On the correlation of binary sequences, II

Katalin Gyarmati, Christian Mauduit

Abstract

This paper concerns the study of the correlation measures of finite binary sequences, more particularily the dependence of correlation measures of even order and correlation measures of odd order. These results generalize previous results due to Gyarmati [7] and to Anantharam [3] and provide a partial answer to a conjecture due to Mauduit [12]. The last part of the paper concerns the generalization of this study to the case of finite binary n-dimensional lattices.

1 Introduction

In 1997 Mauduit and Sárközy [13] initiated the systematic study of finite binary sequences $E_N = \{e_1, e_2, \dots, e_N\}$ with $e_1, e_2, \dots, e_N \in \{+1, -1\}$ (see [14] for the generalization to k symbols). They proposed to use the following measures of pseudorandomness:

*Research supported by Hungarian National Foundation for Scientific Research, Grants No. K67676, PD72264, French-Hungarian exchange program FR-33/2009, the Agence Nationale de la Recherche, grant ANR-10-BLAN 0103 MUNUM and János Bolyai Research Fellowship.

2000 Mathematics Subject Classification: Primary 11K45.

Key words: pseudorandom sequences, correlation.

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

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

where the maximum is taken over all $a, b, t \in \mathbb{N}$ with $1 \le a \le a+(t-1)b \le N$, while for $k \in \mathbb{N}, k \ge 2$ the *correlation measure of order* k of E_N is defined as

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

where the maximum is taken over all $M \in \mathbb{N}$ and non-negative integers $d_1 < d_2 < \dots < d_k$ such that $M + d_k \le N$.

Since 1997 numerous papers have been written on this subject. In the majority of these papers special sequences are constructed and/or tested for pseudorandomness (see [8] for references), while in [1], [2], [4], [5], [6], [7], [11], [15] and [16] the measures of pseudorandomness are studied. In particular in [4] Cassaigne, Mauduit and Sárközy compared correlations of different order. They proved the following

Theorem A *a) For* $k, \ell, N \in \mathbb{N}$, $k \mid \ell$, $E_N \in \{-1,+1\}^N$ *we have*

$$C_k(E_N) \le N \left(\frac{(\ell!)^{k/\ell}}{k!} \left(\frac{C_\ell(E_N)}{N} \right)^{k/\ell} + \left(\frac{\ell^2}{N} \right)^{k/\ell} \right).$$

b) If $k, N \in \mathbb{N}$ *and* $k \le N$, *then there is a sequence* $E_N \in \{-1,+1\}^N$ *such that if* $\ell \le N/2$, *then*

$$C_\ell(E_N) > (N-\ell)/k - 54k^2 N^{1/2} \log N \quad \text{if } k \mid \ell$$
$$C_\ell(E_N) < 27k^2 \ell N^{1/2} \log N \quad \text{if } k \nmid \ell$$

This result shows some kind of independence between C_k and C_ℓ when $k \nmid \ell$ and $\ell \nmid k$. In this paper we will show a link between C_k and C_ℓ when k and ℓ have different parity.

Cassaigne, Mauduit and Sárközy [4] asked the following related question:

Problem 1. For $N \to \infty$, are there sequences E_N such that $C_2(E_N) = O(\sqrt{N})$ and $C_3(E_N) = O(1)$ simultaneously?

In [12] Mauduit also asked another closely related question

Problem 2. Let $k,\ \ell \geq 2$ be integers. Is it true that for every $E_N \in \{-1,+1\}^N$ we have

$$C_{2k+1}(E_N)C_{2\ell}(E_N) \gg N$$

where the implied constant factor depends only on k and ℓ? Or at least

$$C_{2k+1}(E_N)C_{2\ell}(E_N) \gg N^{c(k,\ell)} \tag{1}$$

where the implied constant factor and the constant $\frac{1}{2} < c(k,\ell) \leq 1$ depend only on k and ℓ?

