

A technique to study the correlation measures of binary sequences

Venkat Anantharam

EECS Department, University of California, Berkeley, CA 94720, U.S.A.

ananth@eecs.berkeley.edu

1-510-643-8435(O); 1-510-642-2845(fax)

20 Nov 2005

Short title : Correlation Measures

Keywords : binary sequences, correlation measures, pseudorandomness.

Abstract

Let $\underline{e}^N = (e_1, e_2, \dots, e_N)$ be a binary sequence with $e_i \in \{+1, -1\}$. For $2 \leq k \leq N$, the correlation measure of order k of the sequence is defined by Mauduit and Sárközy as

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

where the maximum is taken over all $M \geq 1$ and $0 \leq d_1 < d_2 < \dots < d_k$ such that $M + d_k \leq N$. These measures have been extensively studied over the last decade. Several inequalities for these measures (that hold for all \underline{e}^N for all large enough N) have been proved, and others conjectured. Further, these measures have been estimated for various special sequences \underline{e}^N .

Fix $M \geq 1$ and $L \geq 1$. For $1 \leq a \leq L$, let $\underline{v}_a^M = (v_a(1), \dots, v_a(M))$ be a binary sequence with $v_a(i) \in \{+1, -1\}$. For $2 \leq k \leq L$ we define the correlation measure of order k of the family of sequences $\underline{V}^{M \times L} = (\underline{v}_1^M, \dots, \underline{v}_L^M)$ as

$$C_k(\underline{V}^{M \times L}) = \max_{1 \leq a_1 < a_2 < \dots < a_k \leq L} \left| \sum_{i=1}^M v_{a_1}(i) v_{a_2}(i) \dots v_{a_k}(i) \right| .$$

We use these new correlation measures as a vehicle to study the correlation measures of Mauduit and Sárközy.

We prove a lower bound on the even correlation measures $C_{2k}(\underline{V}^{M \times L})$ when $L > k(2k - 1)M$ and use it to prove that for each $k \geq 1$ there is an absolute constant $c_{2k} > 0$ such that $C_{2k}(\underline{e}^N) \geq c_{2k} \sqrt{N}$ for all \underline{e}^N for all large enough N (this result was already recently proved by Alon et al. by a different technique).

We study $C_3(\underline{e}^N)$ via $C_3(\underline{V}^{M \times L})$. This allows us to strengthen a recent result of Gyarmati which relates $C_3(\underline{e}^N)$ and $C_2(\underline{e}^N)$. We prove that given any $\kappa > 0$ there is an associated $c > 0$ (depending only on κ) such that, for all sufficiently large N , if $C_2(\underline{e}^N) \leq \kappa N^{2/3}$ we have $C_3(\underline{e}^N) \geq c\sqrt{N}$.

Finally, the study of $C_3(\underline{V}^{M \times L})$ allows us to verify a conjecture that Gyarmati attributes to Mauduit. We prove that there is an absolute constant $c > 0$ such that $C_2(\underline{e}^N)C_3(\underline{e}^N) \geq cN$ for all \underline{e}^N for all large enough N .

1. Discussion

Let $\underline{e}^N = (e_1, e_2, \dots, e_N)$ be a binary sequence with $e_i \in \{+1, -1\}$. For $2 \leq k \leq N$, the correlation measure of order k of the sequence is defined by Mauduit and Sárközy [4] as

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

where the maximum is taken over all $M \geq 1$ and $0 \leq d_1 < d_2 < \dots < d_k$ such that $M + d_k \leq N$. In this paper we develop a simple technique for proving some lower bounds on and relations between these correlation measures.

Fix $1 \leq M \leq N$ and $1 \leq L \leq N - M + 1$. For $1 \leq a \leq L$ define the binary sequence $\underline{v}_a^M = (v_a(1), \dots, v_a(M))$ by setting

$$v_a(i) = e_1 e_{a+i-1} . \tag{1}$$

For $2 \leq k \leq L$ and $1 \leq a_1 < a_2 < \dots < a_k \leq L$ observe that

$$v_{a_1}(i) v_{a_2}(i) \dots v_{a_k}(i) = (e_1)^k e_{a_1+i-1} e_{a_2+i-1} \dots e_{a_k+i-1} .$$

Thus

$$C_k(\underline{e}^N) \geq \left| \sum_{i=1}^M v_{a_1}(i) v_{a_2}(i) \dots v_{a_k}(i) \right| .$$

