_3+d}\right)\right|^2\\
&\leq L(L-1)(L-2)\Gamma_3\left(E_N\right)^2 + L(3L-2)M^2. \qquad (3.2)
\end{aligned}
$$

Combining (3.1) and (3.2), we get

$$
ML^3 - M(M-1)\Gamma_2\left(E_N\right)^3 \leq \Lambda \leq L(L-1)(L-2)\Gamma_3\left(E_N\right)^2 + L(3L-2)M^2, \qquad (3.3)
$$

where

$$
\Lambda = \sum_{n_1=1}^{L}\sum_{n_2=1}^{L}\sum_{n_3=1}^{L}\left|\sum_{d=1}^{M}\varphi\left(e_{n_1+d}\right)\varphi\left(e_{n_2+d}\right)\varphi\left(e_{n_3+d}\right)\right|^2.
$$

Switch elements on both sides of the inequality

$$
L^3\Gamma_3\left(E_N\right)^2 + M^2\Gamma_2\left(E_N\right)^3 \geq ML^3 - 3L^2M^2. \qquad (3.4)
$$

Case I. Assume that

$$
\Gamma_2\left(E_N\right) \leq \frac{1}{7}N^{\frac{2}{3}}.
$$

Taking

$$
L = \left\lfloor \frac{6}{7}N \right\rfloor
$$

and

$$
M = \left\lfloor \frac{1}{7}N \right\rfloor
$$

in (3.4), we get

$$\Gamma_3(E_N) \geq \frac{1}{\sqrt{15}} N^{\frac{1}{2}}.$$

Then, from Theorem 1.1, we immediately have

$$\Gamma_3(E_N)\Gamma_2(E_N) \geq \frac{1}{\sqrt{15}} N^{\frac{1}{2}} \cdot \sqrt{\frac{1}{2}\left\lfloor \frac{N}{3} \right\rfloor} \geq \frac{1}{10} N. \tag{3.5}$$

Case II. Suppose that

$$\Gamma_2(E_N) \geq \frac{1}{7} N^{\frac{2}{3}}.$$

If

$$\Gamma_3(E_N) \geq N^{\frac{1}{3}},$$

then

$$\Gamma_3(E_N)\Gamma_2(E_N) \geq N^{\frac{1}{3}} \cdot \frac{1}{7} N^{\frac{2}{3}} = \frac{1}{7} N. \tag{3.6}$$

While if

$$\Gamma_3(E_N) \leq N^{\frac{1}{3}},$$

then we take

$$L = \left\lceil \frac{N}{2} \right\rceil$$

and

$$M = \left\lfloor 4\Gamma_3(E_N)^2 \right\rfloor$$

in (3.4). Hence, for large enough N, we get

$$M^2 \Gamma_2(E_N)^3 \geq ML^3 - L^3 \Gamma_3(E_N)^2.$$

Then,

$$16\Gamma_3(E_N)^4 \Gamma_2(E_N)^3 \geq 3\Gamma_3(E_N)^2 \cdot \frac{N^3}{8}.$$

Therefore,

$$\Gamma_3(E_N)^2 \Gamma_2(E_N)^3 \geq \frac{N^3}{64}.$$

Note that $\Gamma_3(E_N) \geq 1$. Thus, we get

$$\begin{aligned} \Gamma_3(E_N)^3 \Gamma_2(E_N)^3 &= \Gamma_3(E_N) \cdot \Gamma_3(E_N)^2 \Gamma_2(E_N)^3 \\ &\geq \Gamma_3(E_N)^2 \Gamma_2(E_N)^3 \\ &\geq \frac{N^3}{64}. \end{aligned}$$

So, we have

$$\Gamma_3(E_N)\Gamma_2(E_N) \geq \frac{N}{4}. \tag{3.7}$$

Now combining (3.5)–(3.7), we get

$$\Gamma_3(E_N)\Gamma_2(E_N) \geq \frac{1}{10} N.$$

This completes the proof of Theorem 1.4. □

4. Conclusions

In this paper, our focus centered on exploring the lower bounds of correlation measures of sequences composed of k symbols. This research contributes to a deeper understanding of the sequence properties essential for various applications in mathematics and cryptography.