First Gyarmati [7] solved both Problem 1 and Problem 2 in the weaker form (1) when $k \geq \ell$. The answer follows from the main result of [7]:

Theorem B *If $k,\ell \in \mathbb{N}$, $2k+1 > 2\ell$, $N \in \mathbb{N}$ and $N > 67k^4 + 400$, then for all $E_n \in \{-1,+1\}^N$ we have*

$$\left(17\sqrt{k(2\ell+1)}\ C_{2\ell}\right)^{2k+1} + \left(17\ \frac{2k+1}{2\ell}\right)^{\ell} N^{2k-\ell}C_{2k+1}^2 \geq \frac{1}{9}N^{2k-\ell+1}$$

It follows trivially that

Corollary A *If $k,\ell \in \mathbb{N}$, $\log N \geq 2k+1 > 2\ell$, $N \in \mathbb{N}$ and $N > 67k^4+400$, $E_n \in \{-1,+1\}^N$ and*

$$C_{2\ell}(E_N) < \frac{1}{20\sqrt{k(2\ell+1)}} N^{1-\ell/(2k+1)}$$

then we have

$$C_{2k+1}(E_N) > \frac{1}{8}\left(\frac{2\ell}{17(2k+1)}\right)^{\ell/2} N^{1/2}.$$

Corollary B *If $k,\ell \in \mathbb{N}$, $2k+1 > 2\ell$ then*

$$C_{2k+1}(E_N)C_{2\ell}(E_N) \gg N^{1-\ell/(2k+1)}$$

where the implied constant factor depends only on k and ℓ. (This is the case $c(k,\ell) = 1 - \frac{\ell}{2k+1} > \frac{1}{2}$ in Problem 2.)

Later Anantharam [3] sharpened Theorem A and he proved the following:

Theorem C

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

Theorem C solves Problem 2 in the stronger form in the special case $(2k+1, 2\ell) = (3, 2)$, so (1) holds with $c = 1$.

2 Results

In this paper we would like to generalize the results in the previous section. Theorem B studies only the case $2k+1 > 2\ell$ while Theorem C involves only C_2 and C_3. Here we study the general case, when there is no restriction of the order of the correlation measures. The proof uses methods from [3] and [7]. We will prove the following:

Theorem 1 *There is a constant $c_{k,\ell}$ depending only on k and ℓ such that if*

$$C_{2k+1}(E_N) < c_{k,\ell}N^{1/2}, \tag{2}$$

then

$$C_{2k+1}(E_N)^{2\ell}C_{2\ell}(E_N)^{2k+1} \gg N^{2k+1}, \tag{3}$$

where the implied constant factor depends only on k and ℓ.

Remark 1 Theorem 1 is optimal: For $E_N = \{+1, -1, +1, -1, +1 \dots\}$ we have $C_{2k+1}(E_N) = 1$ and $C_{2\ell}(E_N) = N - 2\ell + 1$.

Remark 2 It is an important question whether condition (2) is necessary in Theorem 1. Cassaigne, Mauduit and Sárközy [4] proved that for every ε and

$N > N_0(\varepsilon)$

$$C_{2k+1}(E_N), C_{2\ell}(E_N) \ll N^{1/2}(\log N)^{1/2} \tag{4}$$

holds with probability $1-\varepsilon$. Fix a sequence E_N for which (4) indeed holds and N is large enough. From (3) and (4)

$$N^{\ell+k+1/2}(\log N)^{\ell+k+1/2} \gg N^{2k+1} \tag{5}$$

follows. Since (5) is true for an N large enough we get from (5):

$$\ell + k + 1/2 \geq 2k+1$$

and thus

$$2\ell \geq 2k+1.$$

But in Theorem 1 2ℓ can be less than $2k+1$ so we need an additional assumption on the size of $C_{2k+1}(E_N)$ and $C_{2\ell}(E_N)$.

Let us see some corollaries of Theorem 1.

Corollary 1 *Suppose that* $C_{2\ell}(E_N) \ll N^{1/2}(\log N)^{1/2}$*, then*

$$C_{2k+1}(E_N) \gg \min\left\{N^{1/2},\ \frac{N^{(2k+1)/(4\ell)}}{(\log N)^{(2k+1)/(4\ell)}}\right\}$$

where the implied constant factor depends on k *and* ℓ*.*

Corollary 2 *If* $C_{2k+1}(E_N) = O(1)$*, then*

$$C_{2\ell}(E_N) \gg N,$$

where the implied constant factor depends on k *and* ℓ*.*

Corollary 3

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

where the implied constant factor depends only on k and ℓ and where

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

Remark 3 Corollary 3 solves Problem 2 in the stronger form when $k \geq \ell$ and in the weaker form (1) when $k < \ell$.

