Available online at www.sciencedirect.com

ScienceDirect

Discrete Mathematics 308 (2008) 6203–6209

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

A technique to study the correlation measures of binary sequences

Venkat Anantharam*

EECS Department, University of California, Berkeley, CA 94720, USA

Received 21 November 2005; received in revised form 19 June 2007; accepted 24 November 2007
Available online 27 December 2007

Abstract

Let $E^N = (e_1, e_2, \ldots, e_N)$ be a binary sequence with $e_i \in \{+1, -1\}$. For $2 \le k \le N$, the correlation measure of order k of the sequence is defined by Mauduit and Sárközy 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 $M \ge 1$ and $0 \le d_1 < d_2 < \ldots < d_k$ such that $M + d_k \le N$. These measures have been extensively studied over the last decade. Several inequalities for these measures (that hold for all E^N for all large enough N) have been proved, and others conjectured. Further, these measures have been estimated for various special sequences E^N.

Fix $M \ge 1$ and $L \ge 1$. For $1 \le a \le L$, let $E^M[a] = (e_1[a], \ldots, e_M[a])$ be a binary sequence with $e_i[a] \in \{+1, -1\}$. For $2 \le k \le L$ we define the correlation measure of order k of the family of sequences $E^M[1 : L] = \{E^M[1], \ldots, E^M[L]\}$ as

$$C_k(E^M[1 : L]) = \max_{1 \le a_1 < a_2 < \cdots < a_k \le L} \left| \sum_{i=1}^{M} e_i[a_1] e_i[a_2] \ldots e_i[a_k] \right|.$$

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

Alon, Kohayakawa, Mauduit, Moreira, and Rödl recently proved that for each $k \ge 1$ there is an absolute constant $c_{2k} > 0$ such that $C_{2k}(E^N) \ge c_{2k}\sqrt{N}$ for all E^N for all large enough N. thus answering a question of Cassaigne, Mauduit, and Sárközy (in stronger form than an earlier result of Kohayakawa, Mauduit, Moreira, and Rödl). We prove a lower bound on the even correlation measures $C_{2k}(E^M[1 : L])$ when $L > k(2k-1)M$ and use it to provide an alternate proof of this result. The constant c_{2k} in our proof is better than that of Alon, Kohayakawa, Mauduit, Moreira, and Rödl for $k = 1$, but poorer for all $k \ge 2$.

We study $C_3(E^N)$ via $C_3(E^M[1 : L])$. This allows us to strengthen a recent result of Gyarmati which relates $C_3(E^N)$ and $C_2(E^N)$. 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 $C_2(E^N) \le \kappa N^{2/3}$ we have $C_3(E^N) \ge c\sqrt{N}$. This also answers a question of Gyarmati.

Finally, the study of $C_3(E^M[1 : L])$ allows us to verify a conjecture of Mauduit. We prove that there is an absolute constant $c > 0$ such that $C_2(E^N)C_3(E^N) \ge cN$ for all E^N for all large enough N.

Keywords: Binary sequences; Correlation measures; Pseudorandomness

* Tel.: +1 510 643 8435(O); fax: +1 510 642 2845.
E-mail address: ananth@eecs.berkeley.edu.

0012-365X/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2007.11.043

1. Discussion

Let $E^N = (e_1, e_2, \dots, e_N)$ be a binary sequence with $e_i \in \{+1, -1\}$. For $2 \le k \le N$, the correlation measure of order k of the sequence is defined by Mauduit and Sárközy [7] 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 $M \ge 1$ and $0 \le d_1 < d_2 < \dots < d_k$ such that $M + d_k \le N$. In this paper we develop a simple technique for proving some lower bounds on and relations between these correlation measures.

Fix $1 \le M \le N$ and $1 \le L \le N - M + 1$. For $1 \le a \le L$ define the binary sequence $E^M[a] = (e_1[a], \dots, e_M[a])$ by setting

$$e_i[a] = e_{a+i-1}. \tag{1}$$

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

$$e_i[a_1]e_i[a_2]\dots e_i[a_k] = e_{a_1+i-1}e_{a_2+i-1}\dots e_{a_k+i-1}.$$

Thus

$$C_k(E^N) \ge \left| \sum_{i=1}^{M} e_i[a_1]e_i[a_2]\dots e_i[a_k] \right|.$$

This motivates us to make the following definition. For arbitrary $M \ge 1$ and $L \ge 1$, for $1 \le a \le L$, let $E^M[a] = (e_1[a], \dots, e_M[a])$ be an arbitrary binary sequence with $e_i[a] \in \{+1, -1\}$. Then, for $2 \le k \le L$ we define the correlation measure of order k of the family of sequences $E^M[1 : L] = \{E^M[1], \dots, E^M[L]\}$ as

$$C_k(E^M[1 : L]) = \max_{1 \le a_1 < a_2 < \dots < a_k \le L} \left| \sum_{i=1}^{M} e_i[a_1]e_i[a_2]\dots e_i[a_k] \right|.$$