Author contributions

Yixin Ren: writing-review and editing, writing-original draft, validation, resources, methodology, formal analysis, conceptualization. Huaning Liu: writing-review and editing, resources, methodology, supervision, validation, formal analysis, funding acquisition.

Use of AI tools declaration

The authors declare they have used Artificial Intelligence (AI) tools in the creation of this article.
AI tools used: we utilize ChatGPT to implement linguistic adjustments to the first paragraph of the second page and the conclusion of the article.

Acknowledgments

The authors express their gratitude to the referees for their nice suggestions and comments. This paper is supported by National Natural Science Foundation of China under Grant No. 12071368, the Science and Technology Program of Shaanxi Province of China under Grant No. 2024JC-JCQN-04, and Shaanxi Fundamental Science Research Project for Mathematics and Physics under Grant No. 22JSY017.

Conflict of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. C. Mauduit, A. Sárközy, On finite pseudorandom binary sequencs I: measure of pseudorandomness, the Legendre symbol, *Acta Arith.*, **82** (1997), 365–377. http://doi.org/10.4064/AA-82-4-365-377
2. J. Cassaigne, S. Ferenczi, C. Mauduit, J. Rivat, A. Sárközy, On finite pseudorandom binary sequencs III: the Liouville function, I, *Acta Arith.*, **87** (1999), 367–390. http://doi.org/10.4064/AA-87-4-367-390
3. J. Cassaigne, S. Ferenczi, C. Mauduit, J. Rivat, A. Sárközy, On finite pseudorandom binary sequencs IV: the Liouville function, II, *Acta Arith.*, **95** (2000), 343–359. http://doi.org/10.4064/aa-95-4-343-359
4. E. Fouvry, P. Michel, J. Rivat, A. Sárközy, On the pseudorandomness of the signs of Kloosterman sums, *J. Aust. Math. Soc.*, **77** (2004), 425–436. https://doi.org/10.1017/S1446788700014543

5. L. Goubin, C. Mauduit, A. Sárközy, Construction of large families of pseudorandom binary sequences, *J. Number Theory*, **106** (2004), 56–69. https://doi.org/10.1016/j.jnt.2003.12.002
6. K. Gyarmati, On a family of pseudorandom binary sequences, *Period. Math. Hung.*, **49** (2004), 45–63. https://doi.org/10.1007/s10998-004-0522-y
7. K. Gyarmati, Pseudorandom sequences constructed by the power generator, *Period. Math. Hung.*, **52** (2006), 9–26. https://doi.org/10.1007/s10998-006-0009-0
8. H. Liu, A family of pseudorandom binary sequences constructed by the multiplicative inverse, *Acta Arith.*, **130** (2007), 167–180. http://doi.org/10.4064/aa130-2-6
9. H. Liu, Gowers uniformity norm and pseudorandom measures of the pseudorandom binary sequences, *Int. J. Number Theory*, **7** (2011), 1279–1302. https://doi.org/10.1142/S1793042111004137
10. H. Liu, J. Gao, Large families of pseudorandom binary sequences constructed by using the Legendre symbol, *Acta Arith.*, **154** (2012), 103–108. http://doi.org/10.4064/aa154-1-6
11. S. R. Louboutin, J. Rivat, A. Sárközy, On a problem of D. H. Lehmer, *Proc. Amer. Math. Soc.*, **135** (2007), 969–975.
12. C. Mauduit, J. Rivat, A. Sárközy, Construction of pseudorandom binary sequences using additive characters, *Monatsh. Math.*, **141** (2004), 197–208. https://doi.org/10.1007/s00605-003-0112-8
13. C. Mauduit, A. Sárközy, On finite pseudorandom binary sequences. II: the Champernowne, Rudin-Shapiro, and Thue-Morse sequences, a further construction, *J. Number Theory*, **73** (1998), 256–276. https://doi.org/10.1006/jnth.1998.2286
14. L. Mérai, Remarks on pseudorandom binary sequences over elliptic curves, *Fund. Inf.*, **114** (2012), 301–308. https://doi.org/10.3233/FI-2012-630
15. L. Mérai, Construction of pseudorandom binary sequences over elliptic curves using multiplicative characters, *Publ. Math. Debrecen*, **80** (2012), 199–213. https://doi.org/10.5486/PMD.2011.5057
16. C. Mauduit, A. Sárközy, Construction of pseudorandom binary sequences by using the multiplicative inverse, *Acta Math. Hung.*, **108** (2005), 239–252. https://doi.org/10.1007/s10474-005-0222-y
17. J. Rivat, A. Sárközy, Modular constructions of pseudorandom binary sequences with composite moduli, *Period. Math. Hung.*, **51** (2005), 75–107. https://doi.org/10.1007/s10998-005-0031-7
18. A. Sárközy, A finite pseudorandom binary sequence, *Stud. Sci. Math. Hung.*, **38** (2001), 377–384. https://doi.org/10.1556/SScMath.38.2001.1-4.28
19. J. Cassaigne, C. Mauduit, A. Sárközy, On finite pseudorandom binary sequences VII: the measures of pseudorandomness, *Acta Arith.*, **103** (2002), 97–118. http://doi.org/10.4064/AA103-2-1
20. N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira, V. Rödl, Measures of pseudorandomness for finite sequences: typical values, *Proc. London Math. Soc.*, **95** (2007), 778–812. https://doi.org/10.1112/plms/pdm027
21. N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira, V. Rödl, Measures of pseudorandomness for finite sequences: minimal values, *Comb. Probab. Comput.*, **15** (2006), 1–29. https://doi.org/10.1017/S0963548305007170