Our method can be adapted in the n-dimensional case. This theory has been extended to n dimensions by Hubert, Mauduit and Sárközy [10]. They introduced the following definitions:

Denote by I_N^n the set of n-dimensional vectors whose coordinates are integers between 0 and $N-1$:

$$I_N^n = \{\mathbf{x} = (x_1, \ldots, x_n) : \ x_1, \ldots, x_n \in \{0, 1, \ldots, N-1\}\}.$$

This set is called an *n-dimensional N-lattice* or briefly an *N-lattice*.

In [10] the definition of binary sequences is extended to more dimensions by considering functions of type

$$e_{\mathbf{x}} = \eta(\mathbf{x}) : \ I_N^n \to \{-1, +1\}.$$

If $\mathbf{x} = (x_1, \ldots, x_n)$ so that $\eta(\mathbf{x}) = \eta((x_1, \ldots, x_n))$ then we will slightly simplify the notation by writing $\eta(\mathbf{x}) = \eta(x_1, \ldots, x_n)$.

Such a function can be visualized as the lattice points of the N-lattice replaced by the two symbols + and −, thus they are called *binary N-lattices*. Binary 2 or 3 dimensional pseudorandom lattices can be used in encryption of digital images.

Gyarmati, Mauduit and Sárközy [9] introduced the correlation measures for binary lattices:

The *correlation measure of order k* of the lattice $\eta : I_N^n \to \{-1,+1\}$ is defined by

$$C_k(\eta) = \max_{B', \mathbf{d_1}, \ldots, \mathbf{d_k}} \left| \sum_{\mathbf{x} \in B'} \eta(\mathbf{x} + \mathbf{d_1}) \cdots \eta(\mathbf{x} + \mathbf{d_k}) \right|,$$

where the maximum is taken over all distinct $\mathbf{d_1}, \ldots, \mathbf{d_k} \in I_N^n$ and all set B of the special form

$$B = \{\mathbf{x} = (x_1, \ldots, x_n) : \ 0 \le x_1 \le t_1(< N), \ldots, \ 0 \le x_n \le t_n(< N)\}$$

such that $B + \mathbf{d_1}, \ldots, B + \mathbf{d_k} \subseteq I_N^n$.

We get in the n-dimensional case

Theorem 2 *There is a constant $c_{k,\ell,n}$ depending only on k, ℓ and n such that for an n-dimensional binary lattice $\eta : \ I_N^n \to \{-1,+1\}$ we have*

$$C_{2k+1}(\eta) < c_{k,\ell,n} N^{n/2},$$

then

$$C_{2k+1}(\eta)^{2\ell} C_{2\ell}(\eta)^{2k+1} \gg N^{n(2k+1)},$$

where the implied constant factor depends only on k, ℓ and n.

We will give a sketch of the proof at the end of the paper.

3 Proof of Theorem 1

Let $L = [N/2]$ and $1 \le M \le N/2$ be integers, where the value of M will be fixed later. Consider the following equation

$$A \overset{\text{def}}{=} \sum_{1 \le n_1 < n_2 < \cdots < n_{2k+1} \le L} \; \sum_{1 \le d_1 < d_2 < \cdots < d_{2\ell} \le M} \; \prod_{j=1}^{2\ell} \prod_{i=1}^{2k+1} e_{n_i+d_j}$$
$$= \sum_{1 \le d_1 < d_2 < \cdots < d_{2\ell} \le M} \; \sum_{1 \le n_1 < n_2 < \cdots < n_{2k+1} \le L} \; \prod_{i=1}^{2k+1} \prod_{j=1}^{2\ell} e_{n_i+d_j} \overset{\text{def}}{=} B.$$

