On the correlation of binary sequences

Katalin Gyarmati*

Abstract

C. Mauduit conjectured that $C_2(E_N)C_3(E_N) \gg N^c$ always holds with some constant $1/2 < c \leq 1$. This will be proved for $c = 2/3$, more exactly if for a sequence $E_N \subseteq \{-1. +1\}^N$ we have $C_2(E_N) \ll N^{2/3}$ then $C_3(E_N) \gg N^{1/2}$. Indeed, a more general theorem is proved, involving correlation measures.

Mathematics Subject Classification 2000 (MSC2000): 11K45.

Keywords and phrases: pseudorandom, correlation measure.

1 Introduction

In 1997 Mauduit and Sárközy [5] initiated the systematic study of finite binary sequences $E_N = (e_1, e_2, \dots, e_N)$ with $e_1, e_2, \dots, e_N \in \{+1, -1\}$. They proposed to use the following measures of pseudorandomness:

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

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

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

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

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

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

Since 1997 about 20 papers have been written on this subject. In the majority of these papers special sequences are constructed and/or tested for pseudorandomness, while in [1], [2], [3] and [6] the measures of pseudorandomness are studied. In particular in [1] Cassaigne, Mauduit and Sárközy compared correlations of different order. They 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?

Recently, Mauduit [4] asked another closely related question

Problem 2. Is it true that for every $E_N \in \{-1, +1\}^N$ we have

$$C_2(E_N)C_3(E_N) \gg N$$

or at least

$$C_2(E_N)C_3(E_N) \gg N^c \tag{1}$$

with some $\frac{1}{2} \leq c \leq 1$?

In this paper I will settle both Problem 1 and Problem 2 in the weaker form (1). The answers will follow from the main result of this paper:

Theorem 1 *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*

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

If follows trivially that

Corollary 1 *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

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

In particular, for $\ell = 1, 2$ *and 3 we obtain:*

(i) if

$$C_2(E_N) < \frac{N^{2/3}}{25\sqrt{\log N}},$$

then

$$C_3(E_N), C_5(E_N), \dots \gg \sqrt{N};$$

(ii) if

$$C_4(E_N) < \frac{N^{3/5}}{32\sqrt{\log N}},$$

then

$$C_5(E_N), C_7(E_N), \dots \gg \sqrt{N};$$

(iii) if

$$C_6(E_N) < \frac{N^{4/7}}{37\sqrt{\log N}},$$

then

$$C_7(E_N), C_9(E_N), \dots \gg \sqrt{N};$$

where the implicit constant may depend on the order of the correlation measure.

From the first statement of Corollary 1 (which is an immediate consequence of Theorem 1), follows the parts (i), (ii) and (iii) by using the inequalities $N^{1-\ell/(2k+1)} \geq N^{1-\ell/(2\ell+1)}$ and $\frac{1}{\sqrt{k}} \geq \frac{1}{\sqrt{\log N/2}}$.

Clearly, (i) in the Corollary answers the question in Problem 1. Moreover, since we have

$$C_k(E_N) \geq 1$$

for all $N \geq k$, thus Problem 2 also follows from (i) with $c = 2/3$.

By Theorem 1 for $N > 467$ we have

$$650C_2^3 + 26NC_3^2 > \frac{1}{32}N^2. \tag{3}$$

For a "truly random sequence" $E_N \in \{-1, +1\}^N$ the left hand side of (3) is $\ll N^{3/2} + N^2$ which shows that the second term is the best possible apart from the constant factor. On the other hand I do not know whether the exponent 3 in the first term is the best possible. In other words, I have not been able to settle the following problem.

Problem 3. Does there exist a sequence $E_N \in \{-1, +1\}^N$ with $C_2(E_N) = O(N^{2/3})$, $C_3(E_N) = o(N^{1/2})$?