This motivates us to make the following definition. For arbitrary $M \geq 1$ and $L \geq 1$, for $1 \leq a \leq L$, let $\underline{v}_a^M = (v_a(1), \dots, v_a(M))$ be an arbitrary binary sequence with $v_a(i) \in \{+1, -1\}$. Then, for $2 \leq k \leq L$ we define the correlation measure of order k of the family of sequences $\underline{V}^{M \times L} = (\underline{v}_1^M, \dots, \underline{v}_L^M)$ as

$$C_k(\underline{V}^{M \times L}) = \max_{1 \leq a_1 < a_2 < \dots < a_k \leq L} \left| \sum_{i=1}^M v_{a_1}(i) v_{a_2}(i) \dots v_{a_k}(i) \right| .$$

We thus have

$$C_k(\underline{e}^N) \geq C_k(\underline{V}^{M \times L}) \quad (2)$$

for any $1 \leq M \leq N$ and $k \leq L \leq N - M + 1$, when \underline{V} is constructed from \underline{e} as in equation (1). Hence, finding estimates on and relations between the correlation measures of the type $C_k(\underline{V}^{M \times L})$ for arbitrary $M \times L$ binary matrices \underline{V} will yield corresponding results for the correlation measures $C_k(\underline{e}^N)$ of Mauduit and Sárközy.

In the following, we will occasionally use the notation $f(\underline{e}^N) \gg g(N)$ where $f(\underline{e}^N)$ is a nonnegative function of correlation measures of \underline{e}^N and $g(N)$ is a nonnegative function. This should be understood to mean that there is an absolute constant $c > 0$ such that $f(\underline{e}^N) \geq cg(N)$ for all \underline{e}^N for all sufficiently large N .

2. Proof of $C_{2k}(\underline{e}^N) \gg \sqrt{N}$

We will first illustrate the power of the matrix viewpoint by giving an elementary proof that for each $k \geq 1$ there is an absolute constant $c_{2k} > 0$ with $C_{2k}(\underline{e}^N) \geq c_{2k}\sqrt{N}$ for all \underline{e}^N for all large enough N . It was conjectured by Cassaigne et al. [2] (see Problem 2 on pg. 107 and the discussion on pp. 109 -110 of [2]) that for some absolute constants $d > 0$ and $c > 0$ we have $C_2(\underline{e}^N) \geq cN^d$ for all \underline{e}^N for all large enough N . Recently, Alon et al. [1] have proved that $C_{2k}(\underline{e}^N) \geq \sqrt{\frac{1}{2} \lfloor \frac{N}{2k+1} \rfloor}$ for all \underline{e}^N for $1 \leq k \leq \lfloor \frac{N}{2} \rfloor$. We get a better constant for $k = 1$ than that of [1], but poorer constants for all $k \geq 2$. In general we have not concerned ourselves with optimizing constants. It should be noted that our proof is elementary and the result is broader in that it also yields, for all $L > k(2k - 1)M$, lower bounds on $C_{2k}(\underline{V}^{M \times L})$ that apply for all $\underline{V}^{M \times L}$.

As a warm up, consider $C_2(\underline{V}^{M \times L})$. We prove :

Theorem 1

For $L > M \geq 1$ and any binary matrix $\underline{V}^{M \times L}$ we have $C_2(\underline{V}^{M \times L}) \geq \sqrt{\frac{M(L-M)}{L-1}}$.

Proof

Let c_{ab} denote $\sum_{i=1}^M v_a(i)v_b(i)$. Write

$$\begin{aligned}
\sum_{a=1}^L \sum_{b=1}^L c_{ab}^2 &= \sum_{a=1}^L \sum_{b=1}^L \left(\sum_{i=1}^M v_a(i)v_b(i) \right)^2 \\
&= \sum_{a=1}^L \sum_{b=1}^L \sum_{i=1}^M \sum_{j=1}^M v_a(i)v_b(i)v_a(j)v_b(j) \\
&= \sum_{i=1}^M \sum_{j=1}^M \left(\sum_{a=1}^L v_a(i)v_a(j) \right)^2 \\
&\stackrel{(a)}{\geq} \sum_{i=1}^M \left(\sum_{a=1}^L v_a^2(i) \right)^2 \\
&\stackrel{(b)}{=} ML^2,
\end{aligned}$$

where step (a) comes from dropping all the off-diagonal terms, which are nonnegative, and step (b) comes from using $v_a(i)^2 = 1$. It should be noted in passing that a similar bound can be proved even when one only assumes that the columns of $\underline{V}^{M \times L}$ are real valued vectors of constant squared norm, see [5].