22. K. Gyarmati, On the correlation of binary sequences, *Stud. Sci. Math. Hung.*, **42** (2005), 79–93. https://doi.org/10.1556/sscmath.42.2005.1.7
23. V. Anantharam, A technique to study the correlation measures of binary sequences, *Discrete Math.*, **308** (2008), 6203–6209. https://doi.org/10.1016/j.disc.2007.11.043
24. K. Gyarmati, C. Mauduit, On the correlation of binary sequences, II, *Discrete Math.*, **312** (2012), 811–818. https://doi.org/10.1016/j.disc.2011.09.013
25. C. Aistleitner, On the limit distribution of the well-distribution measure of random binary sequences, *J. Theor. Nombr. Bordx.*, **25** (2013), 245–259. https://doi.org/10.5802/jtnb.834
26. K. U. Schmidt, The correlation measures of finite sequences: limiting distributions and minimum values, *TTrans. Amer. Math. Soc.*, **369** (2017), 429–446. http://doi.org/10.1090/tran6650
27. C. Mauduit, A. Sárközy, On finite pseudorandom sequences of k symbols, *Indagat. Math.*, **13** (2002), 89–101. https://doi.org/10.1016/S0019-3577(02)90008-X
28. R. Ahlswede, C. Mauduit, A. Sárközy, Large families of pseudorandom sequences of k symbols and their complexity-part I, In: R. Ahlswede, L. Bäumer, N. Cai, H. Aydinian, V. Blinovsky, C. Deppe, et al., *General theory of information transfer and combinatorics*, Springer-Verlag, 2006, 293–307. https://doi.org/10.1007/11889342_16
29. R. Ahlswede, C. Mauduit, A. Sárközy, Large families of pseudorandom sequences of k symbols and their complexity, part II, *Electron. Notes Discrete Math.*, **21** (2005), 199–201. https://doi.org/10.1016/j.endm.2005.07.023
30. D. Gomez, A. Winterhof, Multiplicative character sums of Fermat quotients and pseudorandom sequences, *Period. Math. Hung.*, **64** (2012), 161–168. https://doi.org/10.1007/s10998-012-3747-1
31. Z. Chen, X. Du, C. Wu, Pseudorandomness of certain sequences of k symbols with length pq, *J. Comput. Sci. Technol.*, **26** (2011), 276–282. https://doi.org/10.1007/s11390-011-9434-5
32. K. Mak, More constructions of pseudorandom sequences of k symbols, *Finite Fields Appl.*, **25** (2014), 222–233. https://doi.org/10.1016/j.ffa.2013.09.006
33. B. Gergely, On finite pseudorandom sequences of k symbols, *Period. Math. Hung.*, **47** (2003), 29–44. https://doi.org/10.1023/B:MAHU.0000010809.50836.79
34. L. Welch, Lower bounds on the maximum cross correlation of signals, *IEEE Trans. Inf. Theory*, **20** (1974), 397–399. https://doi.org/10.1109/TIT.1974.1055219