Kohayakawa, Mauduit, Moreira and V. Rödl proved the following for the correlation measure of even order in [3]:

Theorem 2 *If k and N are natural numbers with even k and $2 \leq k \leq N$, then*

$$C_k(E_N) > \sqrt{\frac{N}{3(k+1)}}$$

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

2 Proof of Theorem 1

We may suppose that

$$C_{2k+1}(E_N) \le \sqrt{N} \tag{4}$$

otherwise the theorem is trivial. The crucial idea of the proof is the following identity:

Lemma 1 *Let*

$$S_1 \stackrel{def}{=} \sum_{1\le d_1<\cdots<d_{2\ell-1}\le N-(2k+1)} \sum_{\substack{1\le n_1<\cdots<n_{2k+1}\\ \le N-d_{2\ell-1}}} e_{n_1}e_{n_1+d_1}\ldots e_{n_1+d_{2\ell-1}}e_{n_2}\ldots e_{n_2+d_{2\ell-1}}e_{n_{2k+1}}e_{n_{2k+1}+d_1}\ldots e_{n_{2k+1}+d_{2\ell-1}},$$

$$S_2 \stackrel{def}{=} \sum_{1\le d_1<\cdots<d_{2k}\le N-2\ell} \sum_{\substack{1\le n_1<\cdots<n_{2\ell}\\ \le N-d_{2k}}} e_{n_1}e_{n_1+d_1}\ldots e_{n_1+d_{2k}}e_{n_2}e_{n_2+d_1}\ldots e_{n_2+d_{2k}}e_{n_{2\ell}}e_{n_{2\ell}+d_1}\ldots e_{n_{2\ell}+d_{2k}},$$

Then

$$S_1 - S_2 = 0 \tag{5}$$

We will give an upper bound for $S_1 - S_2$ involving $C_{2\ell}$ and C_{2k+1}. But before this we prove Lemma 1.

Proof of Lemma 1. If a product $e_{n_1}\dots e_{n_{2k+1}+d_{2\ell-1}}$ occurs in S_1, then it also occurs in S_2 and vice-versa, because for all terms $e_{n_1}\dots e_{n_{2k+1}+d_{2\ell-1}}$ in S_1 we have

$$e_{n_1}e_{n_1+d_1}\dots e_{n_1+d_{2\ell-1}}e_{n_2}\dots e_{n_2+d_{2\ell-1}}e_{n_{2k+1}}e_{n_{2k+1}+d_1}\dots e_{n_{2k+1}+d_{2\ell-1}} =$$

$$e_{n_1}e_{n_2}\dots e_{n_{2k+1}}e_{n_1+d_1}e_{n_2+d_1}\dots e_{n_{2k+1}+d_1}\dots e_{n_1+d_{2\ell-1}}e_{n_2+d_{2\ell-1}}\dots e_{n_{2k+1}+d_{2\ell-1}}.$$

Here

$$n_{i+1}-n_i = (n_{i+1}+d_1)-(n_i+d_1) = (n_{i+1}+d_2)-(n_i+d_2) = \dots$$
$$= (n_{i+1}+d_{2\ell-1})-(n_i+d_{2\ell-1})$$

for all $1 \le i \le 2k$, which proves that this product also occurs in S_2. Changing the role of S_1 and S_2 we get the inverse statement. Thus indeed $S_1 - S_2 = 0$.

Considering $\sum\limits_{\substack{1\le n_1<\dots<n_{2k+1}\\ \le N-d_{2\ell-1}}} e_{n_1}\dots e_{n_{2k+1}+d_{2\ell-1}}$ in S_1 we see that this is the sum of all possible products containing $2k+1$ terms from the set $e_1e_{1+d_1}\dots e_{1+d_{2\ell-1}}$, $e_2e_{2+d_1}\dots e_{2+d_{2\ell-1}}, \dots, e_{N-d_{2\ell-1}}e_{N-d_{2\ell-1}+d_1}\dots e_N$. A similar situation holds in the case of S_2. We will use the following lemma.

Lemma 2 *For all $j, M \in \mathbb{N}$, $j \le M$ there is a polynomial $p_{j,M}(x) \in \mathbb{Q}[x]$ with the degree j such that if $x_1, x_2, \dots, x_M \in \{-1, +1\}$ then*

$$p_{j,M}(x_1+\dots+x_M) = \sum_{1\le i_1<i_2\dots<i_j\le M} x_{i_1}x_{i_2}\dots x_{i_j}.$$