We thus have

$$C_k(E^N) \ge C_k(E^M[1 : L]) \tag{2}$$

for any $1 \le M \le N$ and $k \le L \le N - M + 1$, when $E^M[1 : L]$ is constructed from E^N as in Eq. (1). Hence, finding estimates on and relations between the correlation measures of the type $C_k(E^M[1 : L])$ for arbitrary $E^M[1 : L]$ will yield corresponding results for the correlation measures $C_k(E^N)$ of Mauduit and Sárközy.

It should be mentioned that other notions of pseudorandomness for families of binary sequences have been introduced by Ahlswede, Khachatrian, Mauduit, and Sárközy [1].

In the following, we will occasionally use the notation $f(E^N) \gg g(N)$ where $f(E^N)$ is a nonnegative function of correlation measures of 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 $f(E^N) \ge cg(N)$ for all E^N for all sufficiently large N.

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

We will first illustrate the power of the viewpoint provided by the newly defined correlation measures by giving an elementary proof that for each $k \ge 1$ there is an absolute constant $c_{2k} > 0$ with $C_{2k}(E^N) \ge c_{2k}\sqrt{N}$ for all E^N for all large enough N. As mentioned in the abstract, this result is not new. It was conjectured by Cassaigne, Mauduit, and Sárkozy [3] (see Problem 2 on pg. 107 and the discussion on pp. 109–110 of [3]) that for some absolute constants $d > 0$ and $c > 0$ we have $C_2(E^N) \ge cN^d$ for all E^N for all large enough N. Recently, Alon, Kohayakawa, Mauduit, Moreira, and Rödl [2] proved that $C_{2k}(E^N) \ge \sqrt{\frac{1}{2}\lfloor \frac{N}{2k+1} \rfloor}$ for all E^N for $1 \le k \le \lfloor \frac{N}{2} \rfloor$, thus answering the question of [3] in stronger form than an earlier result of Kohayakawa, Mauduit, Moreira, and Rödl [5].

We get a better constant for $k = 1$ than that of [2], but poorer constants for all $k \ge 2$. 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 $C_{2k}(E^M[1 : L])$ that apply for all $E^M[1 : L]$.

As a warm up, consider $C_2(E^M[1:L])$. We prove:

Theorem 1. *For $L > M \geq 1$ and any $E^M[1:L]$ we have $C_2(E^M[1:L]) \geq \sqrt{\frac{M(L-M)}{L-1}}$.*

Proof. Let c_{ab} denote $\sum_{i=1}^{M} e_i[a]e_i[b]$. Write

$$\begin{aligned}
\sum_{a=1}^{L}\sum_{b=1}^{L} c_{ab}^2 &= \sum_{a=1}^{L}\sum_{b=1}^{L}\left(\sum_{i=1}^{M} e_i[a]e_i[b]\right)^2 \\
&= \sum_{a=1}^{L}\sum_{b=1}^{L}\sum_{i=1}^{M}\sum_{j=1}^{M} e_i[a]e_i[b]e_j[a]e_j[b] \\
&= \sum_{i=1}^{M}\sum_{j=1}^{M}\left(\sum_{a=1}^{L} e_i[a]e_j[a]\right)^2 \\
&\overset{\text{(a)}}{\geq} \sum_{i=1}^{M}\left(\sum_{a=1}^{L} e_i[a]^2\right)^2 \\
&\overset{\text{(b)}}{=} ML^2,
\end{aligned}$$

where step (a) comes from dropping all the off-diagonal terms, which are nonnegative, and step (b) comes from using $e_i[a]^2 = 1$. It should be noted in passing that a similar bound can be proved even when one only assumes that the columns of $E^M[1:L]$ are real-valued vectors of constant squared norm, see [8].

