Uniform Distribution Theory **10** (2015), no.1, 107–113

uniform distribution theory

ON A CONNECTION BETWEEN PSEUDORANDOM MEASURES

Richárd Sebők

Dedicated to Professor Harald Niederreiter on the occasion of his 70th birthday

ABSTRACT. Mauduit and Sárközy found the following connection between the well-distribution measure and the correlation measure of order 2: $W(E_N) \leq 3\sqrt{NC_2(E_N)}$. In this paper we will generalize this result to get similar connection between the combined PR-measure and the correlations of even order.

Communicated by Christian Mauduit

Mauduit and Sárközy in [6] introduced different pseudorandom measures of finite binary sequences in order to study their pseudorandom (often called as PR) properties.

For a binary sequence $E_N = (e_1, \dots, e_N) \in \{-1, +1\}^N$ of length N, the *well-distribution measure of* E_N is defined as

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

where the maximum is taken over all $a \in \mathbb{Z}$, $b, t \in \mathbb{N}$ such that $1 \leq a + b \leq a + bt \leq N$.

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

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

where the maximum is taken over all $D = (d_1, \dots, d_k)$ with non-negative integers $d_1 < \dots < d_k$ and $M \in \mathbb{N}$ such that $M + d_k \leq N$.

In [6], the authors showed that a finite binary sequence can be considered as a good PR-sequence, if both the well-distribution measure and the correlation measure are small. For more details, see Katalin Gyarmati's survey paper [4].

2010 Mathematics Subject Classification: Primary 11K45.
Keywords: binary sequences, pseudorandomness, well-distributions, correlation.

The *combined* (well-distribution-correlation) *PR-measure of order k of E_N* is defined as

$$Q_k(E_N) = \max_{a,b,t,D} \left|Z(a,b,t,D)\right| \tag{2}$$
$$= \max_{a,b,t,D} \left| \sum_{j=0}^{t-1} e_{a+jb+d_1} e_{a+jb+d_2} \dots e_{a+jb+d_k} \right|,$$

where the maximum is taken over all $a, b, t, D = (d_1, d_2, \dots, d_k)$ such that all the subscripts $a + jb + d_l$ belongs to $\{1, \dots, N\}$.

In [7] Mauduit and Sárközy found a strong connection between the well distribution measure of E_N and the correlation measure of order 2 of E_N, for every $E_N \in \{-1, +1\}^N$ (in [3], Gyarmati generalized Theorem A).

Theorem A. *For any $N \geq 1$ and $E_N = \{e_1, \dots, e_N\} \in \{-1, +1\}^N$, we have*

$$W(E_N) \leq 3\sqrt{NC_2(E_N)}. \tag{3}$$

We would like to improve this result in the following form:

Theorem 1. *For any $N \geq 1$ and $E_N = \{e_1, \dots, e_N\} \in \{-1, +1\}^N$, $k \in \mathbb{N}$, for $1 \leq l \leq k$, we have*

$$Q_k(E_N) \leq 2\sqrt{N \max_{1\leq l\leq k} C_{2l}(E_N)}. \tag{4}$$

Proof. Assume that

$$a, b, t \in \mathbb{N} \quad \text{and} \quad 1 \leq a \leq a + (t-1)b \leq a + (t-1)b + d_k \leq N \tag{5}$$

and write

$$e_n = 0 \quad \text{for } n > N.$$

If $t = 1$, then

$$|Z(a,b,t,D)| = |Z(a,b,1,D)| = 1 \leq \max_{1\leq l\leq k} C_{2l}(E_N) \leq (N \max_{1\leq l\leq k} C_{2l}(E_N))^{1/2}. \tag{6}$$

If $t \geq 2$, then it follows from (5) that

$$b < N$$

and

$$t - 1 \leq (t-1)b \leq N - a \leq N - 1 \tag{7}$$

whence

$$t \leq N.$$

Let $g_i = d_i - d_1$. Then $g_1 = 0$, but we will write it down sometimes if it makes things more understandable.