Denote the coefficients of $p_{j,M}$ by $c_{i,j,M}$:

$$p_{j,M}(x) = c_{j,j,M}x^j + c_{j-1,j,M}x^{j-1} + \dots + c_{0,j,M}.$$

Then $c_{i,j,M} = 0$ if $i \not\equiv j \pmod 2$, and $(-1)^{(j-i)/2}c_{i,j,M} \ge 0$ if $i \equiv j \pmod 2$. If j is even we also have:

$$c_{0,j,M} = (-1)^{j/2}\binom{M/2}{j/2}.$$

Proof of Lemma 2. We will prove this lemma by induction on j. $p_{1,M}(x) = x$ trivially. Since $x_i^2 = 1$, $p_{2,M}(x) = \frac{1}{2}x^2 - \frac{M}{2}$ because

$$\frac{1}{2}(x_1 + \cdots + x_M)^2 - \frac{M}{2} = \frac{1}{2}\left((x_1 + \cdots + x_M)^2 - x_1^2 - \cdots - x_M^2\right)$$
$$= \sum_{1\le i<j\le M} x_i x_j.$$

Thus

$$c_{0,1,M} = 0,\ c_{1,1,M} = 1$$
$$c_{0,2,M} = -M/2,\ c_{1,2,M} = 0,\ c_{2,2,M} = 1/2. \tag{6}$$

Suppose that the polynomials $p_{1,M}, p_{2,M}, \ldots, p_{j-1,M}$ exist. From this we will prove that $p_{j,M}$ also exists.

Using again $x_i^2 = 1$ we get:

$$\sum_{1\le i_1<i_2<\cdots<i_j\le M} x_{i_1}x_{i_2}\ldots x_{i_j} = \frac{1}{j}\sum_{1\le i_1<i_2<\cdots<i_{j-1}\le M} x_{i_1}x_{i_2}\ldots x_{i_{j-1}}(x_1 + \cdots + x_M)$$
$$- \frac{M-(j-2)}{j}\sum_{1\le i_1<i_2<\cdots<i_{j-2}\le M} x_{i_1}x_{i_2}\ldots x_{i_{j-2}}.$$

Thus for $j \ge 3$ we have

$$p_{j,M}(x) = \frac{1}{j}\ x p_{j-1,M}(x) - \frac{M-(j-2)}{j}\ p_{j-2,M}(x).$$

From this we obtain that the following holds for the coefficients $c_{i,j,M}$:

$$c_{i,j,M} = \frac{1}{j}\ c_{i-1,j-1,M} - \frac{M-(j-2)}{j}\ c_{i,j-2,M}. \tag{7}$$

By induction on j, Lemma 2 follows immediately from this recursion. I leave the details to the reader.

By Lemma 2

$$S_1 - S_2 = 0$$

is equivalent with

$$\sum_{1\le d_1<\cdots<d_{2\ell-1}\le N-(2k+1)} p_{2k+1,N-d_{2\ell-1}} \left(\sum_{n=1}^{N-d_{2\ell-1}} e_n e_{n+d_1}\dots e_{n+d_{2\ell-1}}\right)$$

$$- \sum_{1\le d_1<\cdots<d_{2k}\le N-2\ell} p_{2\ell,N-d_{2k}} \left(\sum_{n=1}^{N-d_{2k}} e_n e_{n+d_1}\dots e_{n+d_{2k}}\right) = 0.$$

So:

$$\sum_{1\le d_1<\cdots<d_{2\ell-1}\le N-(2k+1)} p_{2k+1,N-d_{2\ell-1}} \left(\sum_{n=1}^{N-d_{2\ell-1}} e_n e_{n+d_1}\dots e_{n+d_{2\ell-1}}\right)$$

$$- \sum_{1\le d_1<\cdots<d_{2k}\le N-2\ell} \left(p_{2\ell,N-d_{2k}} \left(\sum_{n=1}^{N-d_{2k}} e_n e_{n+d_1}\dots e_{n+d_{2k}}\right) - c_{0,2\ell,N-d_{2k}}\right)$$

$$= \sum_{1\le d_1<\cdots<d_{2k}\le N-2\ell} c_{0,2\ell,N-d_{2k}}.$$

Using the triangle inequality we get:

$$\sum_{1\le d_1<\cdots<d_{2\ell-1}\le N-(2k+1)} \left| p_{2k+1,N-d_{2\ell-1}} \left(\sum_{n=1}^{N-d_{2\ell-1}} e_n e_{n+d_1}\dots e_{n+d_{2\ell-1}}\right)\right|$$

$$+ \sum_{1\le d_1<\cdots<d_{2k}\le N-2\ell} \left| p_{2\ell,N-d_{2k}} \left(\sum_{n=1}^{N-d_{2k}} e_n e_{n+d_1}\dots e_{n+d_{2k}}\right) - c_{0,2\ell,N-d_{2k}}\right|$$

$$\ge \left| \sum_{1\le d_1<\cdots<d_{2k}\le N-2\ell} c_{0,2\ell,N-d_{2k}} \right|. \tag{8}$$

We will give estimates for both side of (8). In order to estimate the right hand side of (8), we need upper bounds for the coefficients of the polynomials $p_{j,M}$.