On the other hand, we also have

$$\begin{aligned}
\sum_{a=1}^{L}\sum_{b=1}^{L} c_{ab}^2 &= \sum_{a=1}^{L} c_{aa}^2 + 2\sum_{1\leq a<b\leq L} c_{ab}^2 \\
&\leq LM^2 + L(L-1)\Big(C_2(E^M[1:L])\Big)^2.
\end{aligned}$$

It follows that

$$C_2(E^M[1:L]) \geq \sqrt{\frac{M(L-M)}{L-1}},$$

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

We now use Theorem 1 to verify the conjecture in Problem 2 of [3] (which has of course already been settled in [5, 2]). For $\epsilon > 0$ rational with denominator N set $M = \epsilon N$ and $L = N - M + 1$. Assume that $L > M$. Let $E^M[1:L]$ be constructed from E^N as in Eq. (1). From Theorem 1 and Eq. (2) we have

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

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 [2].

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 $E^M[1:L]$ we have, $C_{2k}(E^M[1:L]) \geq \sqrt{\frac{ML^{2k-2}(L-k(2k-1)M)}{(L-1)\ldots(L-(2k-1))}}$.*

Proof. Let $c_{a_1a_2\dots a_{2k}}$ denote $\sum_{i=1}^{M} e_i[a_1]e_i[a_2]\dots e_i[a_{2k}]$. Write

$$\begin{aligned}\sum_{a_1,a_2,\dots,a_{2k}=1}^{L} c^2_{a_1a_2\dots a_{2k}} &= \sum_{a_1,a_2,\dots,a_{2k}=1}^{L}\left(\sum_{i=1}^{M} e_i[a_1]e_i[a_2]\dots e_i[a_{2k}]\right)^2\\ &= \sum_{a_1,a_2,\dots,a_{2k}=1}^{L}\sum_{i=1}^{M}\sum_{j=1}^{M} e_i[a_1]e_j[a_1]\dots e_i[a_{2k}]e_j[a_{2k}]\\ &= \sum_{i=1}^{M}\sum_{j=1}^{M}\left(\sum_{a=1}^{L} e_i[a]e_j[a]\right)^{2k}\\ &\overset{\text{(a)}}{\geq} \sum_{i=1}^{M}\left(\sum_{a=1}^{L} e_i[a]^2\right)^{2k}\\ &= ML^{2k},\end{aligned}$$

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

Now, we may write

$$\sum_{a_1,a_2,\dots,a_{2k}=1}^{L} c^2_{a_1a_2\dots a_{2k}} = (2k)! \sum_{1\leq a_1<a_2<\dots<a_{2k}\leq L} c^2_{a_1a_2\dots a_{2k}} + \text{other terms},$$

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

$$\sum_{a_1,a_2,\dots,a_{2k}=1}^{L} c^2_{a_1a_2\dots a_{2k}} \leq L(L-1)\dots(L-(2k-1))\left(C_{2k}(E^M[1:L])\right)^2 + k(2k-1)L^{2k-1}M^2.$$

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

$$C_{2k}(E^M[1:L]) \geq \sqrt{\frac{ML^{2k-2}(L-k(2k-1)M)}{(L-1)\dots(L-(2k-1))}},$$

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 $C_{2k}(E^N) \geq c_{2k}\sqrt{N}$ for all 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 $E^M[1:L]$ be constructed from E^N as in Eq. (1). From Theorem 2 and Eq. (2) we have

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

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 [2]. 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. Resolution of a question of Gyarmati

We turn to study $C_3(E^N)$ via $C_3(E^M[1:L])$. Gyarmati [4] has proved that there is an absolute constant $c > 0$ such that, if N is sufficiently large, for any E^N satisfying $C_2(E^N) < \frac{N^{2/3}}{50\sqrt{\log(N)}}$ we have $C_3(E^N) \geq c\sqrt{N}$. We prove the following result, which answers the third question in [4]:

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

Proof. Pick $M \geq 1$, and $L \geq 1$ such that $3 \leq L \leq N - M + 1$. Let $E^M[1:L]$ be constructed from E^N as in Eq. (1). Let c_{abc} denote $\sum_{i=1}^{M} e_i[a]e_i[b]e_i[c]$. Observe that

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

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

$$\begin{aligned}
\left|\sum_{a=1}^{L} e_i[a]e_j[a]\right| &\overset{(a)}{=} \left|\sum_{a=1}^{L} e_{a+i-1}e_{a+j-1}\right| \\
&\overset{(b)}{\leq} \kappa N^{2/3},
\end{aligned} \tag{4}$$

where step (a) comes from using Eq. (1), and step (b) comes from the hypothesized upper bound on $C_2(E^N)$. 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

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

where step (a) comes from Eq. (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

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

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

$$L(L-1)(L-2)C_3^2(E^N) + L(3L-2)M^2 \geq ML^3 - M(M-1)\kappa^3 N^2.$$

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 E^N satisfying $C_2(E^N) \leq \kappa N^{2/3}$.