We will use the following lemmas

Lemma 1 *For all $t, A \in \mathbb{N}$, $t \le A$ there is a polynomial $p_{t,A}(x) \in \mathbb{Q}[x]$ with the degree t such that if $x_1, x_2, \ldots, x_A \in \{-1, +1\}$ then*

$$p_{t,A}(x_1 + \cdots + x_A) = \sum_{1 \le i_1 < i_2 < \cdots < i_t \le A} x_{i_1} x_{i_2} \ldots x_{i_t}.$$

Denote the coefficients of $p_{t,A}$ by $a_{r,t,A}$:

$$p_{t,A}(x) = a_{t,t,A} x^t + a_{t-1,t,A} x^{t-1} + \cdots + a_{0,t,A}.$$

Then $a_{r,t,A} = 0$ if $r \not\equiv t \pmod 2$, and $(-1)^{(t-r)/2} a_{r,t,A} \ge 0$ if $r \equiv t \pmod 2$. If t is even we also have:

$$a_{0,t,A} = (-1)^{t/2} \binom{A/2}{t/2}.$$

Proof of Lemma 1. This is Lemma 2 in [7].

Lemma 2

$$|a_{r,t,A}| \le A^{(t-r)/2}.$$

Proof of Lemma 2 This follows from Lemma 3 and Lemma 5 in [7]. (Indeed in [7] by Lemma 3 we get $|a_{r,t,A}| \le d_{i,j} A^{(t-r)/2}$. In [7] ω_j is defined by $d_{0,j} + d_{1,j} + \cdots + d_{j,j}$ in Lemma 4 and in Lemma 5 $d_{i,j} \le \omega_j \le 1$ is proved.)

Next we return to the proof of Theorem 1. First we rearrange A. For a moment we fix the value of $n_1, n_2, \dots, n_{2k+1}$ in the first sum. Next we use Lemma 1 with $t = 2\ell$, $A = M$ and $x_u = \prod_{i=1}^{2k+1} e_{n_i+u}$ for $1 \le u \le M$. We get

$$\begin{aligned} A &= \sum_{1\le n_1<n_2<\dots<n_{2k+1}\le L} \ \sum_{1\le d_1<d_2<\dots<d_{2\ell}\le M} \prod_{j=1}^{2\ell} \prod_{i=1}^{2k+1} e_{n_i+d_j} \\ &= \sum_{1\le n_1<n_2<\dots<n_{2k+1}\le L} p_{2\ell,M}\left(\sum_{u=1}^{M} \prod_{i=1}^{2k+1} e_{n_i+u} \right). \end{aligned}$$

Similarly we rearrange B. For a moment we fix the value of $d_1, d_2, \dots, d_{2\ell}$ in the first sum. Next we use Lemma 1 with $t = 2k+1$, $A = L$ and $x_u = \prod_{j=1}^{2\ell} e_{u+d_j}$ for $1 \le u \le M$. We get

$$\begin{aligned} B &= \sum_{1\le d_1<d_2<\dots<d_{2\ell}\le M} \ \sum_{1\le n_1<n_2<\dots<n_{2k+1}\le L} \prod_{i=1}^{2k+1} \prod_{j=1}^{2\ell} e_{n_i+d_j} \\ &= \sum_{1\le d_1<d_2<\dots<d_{2\ell}\le M} p_{2k+1,L}\left(\sum_{u=1}^{L} \prod_{j=1}^{2\ell} e_{u+d_j} \right). \end{aligned}$$

We denoted the coefficients of $p_{t,A}(x)$ by $a_{r,t,A}$ in Lemma 1. Using these notations we get

$$\begin{aligned} &\sum_{1\le n_1<n_2<\dots<n_{2k+1}\le L} \Bigg(a_{2\ell,2\ell,M} \left(\sum_{u=1}^{M} \prod_{i=1}^{2k+1} e_{n_i+u} \right)^{2\ell} \\ &\qquad + a_{2\ell-1,2\ell,M} \left(\sum_{u=1}^{M} \prod_{i=1}^{2k+1} e_{n_i+u} \right)^{2\ell-1} + \dots + a_{0,2\ell,M} \Bigg) \\ &= \sum_{1\le d_1<d_2<\dots<d_{2\ell}\le M} \Bigg(a_{2k+1,2k+1,L} \left(\sum_{u=1}^{L} \prod_{j=1}^{2\ell} e_{u+d_j} \right)^{2k+1} \\ &\qquad + a_{2k,2k+1,L} \left(\sum_{u=1}^{L} \prod_{j=1}^{2\ell} e_{u+d_j} \right)^{2k} + \dots + a_{0,2k+1,L} \Bigg). \end{aligned} \tag{6}$$