Definition 1 *Let*

$$d_{0,1} = 0,\ \ d_{1,1} = 1$$

$$d_{0,2} = 1/2,\ \ d_{1,2} = 0,\ \ d_{2,2} = 1/2.$$

If $i < 0$ or $j < i$ let $d_{i,j} = 0$.

For $i > 2$ let

$$d_{i,j} = \frac{1}{j}\left(d_{i-1,j-1} + d_{i,j-2}\right). \tag{9}$$

Lemma 3 *If $j \leq M$ then*

$$|c_{i,j,M}| \leq d_{i,j} M^{(j-i)/2}.$$

Proof of Lemma 3. We will prove the lemma by induction on j. For $j = 1, 2$ by (6) the assertion is trivial. If the lemma holds for $j \leq k-1$ then it also holds for $j = k$ because of triangle-inequality and (7):

$$\begin{aligned} |c_{i,k,M}| &\leq \frac{1}{k}\left|c_{i-1,k-1,M}\right| + \frac{M-(k-2)}{k}\left|c_{i,k-2,M}\right| \leq \frac{1}{k}\left|c_{i-1,k-1,M}\right| + \frac{M}{k}\left|c_{i,k-2,M}\right| \\ &\leq \frac{1}{k} d_{i-1,k-1} M^{(k-i)/2} + \frac{M}{k} d_{i,k-2} M^{(k-i-2)/2} = M^{(k-i)/2} d_{i,k}. \end{aligned}$$

Thus Lemma 3 is proved.

Next we give an upper bound for the polynomial $p_{j,M}$.

Lemma 4 *Let $w_j \stackrel{def}{=} d_{0,j} + d_{1,j} + \cdots + d_{j,j},\ j \leq M$*

(i) If $|x| \leq y,\ v > 0,\ y > \sqrt{\frac{N}{3(v+1)}}$ and $M \leq N$ then

$$|p_{j,M}(x)| \leq (3(v+1))^{j/2}\, w_j\, |y|^j .$$

(ii) If j is even $|x| \leq \sqrt{N}$ and $M \leq N$ then

$$|p_{j,M}(x) - c_{0,j,M}| \leq w_j N^{(j-2)/2} x^2.$$

Proof of Lemma 4. (i) By Lemma 3

$$|c_{i,j,M}| \leq d_{i,j} M^{(j-i)/2} \leq d_{i,j} N^{(j-i)/2}. \tag{10}$$

Using this and $|x| \le y$ we obtain:

$$p_{j,M}(x) \le d_{j,j}y^j + d_{j-1,j}N^{1/2}y^{j-1} + d_{j-2,j}Ny^{j-2} + \cdots + d_{0,j}N^{j/2}$$
$$= y^j\left(d_{j,j} + d_{j-1,j}\frac{N^{1/2}}{y} + \cdots + d_{0,j}\left(\frac{N^{1/2}}{y}\right)^j\right).$$

By $y > \sqrt{\frac{N}{3(v+1)}}$ we have

$$p_{j,M}(x) \le y^j\left(d_{j,j} + d_{j-1,j}(3(v+1))^{1/2} + \cdots + d_{0,j}(3(v+1))^{j/2}\right)$$
$$\le (3(v+1))^{j/2}(d_{j,j} + d_{j-1,j} + \cdots + d_{0,j})y^j = (3(v+1))^{j/2}w_jy^j.$$

which proves (i).

(ii) Since j is even, by Lemma 2 we have $c_{1,j,M} = 0$. Using again (10) we get

$$|p_{j,M}(x) - c_{0,j,M}| \le d_{j,j}x^j + d_{j-1,j}N^{1/2}x^{j-1} + \cdots + d_{2,j}N^{(j-2)/2}x^2$$
$$= x^2\left(d_{j,j}x^{j-2} + d_{j-1,j}N^{1/2}x^{j-3} + \cdots + d_{2,j}N^{(j-2)/2}\right)$$

Because of $x \le N^{1/2}$ we have

$$|p_{j,M}(x) - c_{0,j,M}| \le w_jN^{(j-2)/2}x^2.$$

This completes the proof of Lemma 4.