$$\begin{aligned}
&\sum_{i=a}^{a+b-1} \left(\sum_{j=0}^{t-1} e_{i+jb+d_1} \dots e_{i+jb+d_k} \right)^2 \\
&= \sum_{i=a}^{a+b-1} \left(\sum_{j_1=0}^{t-1} e_{i+j_1b+d_1} \dots e_{i+j_1b+d_k} \right) \left(\sum_{j_2=0}^{t-1} e_{i+j_2b+d_1 \dots} e_{i+j_2b+d_k} \right) \\
&= \sum_{i=a}^{a+b-1} \left(\sum_{j_1=j_2} 1 + 2 \sum_{0\le j_1<j_2\le t-1} e_{i+j_1b+d_1} \dots e_{i+j_1b+d_k} e_{i+j_2b+d_1} \dots e_{i+j_2b+d_k} \right) \\
&= tb + 2 \sum_{i=a+d_1}^{a+d_1+b-1} \sum_{0\le j_1<j_2\le t-1} e_{i+j_1b+g_1} \dots e_{i+j_1b+g_k} e_{i+j_2b+g_1} \dots e_{i+j_2b+g_k} \\
&= tb + 2 \sum_{i=a+d_1}^{a+d_1+b-1} \sum_{f=1}^{t-1} \sum_{j_1=0}^{t-1-f} e_{i+j_1b+g_1} \dots e_{i+j_1b+g_k} e_{i+j_1b+fb+g_1} \dots e_{i+j_1b+fb+g_k} \\
&= tb + 2 \sum_{f=1}^{t-1} \sum_{i=a+d_1}^{a+d_1+b-1} \sum_{j_1=0}^{t-1-f} e_{i+j_1b+g_1} \dots e_{i+j_1b+g_k} e_{i+j_1b+fb+g_1} \dots e_{i+j_1b+fb+g_k} \\
&= (t-1)b + b + 2 \sum_{f=1}^{t-1} \sum_{n=a+d_1}^{a+d_1+(t-f)b-1} e_{n+g_1} \dots e_{n+g_k} e_{n+fb+g_1} \dots e_{n+fb+g_k} \\
&< N + N + 2 \sum_{f=1}^{t-1} \left| \sum_{n=a+d_1}^{a+d_1+(t-f)b-1} e_n \dots e_{n+g_k} e_{n+fb} \dots e_{n+fb+g_k} \right| \qquad (8)
\end{aligned}$$

By investigating the innermost sum, we need to find the cases when

$$n + g_i = n + fb + g_j,$$

thus

$$fb = g_i - g_j = d_i - d_1 - (d_j - d_1) = d_i - d_j$$

for some $1 \le f \le t-1$.

If there is no such i and j that $fb = d_i - d_j$, then we sum the product of $2k$ different elements of the sequence E_N, and by the choice of $D' = (d'_1, \dots, d'_{2k})$, with

$$0 \le d'_1 \le \dots \le d'_{2k} \le a + (t-1)b + d'_{2k} \le N$$

and

$$\{a+d_1+g_1, a+d_1+g_2, \dots, a+d_1+g_k,\\ , a+d_1+fb+g_1, a+d_1+fb+g_2, \dots, a+d_1+fb+g_k\} = \{d'_1, \dots, d'_{2k}\}$$

we got that

$$\sum_{n=0}^{(t-f)b-1} e_{n+a+d_1+g_1} \dots e_{n+a+d_1+g_k} e_{n+a+d_1+fb} \dots e_{n+a+d_1+fb+g_k} =$$

$$= V(E_N, (t-f)b-1, D')$$

whence

$$\left| \sum_{n=0}^{(t-f)b-1} e_{n+a+d_1+g_1} \dots e_{n+a+d_1+g_k} e_{n+a+d_1+fb} \dots e_{n+a+d_1+fb+g_k} \right| \leq \tag{9}$$

$$\leq |V(E_N, (t-f)b-1, D')| \leq C_{2k}(E_N).$$

If there exist some i and j such that $fb = d_i - d_j$, then as we sum the product of $2k$ elements of the sequence E_N in the innermost sum, some of them are pairwise equal since their indices are identical. Of course the product of elements are 1, and $n+a+d_1+g_0$ are smaller than all the others, and $n+a+d_1+fb+g_k$ are greater than all the others, so at least two elements with those indices will remain.