On the other hand, we also have

$$\begin{aligned}
\sum_{a=1}^L \sum_{b=1}^L c_{ab}^2 &= \sum_{a=1}^L c_{aa}^2 + 2 \sum_{1 \leq a < b \leq L} c_{ab}^2 \\
&\leq LM^2 + L(L-1) \left(C_2(\underline{V}^{M \times L}) \right)^2.
\end{aligned}$$

It follows that

$$C_2(\underline{V}^{M \times L}) \geq \sqrt{\frac{M(L-M)}{L-1}},$$

when $L > M$, which was to be proved. □

We now use Theorem 1 to verify the conjecture in Problem 2 of [2] (which has of course already been settled in [1]). For $\epsilon > 0$ rational with denominator N set $M = \epsilon N$ and $L = N - M + 1$. Assume that $L > M$. Let $\underline{V}^{M \times L}$ be

constructed from \underline{e}^N as in equation (1). From Theorem 1 and equation (2) we have

$$C_2(\underline{e}^N) \geq \sqrt{\frac{\epsilon(1-2\epsilon)}{1-\epsilon}} N .$$

The coefficient $\sqrt{\frac{\epsilon(1-2\epsilon)}{1-\epsilon}}$ can be optimized over real values $0 < \epsilon < \frac{1}{2}$. The maximum occurs at $1 - \frac{\sqrt{2}}{2}$ and equals $\sqrt{2} - 1$. This is better than $\sqrt{\frac{1}{6}}$, which is the constant in the result of [1].

We turn next to higher order even correlations. We prove :

Theorem 2

For any $k \geq 1$, for $M \geq 1$ and $L > k(2k-1)M$ and any binary matrix $\underline{V}^{M \times L}$ we have, $C_{2k}(\underline{V}^{M \times L}) \geq \sqrt{\frac{ML^{2k-2}(L-k(2k-1)M)}{(L-1)\dots(L-(2k-1)M)}}$.

Proof

Let $c_{a_1 a_2 \dots a_{2k}}$ denote $\sum_{i=1}^M v_{a_1}(i) v_{a_2}(i) \dots v_{a_{2k}}(i)$. Write

$$\begin{aligned} \sum_{a_1, a_2, \dots, a_{2k}=1}^L c_{a_1 a_2 \dots a_{2k}}^2 &= \sum_{a_1, a_2, \dots, a_{2k}=1}^L \left(\sum_{i=1}^M v_{a_1}(i) v_{a_2}(i) \dots v_{a_{2k}}(i) \right)^2 \\ &= \sum_{a_1, a_2, \dots, a_{2k}=1}^L \sum_{i=1}^M \sum_{j=1}^M v_{a_1}(i) v_{a_1}(j) \dots v_{a_{2k}}(i) v_{a_{2k}}(j) \\ &= \sum_{i=1}^M \sum_{j=1}^M \left(\sum_{a=1}^L v_a(i) v_a(j) \right)^{2k} \\ &\stackrel{(a)}{\geq} \sum_{i=1}^M \left(\sum_{a=1}^L v_a^2(i) \right)^{2k} \\ &= ML^{2k} , \end{aligned}$$

where step (a) comes from dropping all the off-diagonal terms, which are nonnegative.

Now, we may write

$$\sum_{a_1, a_2, \dots, a_{2k}=1}^L c_{a_1 a_2 \dots a_{2k}}^2 = (2k)! \sum_{1 \leq a_1 < a_2 < \dots < a_{2k} \leq L} c_{a_1 a_2 \dots a_{2k}}^2 + \text{other terms} ,$$

where the total number of other terms is $L^{2k} - L(L-1)\dots(L-(2k-1))$ and each of the other terms is bounded above by M^2 . It is straightforward to prove by induction that

$$L^{2k} - L(L-1)\dots(L-(2k-1)) \leq k(2k-1)L^{2k-1}.$$

It follows that

$$\sum_{a_1, a_2, \dots, a_{2k}=1}^L c_{a_1 a_2 \dots a_{2k}}^2 \leq L(L-1)\dots(L-(2k-1)) \left(C_{2k}(\underline{V}^{M \times L}) \right)^2 + k(2k-1)L^{2k-1}M^2.$$