Using Lemma 4 we are able to estimate the right hand-side of (8). Indeed, by the definition of the correlation measure and Theorem 2 (which was proved in [3]) we have

$$\left|\sum_{n=1}^{N-d_{2\ell-1}} e_ne_{n+d_1}\dots e_{n+d_{2\ell-1}}\right| \le C_{2\ell}(E_N),\ C_{2\ell}(E_N) > \sqrt{\frac{N}{3(2\ell+1)}}.$$

Thus by Lemma 4 (i) we have

$$\left|p_{2k+1,N-d_{2\ell-1}}\left(\sum_{n=1}^{N-d_{2\ell-1}} e_ne_{n+d_1}\dots e_{n+d_{2\ell-1}}\right)\right| \le (3(2\ell+1))^{(2k+1)/2}w_{2k+1}C_{2\ell}^{2k+1}(E_N). \tag{11}$$

On the other hand by (4) we have

$$\left|\sum_{n=1}^{N-d_{2k}} e_n e_{n+d_1}\dots e_{n+d_{2k}}\right| \le C_{2k+1}(E_N) \le \sqrt{N}.$$

Using Lemma 4 (ii) we get

$$\left| p_{2\ell,N-d_{2k}}\left(\sum_{n=1}^{N-d_{2k}} e_n e_{n+d_1}\dots e_{n+d_{2k}}\right) - c_{0,2\ell,N-d_{2k}}\right| \le w_{2\ell} N^{\ell-1} C_{2k+1}^2(E_N). \tag{12}$$

We also have

$$\sum_{1\le d_1<\dots<d_{2\ell-1}\le N-(2k+1)} 1 = \binom{N-(2k+1)}{2\ell-1} \le \frac{N^{2\ell-1}}{(2\ell-1)!},$$
$$\sum_{1\le d_1<\dots<d_{2k}\le N-2\ell} 1 = \binom{N-2\ell}{2k} \le \frac{N^{2k}}{(2k)!}, \tag{13}$$

By (8), (11), (12) and (13) we have

$$(3(2\ell+1))^{(2k+1)/2} w_{2k+1}\frac{N^{2\ell-1}}{(2\ell-1)!}C_{2\ell}^{2k+1} + w_{2\ell}\frac{N^{2k+\ell-1}}{(2k)!}C_{2k+1}^2(E_N)$$
$$\ge \left|\sum_{1\le d_1<\dots<d_{2k}\le N-2\ell} c_{0,2\ell,N-d_{2k}}\right|. \tag{14}$$

The following lemma gives an upper bound for w_j.

Lemma 5

$$w_j \le \frac{1}{[j/2]!}.$$

Proof of Lemma 5. The lemma is true for $j=1,2$. We will prove that if it is true for $j\le k-1$ then it is also true for $j=k$. By the recursion (9) we get

$$w_k = \frac{1}{k}(w_{k-1}+w_{k-2})$$

Thus by the inductive hypothesis we have

$$w_k \le \frac{1}{k}\left(\frac{1}{[(k-1)/2]!} + \frac{1}{[(k-2)/2]!}\right) \le \frac{1}{[k/2]!}$$

which completes the proof of Lemma 5.

Using Lemma 5, from (14) we get:

$$\begin{aligned}
&(3(2\ell+1))^{(2k+1)/2}\frac{N^{2\ell-1}}{k!(2\ell-1)!}C_{2\ell}^{2k+1} + \frac{N^{2k+\ell-1}}{\ell!(2k)!}C_{2k+1}^{2}(E_N)\\
&\ge \left|\sum_{1\le d_1<\cdots<d_{2k}\le N-2\ell} c_{0,2\ell,N-d_{2k}}\right| \stackrel{\text{def}}{=} L. \qquad (15)
\end{aligned}$$