By Lemma 1 $a_{0,2k+1,L}=0$. From this and (6) we get

$$\sum_{1\le d_1<d_2<\cdots<d_{2\ell}\le M}\left(a_{2k+1,2k+1,L}\left(\sum_{u=1}^{L}\prod_{j=1}^{2\ell}e_{u+d_j}\right)^{2k+1}\right.$$
$$\left.+\,a_{2k,2k+1,L}\left(\sum_{u=1}^{L}\prod_{j=1}^{2\ell}e_{u+d_j}\right)^{2k}+\cdots+a_{1,2k+1,L}\left(\sum_{u=1}^{L}\prod_{j=1}^{2\ell}e_{u+d_j}\right)\right)$$
$$-\sum_{1\le n_1<n_2<\cdots<n_{2k+1}\le L}\left(a_{2\ell,2\ell,M}\left(\sum_{u=1}^{M}\prod_{i=1}^{2k+1}e_{n_i+u}\right)^{2\ell}\right.$$
$$\left.+\,a_{2\ell-1,2\ell,M}\left(\sum_{u=1}^{M}\prod_{i=1}^{2k+1}e_{n_i+u}\right)^{2\ell-1}+\cdots+a_{1,2\ell,M}\left(\sum_{u=1}^{M}\prod_{i=1}^{2k+1}e_{n_i+u}\right)\right)$$
$$=\sum_{1\le n_1<n_2<\cdots<n_{2k+1}\le L}a_{0,2\ell,M}.$$

Again by Lemma 1 there is a constant c_1 depending only on k and ℓ such that

$$\left|\sum_{1\le d_1<d_2<\cdots<d_{2\ell}\le M}\left(a_{2k+1,2k+1,L}\left(\sum_{u=1}^{L}\prod_{j=1}^{2\ell}e_{u+d_j}\right)^{2k+1}\right.\right.$$
$$\left.+\,a_{2k,2k+1,L}\left(\sum_{u=1}^{L}\prod_{j=1}^{2\ell}e_{u+d_j}\right)^{2k}+\cdots+a_{1,2k+1,L}\left(\sum_{u=1}^{L}\prod_{j=1}^{2\ell}e_{u+d_j}\right)\right)$$
$$-\sum_{1\le n_1<n_2<\cdots<n_{2k+1}\le L}\left(a_{2\ell,2\ell,M}\left(\sum_{u=1}^{M}\prod_{i=1}^{2k+1}e_{n_i+u}\right)^{2\ell}\right.$$
$$\left.\left.+\,a_{2\ell-1,2\ell,M}\left(\sum_{u=1}^{M}\prod_{i=1}^{2k+1}e_{n_i+u}\right)^{2\ell-1}+\cdots+a_{1,2\ell,M}\left(\sum_{u=1}^{M}\prod_{i=1}^{2k+1}e_{n_i+u}\right)\right)\right|$$
$$\ge c_1L^{2k+1}M^{\ell}. \tag{7}$$

By Lemma 1 $a_{r,t,A}=0$ if $r\not\equiv t \pmod 2$. Using this and the triangleinequality we get from (7)

$$\sum_{1\le d_1<d_2<\dots<d_{2\ell}\le M} \sum_{\substack{r=1 \\ r\equiv 1 \pmod 2}}^{2k+1} |a_{r,2k+1,L}| \left| \sum_{u=1}^{L} \prod_{j=1}^{2\ell} e_{u+d_j} \right|^r$$
$$+ \sum_{1\le n_1<n_2<\dots<n_{2k+1}\le L} \sum_{\substack{r=2 \\ r\equiv 0 \pmod 2}}^{2\ell} |a_{r,2\ell,M}| \left| \sum_{u=1}^{M} \prod_{i=1}^{2k+1} e_{n_i+u} \right|^r \ge c_1 L^{2k+1} M^{\ell}. \quad (8)$$