Combining this with the lower bound that was previously proved, we get

$$C_{2k}(\underline{V}^{M \times L}) \geq \sqrt{\frac{ML^{2k-2}(L-k(2k-1)M)}{(L-1)\dots(L-(2k-1))}},$$

when $L > k(2k-1)M$, which was to be proved. □

We now show that for each $k \geq 1$ there is an absolute constant $c_{2k} > 0$ such that $C_{2k}(\underline{e}^N) \geq c_{2k}\sqrt{N}$ for all \underline{e}^N for all sufficiently large N . For $\epsilon > 0$ rational with denominator N , set $M = \epsilon N$ and $L = N - M + 1$. Assume that $L > k(2k-1)M$. Let $\underline{V}^{M \times L}$ be constructed from \underline{e}^N as in equation (1). From Theorem 2 and equation (2) we have

$$C_{2k}(\underline{e}^N) \geq \sqrt{\frac{\epsilon(1-(k(2k-1)+1)\epsilon)}{1-\epsilon}} N.$$

The coefficient $\sqrt{\frac{\epsilon(1-(k(2k-1)+1)\epsilon)}{1-\epsilon}}$ can be optimized over real values $0 < \epsilon < \frac{1}{k(2k-1)+1}$. The maximum occurs at $1 - \sqrt{\frac{2k^2-k}{2k^2-k+1}}$ and the resulting optimum constant is $\sqrt{2k^2-k+1} - \sqrt{2k^2-k}$. For $k \geq 2$ this is not as good as $\sqrt{\frac{1}{2(2k+1)}}$, which is the constant in the result of [1]. It will be noted that our bounding technique is quite crude, so it may be possible to improve these constants with some more effort.

3. Proof of $C_2(\underline{e}^N) \ll N^{2/3} \implies C_3(\underline{e}^N) \gg \sqrt{N}$

We turn to study $C_3(\underline{e}^N)$ via $C_3(\underline{V}^{M \times L})$. Gyarmati [3] has proved that there is an absolute constant $c > 0$ such that, if N is sufficiently large, for any \underline{e}^N satisfying $C_2(\underline{e}^N) < \frac{N^{2/3}}{50\sqrt{\log(N)}}$ we have $C_3(\underline{e}^N) \geq c\sqrt{N}$. We prove :

Theorem 3

Given any $\kappa > 0$ there is an associated $c > 0$ (depending only on κ) such that, for all sufficiently large N , if $C_2(\underline{e}^N) \leq \kappa N^{2/3}$ we have $C_3(\underline{e}^N) \geq c\sqrt{N}$.

Proof

Pick $M \geq 1$, and $L \geq 1$ such that $3 \leq L \leq N - M + 1$. Let $\underline{V}^{M \times L}$ be constructed from \underline{e}^N as in equation (1). Let c_{abc} denote $\sum_{i=1}^M v_a(i)v_b(i)v_c(i)$. Observe that

$$\begin{aligned}
\sum_{a=1}^L \sum_{b=1}^L \sum_{c=1}^L c_{abc}^2 &= \sum_{a=1}^L \sum_{b=1}^L \sum_{c=1}^L \left(\sum_{i=1}^M v_a(i)v_b(i)v_c(i) \right)^2 \\
&= \sum_{a=1}^L \sum_{b=1}^L \sum_{c=1}^L \sum_{i=1}^M \sum_{j=1}^M v_a(i)v_a(j)v_b(i)v_b(j)v_c(i)v_c(j) \\
&= \sum_{i=1}^M \sum_{j=1}^M \left(\sum_{a=1}^L v_a(i)v_a(j) \right)^3 \\
&= \sum_{i=1}^M \left(\sum_{a=1}^L v_a^2(i) \right)^3 + \text{off-diagonal terms} \\
&= ML^3 + \text{off-diagonal terms} . \tag{3}
\end{aligned}$$