In order to prove Theorem 1 we need a lower bound for the right hand-side of (15). By Lemma 2 we have

$$\begin{aligned}
L &= \left|\sum_{1\le d_1<\cdots<d_{2k}\le N-2\ell} c_{0,2\ell,N-d_{2k}}\right| = \sum_{1\le d_1<\cdots<d_{2k}\le N-2\ell} \binom{(N-d_{2k})/2}{\ell}\\
&= \sum_{d_{2k}=2k}^{N-2\ell}\left(\sum_{1\le d_1<\cdots<d_{2k-1}\le d_{2k}-1} 1\right)\binom{(N-d_{2k})/2}{\ell}\\
&= \sum_{d_{2k}=2k}^{N-2\ell}\binom{d_{2k}-1}{2k-1}\binom{(N-d_{2k})/2}{\ell}. \qquad (16)
\end{aligned}$$

We will use the following lemma

Lemma 6 *If $a > 2\ell^2$ then*

$$\binom{a}{\ell} \ge \frac{a^\ell}{e\ell!}$$

and

$$\binom{a/2}{\ell} \ge \frac{1}{e2^\ell}\binom{a}{\ell}.$$

Proof of Lemma 6. By $a \ge \ell^2 - 1$ and $1 + x \le e^x$ we get:

$$\begin{aligned}
\binom{a}{\ell} &\ge \frac{(a+1-\ell)^\ell}{\ell!} = \frac{a^\ell}{\ell!\left(1+\frac{\ell-1}{a-(\ell-1)}\right)^\ell} \ge \frac{a^\ell}{\ell!\left(1+\frac{\ell-1}{(\ell^2-1)-(\ell-1)}\right)^\ell}\\
&= \frac{a^\ell}{\ell!\left(1+\frac{1}{\ell}\right)^\ell} \ge \frac{a^\ell}{e\ell!}.
\end{aligned}$$

On the other hand

$$\binom{a/2}{\ell}\Big/\binom{a}{\ell} = \frac{a(a-2)\dots(a-2(\ell-1))}{2^\ell a(a-1)\dots(a-(\ell-1))}. \tag{17}$$

By $a \geq 2\ell^2 \geq \ell^2+\ell-2$ for $1 \leq i \leq \ell-1$ we have

$$\frac{a-2i}{a-i} = 2-\frac{a}{a-i} \geq 2-\frac{a}{a-(\ell-1)} = 1-\frac{\ell-1}{a-(\ell-1)} \geq 1-\frac{\ell-1}{\ell^2-1} = \frac{1}{\left(1+\frac{1}{\ell}\right)}. \tag{18}$$

By (17) and (18) we have

$$\binom{a/2}{\ell}\Big/\binom{a}{\ell} \geq \frac{1}{2^\ell\left(1+\frac{1}{\ell}\right)^\ell} \geq \frac{1}{e2^\ell}$$

which completes the proof of Lemma 6.

Let

$$H \stackrel{\mathrm{def}}{=} \frac{1}{e2^\ell} \sum_{d_{2k}=N-2\ell^2+1}^{N-\ell} \binom{d_{2k}-1}{2k-1}\binom{N-d_{2k}}{\ell}. \tag{19}$$

By Lemma 6 from (16) we obtain

$$\begin{aligned} L &\geq \sum_{d_{2k}=2k}^{N-2\ell^2} \binom{d_{2k}-1}{2k-1}\binom{(N-d_{2k})/2}{\ell} \geq \frac{1}{e2^\ell}\sum_{d_{2k}=2k}^{N-2\ell^2} \binom{d_{2k}-1}{2k-1}\binom{N-d_{2k}}{\ell} \\ &\geq \frac{1}{e2^\ell}\sum_{d_{2k}=2k}^{N-\ell} \binom{d_{2k}-1}{2k-1}\binom{N-d_{2k}}{\ell} - H. \end{aligned} \tag{20}$$

Consider how many ways we can choose from the integers $1, 2, \dots, N$ exactly $2k+\ell$ pieces. This is trivially $\binom{N}{2k+\ell}$. On the other hand if we fixed the value of the $2k$-th largest integer from these $2k+\ell$ pieces, let it be d_{2k}, then the number of the possibilities is $\binom{d_{2k}-1}{2k-1}\binom{N-d_{2k}}{\ell}$. Therefore

$$\binom{N}{2k+\ell} = \sum_{d_{2k}=2k}^{N-\ell} \binom{d_{2k}-1}{2k-1}\binom{N-d_{2k}}{\ell}. \tag{21}$$