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

$$\alpha^3 N^3 C_3^2(E^N) \geq \epsilon \alpha^3 N^4 - \epsilon^2 \kappa^3 N^4 - 3\epsilon^2 \alpha^2 N^4.$$

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 $C_2(E^N)C_3(E^N) \gg N$

In Problem 2 on pg. 80 of [4] Gyarmati mentions that Mauduit [6] conjectured that $C_2(E^N)C_3(E^N) \gg N$. We verify this conjecture. We prove:

Theorem 4. *There is an absolute constant $c > 0$ such that for all E^N for all sufficiently large N we have $C_2(E^N)C_3(E^N) \geq cN$.*

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

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

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

$$L(L-1)(L-2)C_3^2(E^N) + L(3L-2)M^2 \geq ML^3 - M(M-1)C_2^3(E^N).$$

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

We rearrange this inequality to get

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

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

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

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

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

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

We now set $M = 3C_3^2(E^N)$. Thus

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

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

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

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

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

which is to say that

$$81 C_3^2(E^N) C_2^3(E^N) \geq 2N^3.$$

Writing this as

$$81 \left(C_2(E^N) C_3(E^N) \right)^2 C_2(E^N) \geq 2N^3,$$

we see that either $C_2(E^N) \geq \frac{1}{2}N$, in which case the lower bound in Eq. (7) gives $C_2(E^N)C_3(E^N) \geq \frac{1}{2}N$, or $C_2(E^N)C_3(E^N) \geq \frac{2}{9}N$. 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 $C_2(E^N)C_3(E^N) \geq \frac{2}{25}N$ for all E^N for all sufficiently large N. □

5. Concluding remarks

Our aim was to attack the conjecture of Mauduit [6], which we learnt from Gyarmati [4]. This has been settled in the affirmative in Theorem 4. 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 introduced by Mauduit and Sárközy.

Acknowledgements

This work was done towards the end of 2005, while visiting the Boole Center for Research in Informatics at University College Cork in Ireland. I would like to thank Neil O'Connell for his warm hospitality. The visit was supported by the Science Foundation of Ireland Grant Number SFI 04/RP1/1512. Research of the author is supported by the U. S. National Science Foundation Grants CCF-0500234, CNS-0627161, CCF-0635372, by Marvell Semiconductor, and by the University of California MICRO program. The author would also like to acknowledge TRUST (The Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422) and the following organizations: Cisco, ESCHER, HP, IBM, Intel, Microsoft, ORNL, Pirelli, Qualcomm, Sun, Symantec, Telecom Italia, and United Technologies for the support of his work.

References

[1] R. Ahlswede, L. Khachatrian, C. Mauduit, A. Sárközy, A complexity measure for families of binary sequences, Periodica Mathematica Hungarica 46 (2) (2003) 107–118.

[2] N. Alon, Y. Kohayakawa, C. Mauduit, C.G. Moreira, V. Rödl, Measures of pseudorandomness for finite sequences: Minimal values, Combinatorics, Probability, and Computing 15 (1–2) (2006) 1–29.

[3] J. Cassaigne, C. Mauduit, A. Sárközy, On finite pseudorandom binary sequences VII: The measures of pseudorandomness", Acta Arithmetica 103 (2) (2002) 97–118.

[4] K. Gyarmati, On the correlation of binary sequences, Studia Scientarium Mathematicarum Hungarica 42 (1) (2005) 79–93.

[5] Y. Kohayakawa, C. Mauduit, C.G. Moreira, V. Rödl, Measure of pseudorandomness for finite sequences: Minimum and typical values, in: Proceedings of WORDS'03, TUCS Gen. Publ., 27, Turku Cent. Comput. Sci., Turku, 2003. pp. 159–169.

[6] C. Mauduit, Construction of pseudorandom finite sequences, Unpublished lecture notes to the Conference on Information Theory and Some Friendly Neighbours - ein Wunschkonzert, University of Bielefeld, 2003.

[7] C. Mauduit, A. Sárközy, On finite pseudorandom binary sequences I. Measures of pseudorandomness, the Legendre symbol, Acta Arithmetica 82 (4) (1997) 365–377.

[8] L.R. Welch, Lower bounds on the maximum cross correlation of signals, IEEE Transactions on Information Theory 20 (3) (1974) 397–399.