By the definition of the correlation measures we have

$$\left| \sum_{u=1}^{L} \prod_{j=1}^{2\ell} e_{u+d_j} \right| \le C_{2\ell}(E_N),$$
$$\left| \sum_{u=1}^{M} \prod_{i=1}^{2k+1} e_{n_i+u} \right| \le C_{2k+1}(E_N).$$

By this and (8) we get

$$\sum_{1\le d_1<d_2<\dots<d_{2\ell}\le M} \sum_{\substack{r=1 \\ r\equiv 1 \pmod 2}}^{2k+1} |a_{r,2k+1,L}|\, C_{2\ell}(E_N)^r$$
$$+ \sum_{1\le n_1<n_2<\dots<n_{2k+1}\le L} \sum_{\substack{r=2 \\ r\equiv 0 \pmod 2}}^{2\ell} |a_{r,2\ell,M}|\, C_{2k+1}(E_N)^r \ge c_1 L^{2k+1} M^{\ell}.$$

By this and Lemma 2

$$M^{2\ell} \sum_{\substack{r=1 \\ r\equiv 1 \pmod 2}}^{2k+1} L^{(2k+1-r)/2} C_{2\ell}(E_N)^r + L^{2k+1} \sum_{\substack{r=2 \\ r\equiv 0 \pmod 2}}^{2\ell} M^{(2\ell-r)/2} C_{2k+1}(E_N)^r$$
$$\ge c_1 L^{2k+1} M^{\ell}. \quad (9)$$

Lemma 3

$$C_{2\ell}(E_N) \gg N^{1/2}$$

where the implied constant factor depends only on ℓ.

Proof of Lemma 3 See in [1] and [11].

By this for $1 \le r \le 2k+1$ we have

$$L^{(2k+1-r)/2} C_{2\ell}(E_N)^r \ll C_{2\ell}(E_N)^{2k+1}.$$

Using this and (9) we get there is a constant c_2 depending only on k and ℓ such that

$$\begin{aligned} &c_2 M^{2\ell} C_{2\ell}(E_N)^{2k+1} + L^{2k+1} \sum_{\substack{r=2 \\ r \equiv 0 \pmod 2}}^{2\ell} M^{(2\ell-r)/2} C_{2k+1}(E_N)^r \\ &\ge c_1 L^{2k+1} M^{\ell}. \end{aligned} \tag{10}$$

Now we fix the value of M. Let $M = c_3 C_{2k+1}(E_N)^2$, where the value of the constant c_3 will depend only on k and ℓ. We choose the value of c_3 such that

$$\left\lceil \max_{2 \le r \le 2\ell} \left(\frac{\ell+1}{c_1} \right)^{2/r} \right\rceil \le c_3.$$

Then

$$M^{(2\ell-r)/2} C_{2k+1}(E_N)^r \le \frac{c_1}{\ell+1} M^{\ell} \tag{11}$$

holds. Now we fix the constant $c_{k,\ell}$ in Theorem 1, we put $c_{k,\ell} = \frac{1}{2c_3}$. Then $2c_3 C_{2k+1}(E_N)^2 \le N$, so $M \le N/2$ indeed. By (10) and (11) we get

$$\begin{aligned} c_2 M^{2\ell} C_{2\ell}(E_N)^{2k+1} + L^{2k+1} \frac{c_1 \ell}{\ell+1} M^{\ell} &\ge c_1 L^{2k+1} M^{\ell} \\ c_2 M^{2\ell} C_{2\ell}(E_N)^{2k+1} &\ge \frac{c_1}{\ell+1} L^{2k+1} M^{\ell} \\ M^{2\ell} C_{2\ell}(E_N)^{2k+1} &\ge \frac{c_1}{c_2(\ell+1)} L^{2k+1} M^{\ell}. \end{aligned}$$

Writing $L = [N/2]$ and $M = c_3 C_{2k+1}(E_N)^2$ we get

$$\begin{aligned} c_3^{2\ell} C_{2k+1}(E_N)^{4\ell} C_{2\ell}(E_N)^{2k+1} &\ge \frac{c_1}{c_2(\ell+1)} \left[\frac{N}{2} \right]^{2k+1} c_3^{\ell} C_{2k+1}(E_N)^{2\ell} \\ C_{2k+1}(E_N)^{2\ell} C_{2\ell}(E_N)^{2k+1} &\gg N^{2k+1} \end{aligned}$$

which was to be proved.