By Lemma 6 we have

$$\binom{N}{2k+\ell} \geq \frac{N^{2k+\ell}}{e(2k+\ell)!}. \tag{22}$$

By (20), (21) and (22) we have

$$L \geq \frac{N^{2k+\ell}}{e^2 2^\ell (2k+\ell)!} - H. \tag{23}$$

Lemma 7

$$H = \frac{1}{e2^\ell} \sum_{d_{2k}=N-2\ell^2+1}^{N-\ell} \binom{d_{2k}-1}{2k-1}\binom{N-d_{2k}}{\ell} \leq \frac{N^{2k+\frac{2}{3}\ell}}{e^2 2^\ell (2k+\ell)!}.$$

Proof of Lemma 7. By the Stirling-formula if $d_{2k} \geq N - 2\ell^2 + 1$ we have:

$$\binom{N-d_{2k}}{\ell} \leq \binom{2\ell^2}{\ell} < \frac{(2\ell^2)^\ell}{\ell!} \leq \frac{(2\ell^2)^\ell}{\left(\frac{\ell}{e}\right)^\ell} \leq (2e\ell)^\ell. \tag{24}$$

On the other hand

$$\binom{d_{2k}-1}{2k-1} \leq \frac{N^{2k-1}}{(2k-1)!} = \frac{1}{(2k+\ell)!}\frac{(2k+\ell)!}{(2k-1)!}N^{2k-1} \leq \frac{(2k+\ell)^{\ell+1}}{(2k+\ell)!}N^{2k-1}. \tag{25}$$

By $\ell \leq k$ and $67k^3 \leq N$:

$$H \leq \frac{1}{e2^\ell}\left(2\ell^2(2e\ell)^\ell \frac{(2k+\ell)^{\ell+1}}{(2k+\ell)!}N^{2k-1}\right) \leq \frac{1}{e^2 2^\ell (2k+\ell)!}\left(\sqrt{6e}k\right)^{2\ell+3} N^{2k-1}$$
$$\leq \frac{1}{e^2 2^\ell (2k+\ell)!} N^{2k+\frac{2}{3}\ell}$$

which proves Lemma 7.

By Lemma 7, (23) and $N > 200$ we have

$$L \geq \frac{N^{2k+\ell}}{e^2 2^\ell (2k+\ell)!}\left(1 - \frac{1}{N^{\ell/3}}\right) \geq \frac{N^{2k+\ell}}{9 \cdot 2^\ell (2k+\ell)!}. \tag{26}$$

From (15) and (26) and $2^\ell \leq 2^k \leq (\sqrt{2})^{2k+1}$ we have

$$(3\sqrt{2}(2\ell+1))^{(2k+1)/2}\frac{(2k+\ell)!}{k!(2\ell-1)!}C_{2\ell}^{2k+1} + 2^\ell \frac{(2k+\ell)!}{\ell!(2k)!}N^{2k-\ell}C_{2k+1}^2(E_N)$$
$$\geq \frac{N^{2k-\ell+1}}{9}.$$

Here,

$$\frac{(2k+\ell)!}{k!(2\ell-1)!} \le \frac{(2k+\ell)^{2k-2\ell+2}}{k!} \le \frac{(3k)^{2k}}{\left(\frac{k}{e}\right)^k} \le \left(9e^2k\right)^{(2k+1)/2}$$

$$\frac{(2k+\ell)!}{\ell!(2k)!} \le \frac{(2k+\ell)^{\ell}}{\ell!} \le \frac{(3k)^{\ell}}{\left(\frac{\ell}{e}\right)^\ell} \le \left(8.16\frac{k}{\ell}\right)^{\ell}.$$

Thus

$$\left(17\sqrt{k(2\ell+1)}\; C_{2\ell}\right)^{2k+1} + \left(17\;\frac{2k+1}{2\ell}\right)^{\ell} N^{2k-\ell}C_{2k+1}^2 \ge \frac{1}{9}N^{2k-\ell+1}, \quad (27)$$

which was to be proved.

I would like to thank Professors Julien Cassaigne and András Sárközy for the valuable discussions.

References

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

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

[3] Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, *Measures of pseudorandomness for finie sequences: minimum and typical values*, submitted to J. London Math. Soc.

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

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

[6] C. Mauduit and A. Sárközy, *On the measures of pseudorandomness of binary sequences*, Discrete Math., to appear