The total number of off-diagonal terms is $M(M-1)$. Suppose $1 \leq i \neq j \leq M$. Then we have

$$\begin{aligned}
\left| \sum_{a=1}^L v_a(i)v_a(j) \right| &\stackrel{(a)}{=} \left| \sum_{a=1}^L e_{a+i-1}e_{a+j-1} \right| \\
&\stackrel{(b)}{\leq} \kappa N^{2/3} . \tag{4}
\end{aligned}$$

where step (a) comes from using equation (1), and step (b) comes from the hypothesized upper bound on $C_2(\underline{e}^N)$. It follows that the sum of the off-diagonal terms in the preceding equation is at least $-M(M-1)\kappa^3 N^2$, so we

have

$$\sum_{a=1}^L \sum_{b=1}^L \sum_{c=1}^L c_{abc}^2 \geq ML^3 - M(M-1)\kappa^3 N^2 .$$

On the other hand, we also have

$$\begin{aligned} \sum_{a=1}^L \sum_{b=1}^L \sum_{c=1}^L c_{abc}^2 &= 6 \sum_{1 \leq a < b < c \leq L} c_{abc}^2 + \text{off-diagonal terms} \\ &\stackrel{(a)}{\leq} L(L-1)(L-2)C_3^2(\underline{e}^N) + \text{off-diagonal terms} , \end{aligned}$$

where step (a) comes from equation (2). The number of off-diagonal terms is $L^3 - L(L-1)(L-2) = L(3L-2)$, and each of them is bounded above by M^2 . We thus have

$$\sum_{a=1}^L \sum_{b=1}^L \sum_{c=1}^L c_{abc}^2 \leq L(L-1)(L-2)C_3^2(\underline{e}^N) + L(3L-2)M^2 . \quad (5)$$

Combining this upper bound with the previously proved lower bound on the same quantity, we have

$$L(L-1)(L-2)C_3^2(\underline{e}^N) + L(3L-2)M^2 \geq ML^3 - M(M-1)\kappa^3 N^2 .$$

Note that this inequality holds for all $M \geq 1$, for all $L \geq 1$ satisfying $3 \leq L \leq N - M + 1$, and for all \underline{e}^N satisfying $C_2(\underline{e}^N) \leq \kappa N^{2/3}$.

Now pick $0 < \epsilon < 1$ rational with denominator N , $0 < \alpha < 1$ rational with denominator N , set $M = \epsilon N$ and $L = \alpha N$, and assume that $3 \leq L \leq N - M + 1$. From the preceding inequality, we get

$$\alpha^3 N^3 C_3^2(\underline{e}^N) \geq \epsilon \alpha^3 N^4 - \epsilon^2 \kappa^3 N^4 - 3\epsilon^2 \alpha^2 N^4 .$$

It is easily seen that choosing α roughly $\frac{1}{2}$ and ϵ roughly $\frac{1}{12+16\kappa^3}$ proves the theorem with $c = \sqrt{\frac{1}{24+32\kappa^3}}$. We have not bothered to optimize constants.

□

4. Proof of $C_2(\underline{e}^N)C_3(\underline{e}^N) \gg N$

In Problem 2 on pg. 80 of [3] Gyarmati attributes to Mauduit the conjecture that $C_2(\underline{e}^N)C_3(\underline{e}^N) \gg N$. We verify this conjecture. We prove :

Theorem 4

There is an absolute constant $c > 0$ such that for all \underline{e}^N for all sufficiently large N we have $C_2(\underline{e}^N)C_3(\underline{e}^N) \geq cN$.

Proof

Consider the estimate in equation (3). In general (i.e. without using the hypothesis of Theorem 3) from the first line in equation (4) we see that each of the off-diagonal terms is upper bounded in absolute value by $C_2(\underline{e}^N)$, so a consequence of this estimate would be

$$\sum_{a=1}^L \sum_{b=1}^L \sum_{c=1}^L c_{abc}^2 \geq ML^3 - M(M-1)C_2^3(\underline{e}^N) .$$

The lower bound of equation (5) always holds, and so we have in general that

$$L(L-1)(L-2)C_3^2(\underline{e}^N) + L(3L-2)M^2 \geq ML^3 - M(M-1)C_2^3(\underline{e}^N) .$$

This inequality holds for all $M \geq 1$, for all $L \geq 1$ satisfying $3 \leq L \leq N - M + 1$, and for all \underline{e}^N .

We rearrange this inequality to get

$$M^2C_2^3(\underline{e}^N) \geq ML^3 - L^3C_3^2(\underline{e}^N) - 3L^2M^2 , \tag{6}$$

which again holds for all $M \geq 1$, for all $L \geq 1$ satisfying $3 \leq L \leq N - M + 1$, and for all \underline{e}^N .