The proofs of Corollary 1 and 2 are immediate from Theorem 1.

4 Proof of Corollary 3

If $C_{2k+1}(E_N) \gg N^{1/2}$ then Corollary 3 is trivial since by Lemma 3 $C_{2\ell}(E_N) \gg N^{1/2}$ also holds and then $C_{2k+1}(E_N)C_{2\ell}(E_N) \gg N$. Thus we may assume that $C_{2k+1}(E_N) \ll N^{1/2}$

If $k < \ell$ by Theorem 1 and Lemma 3:

$$\begin{aligned}(C_{2k+1}(E_N)C_{2\ell}(E_N))^{2\ell} &= C_{2k+1}(E_N)^{2\ell}C_{2\ell}(E_N)^{2k+1}C_{2\ell}(E_N)^{2\ell-(2k+1)} \\ &\gg N^{2k+1}C_{2\ell}(E_N)^{2\ell-(2k+1)} \\ &\gg N^{2k+1}N^{\ell-k-1/2} = N^{\ell+k+1/2},\end{aligned}$$

so that

$$C_{2k+1}(E_N)C_{2\ell}(E_N) \gg N^{1/2+(2k+1)/(4\ell)}.$$

If $k \geq \ell$ then by Theorem 1

$$\begin{aligned}(C_{2k+1}(E_N)C_{2\ell}(E_N))^{2k+1} &= C_{2k+1}(E_N)^{2\ell}C_{2\ell}(E_N)^{2k+1}C_{2k+1}(E_N)^{2k-2\ell+1} \\ &\gg N^{2k+1}C_{2k+1}(E_N)^{2k-2\ell+1} \\ &\gg N^{2k+1},\end{aligned}$$

so that

$$C_{2k+1}(E_N)C_{2\ell}(E_N) \gg N.$$

5 Sketch of the proof of Theorem 2

Since the method of the proof is very similar to the proof of Theorem 1 we only write a sketch of the proof.

Let $P_t(S)$ denote the set of those subsets of S which contains exactly t elements. Let $L = [N/2]$ and $1 \le M \le N/2$ be integers where the value of M will be fixed later. In order to compare $C_{2k+1}(\eta)$ and $C_{2\ell}(\eta)$ consider the following equation

$$\begin{aligned} A &\stackrel{\text{def}}{=} \sum_{\{n_1,n_2,\dots,n_{2k+1}\}\in P_{2k+1}(I_L^n)} \ \sum_{\{d_1,d_2,\dots,d_{2\ell}\}\in P_{2\ell}(I_M^n)} \prod_{j=1}^{2\ell} \prod_{i=1}^{2k+1} \eta\,(n_i+d_j) \\ &= \sum_{\{d_1,d_2,\dots,d_{2\ell}\}\in P_{2\ell}(I_M^n)} \ \sum_{\{n_1,n_2,\dots,n_{2k+1}\}\in P_{2k+1}(I_L^n)} \prod_{i=1}^{2k+1} \prod_{j=1}^{2\ell} \eta\,(n_i+d_j) \stackrel{\text{def}}{=} B. \end{aligned}$$

Then by using the same arguments as in the proof of Theorem 1 we get

$$\begin{aligned} &M^{2n\ell} \sum_{\substack{r=1 \\ r\equiv 1 \pmod 2}}^{2k+1} L^{n(2k+1-r)/2} C_{2\ell}(\eta)^r \\ &+ L^{n(2k+1)} \sum_{\substack{r=2 \\ r\equiv 0 \pmod 2}}^{2\ell} M^{(2\ell-r)n/2} C_{2k+1}(\eta)^r \ge c_1 L^{n(2k+1)} M^{n\ell}. \end{aligned} \tag{12}$$

Here we need the following extension of Lemma 3:

Lemma 4 *If $\eta:\ I_N^n \to \{-1,+1\}$ is an n-dimensional binary lattice then*

$$C_{2\ell}(\eta) \gg N^{n/2}$$

where the implied constant factor depends only on ℓ and n.

Proof of Lemma 4 For $n = 1$ this is Lemma 3. For $n = 2$ this is Theorem 4 in [9] and the proof can be easily extended for $n > 2$ thus we omit here the proof.

Using this and (12) we get there are constant c_1 and c_2 depending only on k, ℓ and n such that

$$c_2 M^{2n\ell} C_{2\ell}(\eta)^{2k+1} + L^{n(2k+1)} \sum_{\substack{r=2 \\ r\equiv 0 \pmod 2}}^{2\ell} M^{n(2\ell-r)/2} C_{2k+1}(\eta)^r$$
$$\geq c_1 L^{n(2k+1)} M^{n\ell}. \tag{13}$$

Now we fix the value of M. Let $M = c_3 C_{2k+1}(\eta)^2$, where the value of the constant c_3 will depend only on k and ℓ. We choose the value of c_3 such that

$$\left\lceil \max_{2\leq r\leq 2\ell} \left(\frac{\ell+1}{c_1}\right)^{2/r} \right\rceil \leq c_3.$$

Then similarly to the proof of Theorem 1 from (13) we obtain

$$C_{2k+1}(\eta)^{2\ell} C_{2\ell}(\eta)^{2k+1} \gg N^{n(2k+1)}$$

which was to be proved.

References

[1] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira, V. Rödl, *Measures of pseudorandomness for finite sequences: minimal values*, Combin. Probab. Comput. 15 (2006), no. 1-2, 1-29.

[2] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira, V. Rödl, *Measures of pseudorandomness for finite sequences: typical values*, Proc. Lond. Math. Soc. (3) 95 (2007), no. 3, 778-812.

[3] V. Anantharam, *A technique to study the correlation measures of binary sequences*, Discrete Math. 308, 24 (2008), 6203 -6209.

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

[5] K. Gyarmati, *An inequality between the measures of pseudorandomness*, Ann. Univ. Sci. Budapest. Etvs Sect. Math. 46 (2003), 157-166.

[6] K. Gyarmati, *On a pseudorandom property of binary sequences*, Ramanujan J. 8 (2004), 289-302,

[7] K. Gyarmati, *On the correlation of binary sequences*, Studia Sci. Math. Hungar. 42 (2005), 59-75,

[8] K. Gyarmati, C. Mauduit and A. Sárközy, *Measures of pseudorandomness of binary lattices, I. (The measures Q_k, normality.)*, Acta Arith. 144 (2010), 295-313.

[9] K. Gyarmati, C. Mauduit and A. Sárköy, *Measures of pseudorandomness of binary lattices, III. (Q_k, correlation, normality, minimal values.)*, Unif. Distrib. Theory 5 (2010), 183-207.

[10] P. Hubert, C. Mauduit and A. Sárközy, *On pseudorandom binary lattices*, Acta Arith. 125 (2006), 51-62.

[11] Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, *Measures of pseudorandomness for finie sequences: minimum and typical values*, Proceedings of WORDS‘03, 159-169, TUCS Gen. Publ. 27, Turku Cent. Comput. Sci., Turku 2003.

[12] C. Mauduit, *Construction of pseudorandom finite sequences*, unpublished lecture notes to the conference, Information Theory and Some Friendly Neighbours- ein Wunschkonzert, Bielefeld, 2003.

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

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

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

[16] B. Sziklai, *On the symmetry of finite pseudorandom binary sequences*, Unif. Distrib. Theory, to appear.

Katalin Gyarmati
Eötvös Loránd University
Department of Algebra and Number Theory
H-1117 Budapest, Pázmány Péter sétány 1/C, Hungary
e-mail: gykati@cs.elte.hu
(corresponding author; fax: 36-13812146)

Christian Mauduit
Institut de Mathématiques de Luminy
CNRS, UMR 6206
163 avenue de Luminy, Case 907
F-13288 Marseille Cedex 9, France
e-mail: mauduit@iml.univ-mrs.fr