Now suppose N is sufficiently large and $C_2(\underline{e}^N) \leq \frac{1}{4}N^{2/3}$. Then, from the proof of Theorem 3, we have $C_3(\underline{e}^N) \geq \frac{1}{5}N^{1/2}$. From the remarks following the proof of Theorem 1, since $\sqrt{2} - 1 > \frac{2}{5}$ we have $C_2(\underline{e}^N) \geq \frac{2}{5}N^{1/2}$ for all sufficiently large N . Thus we would get $C_2(\underline{e}^N)C_3(\underline{e}^N) \geq \frac{2}{25}N$, which meets the goals of the theorem. Thus we may assume that $C_2(\underline{e}^N) \geq \frac{1}{4}N^{2/3}$,

Next, suppose that $C_3(\underline{e}^N) \geq \frac{1}{3}N^{1/3}$. Then $C_2(\underline{e}^N)C_3(\underline{e}^N) \geq \frac{1}{12}N$, which meets the goals of the theorem. Thus we may assume that

$$1 \leq C_3(\underline{e}^N) \leq \frac{1}{3}N^{1/3} , \tag{7}$$

(it is straightforward to see that the lower bound holds).

We now set $M = 3C_3^2(\underline{e}^N)$. Thus

$$3 \leq M \leq \frac{1}{3}N^{2/3} .$$

We take $L = \lceil \frac{N}{2} \rceil$ and substitute these values into equation (6). For sufficiently large N we get

$$9C_3^4(\underline{e}^N)C_2^3(\underline{e}^N) \geq \frac{1}{4}C_3^2(\underline{e}^N)N^3 - 7C_3^4(\underline{e}^N)N^2 ,$$

where we have been generous in the term subtracted on the right, to deal with integer part issues. Using the assumed upper bound in equation (7) we get from this, for sufficiently large N , that

$$9C_3^4(\underline{e}^N)C_2^3(\underline{e}^N) \geq \frac{2}{9}C_3^2(\underline{e}^N)N^3 ,$$

which is to say that

$$81C_3^2(\underline{e}^N)C_2^3(\underline{e}^N) \geq 2N^3 .$$

Writing this as

$$81 \left(C_2(\underline{e}^N)C_3(\underline{e}^N) \right)^2 C_2(\underline{e}^N) \geq 2N^3 ,$$

we see that either $C_2(\underline{e}^N) \geq \frac{1}{2}N$, in which case the lower bound in equation (7) gives $C_2(\underline{e}^N)C_3(\underline{e}^N) \geq \frac{1}{2}N$, or $C_2(\underline{e}^N)C_3(\underline{e}^N) \geq \frac{2}{9}N$. In either case, we have completed the proof of the theorem. Note that without worrying too much about optimizing constants we have actually proved that $C_2(\underline{e}^N)C_3(\underline{e}^N) \geq \frac{2}{25}N$ for all \underline{e}^N for all sufficiently large N .

□

5. Concluding remarks

Our aim was to attack the conjecture attributed by Gyarmati to Mauduit in [3]. This has been settled in the affirmative in Theorem 4 above. The technique used seems to be more broadly applicable, so it may be reasonable to hope that it can lead to further progress in understanding the properties of the correlation measures of Mauduit and Sárközy.

This work was completed while visiting the Boole Center for Informatics at University College Cork in Ireland. I would like to thank Neil O'Connell for his warm hospitality.

References

- [1] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira, and V. Rödl (2005), “Measures of pseudorandomness for finite sequences : minimal values”. *Combinatorics, Probability, and Computing*, to appear.
- [2] J. Cassaigne, C. Mauduit, and A. Sárközy (2002). “On finite pseudorandom binary sequences VII : the measures of pseudorandomness”. *Acta Arithmetica*, Vol. 103, No. 2, pp. 97 -118.
- [3] K. Gyarmati (2005), “On the correlation of binary sequences”. *Studia Scientiarum Mathematicarum Hungarica*, Vol. 42, No. 1, pp. 79 -93.
- [4] C. Mauduit and A. Sárközy (1997), “On finite pseudorandom binary sequences I. Measures of pseudorandomness, the Legendre symbol”. *Acta Arithmetica*, Vol. 82, No. 4, pp. 365 -377.
- [5] L. R. Welch (1974), “Lower bounds on the maximum cross correlation of signals”. *IEEE Transactions on Information Theory*, Vol. 20, No. 3, pp. 397 -399.