$$\sum_{n=0}^{(t-f)b-1} e_{n+a+d_1+g_1} \dots e_{n+a+d_1+g_k} e_{n+a+d_1+fb} \dots e_{n+a+d_1+fb+g_k} =$$

$$= \sum_{n=0}^{(t-f)b-1} e_{n+j_1} e_{n+j_2} e_{n+j_3} \dots e_{n+j_{2l}},$$

where $1 \leq l < k$. With $D'' = (j_1, j_2, \dots, j_{2l})$

$$\sum_{n=0}^{(t-f)b-1} e_{n+j_1} e_{n+j_2} \dots e_{n+j_{2l}} = V(E_N, (t-f)b-1, D'),$$

thus

$$\left| \sum_{n=a+d_1}^{a+d_1+(t-f)b-1} e_{n+j_1} e_{n+j_2} \dots e_{n+j_{2l}} \right| \leq \tag{10}$$

$$\leq |V(E_N, (t-f)b-1, D'')| \leq C_{2l}(E_N).$$

If we take a look at (8) again, for every f in

$$\sum_{f=1}^{t-1}\left|\sum_{n=a+d_1}^{a+d_1+(t-f)b-1} e_n\dots e_{n+g_k}e_{n+fb}\dots e_{n+fb+g_k}\right|$$

we can give an upper bound to the innermost sum as

$$\left|\sum_{n=a+d_1}^{a+d_1+(t-f)b-1} e_n\dots e_{n+g_k}e_{n+fb}\dots e_{n+fb+g_k}\right|\le C_{2l}(E_N)$$

for some $1\le l\le k$, which means

$$\sum_{f=1}^{t-1}\left|\sum_{n=a+d_1}^{a+d_1+(t-f)b-1} e_n\dots e_{n+g_k}e_{n+fb}\dots e_{n+fb+g_k}\right|\le \sum_{f=1}^{t-1}\max_{1\le l\le k} C_{2l}(E_N). \quad (11)$$

So by (11) and (7), from (8) we get that

$$\begin{aligned}(Z(a,b,t,D))^2 &< 2N+2(t-1)\max_{1\le l\le k} C_{2l}(E_N)\\ &\le (2N+2(t-1))\max_{1\le l\le k} C_{2l}(E_N)\\ &< 4N\max_{1\le l\le k} C_{2l}(E_N), \qquad (12)\end{aligned}$$

in the case when $t\ge 2$, and with (6), it proves the theorem. □

Cassaigne, Mauduit and Sárközy in [2] Theorem 4 proved a result for a connection between correlation measures of different order.

Theorem B. *For $k\in\mathbb{N}$, $l\in\mathbb{N}, k|l$, $N\in\mathbb{N}$ $E_N\in\{-1,+1\}^N$, we have*

$$C_k(E_N)\le N^{1-\frac{k}{l}}\left((C_l(E_N))^{\frac{k}{l}}\frac{(l!)^{\frac{k}{l}}}{k!}+\left(l^2\right)^{\frac{k}{l}}\right)$$

Using this result we will see that $Q_2(E_N)$ can be bounded by $C_4(E_N)$

Corollary 1. *For all $E_N=\{e_1,\dots,e_N\}\in\{-1,+1\}^N$, we have*

$$Q_2(E_N)\le 5\sqrt{NC_4(E_N)}. \quad (13)$$

Proof. If $t=1$, then

$$|Z(a,b,t,D)|=|Z(a,b,1,D)|=1\le C_4(E_N)\le 5(NC_4(E_N))^{1/2}. \quad (14)$$

If $t \geq 2$, then take (8) with $k = 2$, which yields

$$\sum_{i=a}^{a+b-1} \left(\sum_{j=0}^{t-1} e_{i+jb+d_1} e_{i+jb+d_2} \right)^2 < \tag{15}$$

$$< 2N + 2 \sum_{f=1}^{t-1} \left| \sum_{n=a+d_1}^{a+d_1+(t-f)b-1} e_n e_{n+d} e_{n+fb} e_{n+fb+d} \right| .$$

From Theorem B we can give an upper bound for $C_2(E_N)$

$$C_2(E_N) \leq \sqrt{N} \left(\sqrt{6} \sqrt{C_4(E_N)} + 4 \right) < 7 \sqrt{N C_4(E_N)}. \tag{16}$$

In the case $b|d$, for a fix f, $fb = d$ and the upper bound for the innermost sum in (15) is given by $C_2(E_N)$, otherwise by $C_4(E_N)$. By Theorem B and (16) we got

$$\begin{aligned} (Z(a,b,t,D))^2 &= \left(\sum_{j=0}^{t-1} e_{i+jb+d_1} e_{i+jb+d_2} \right)^2 \leq \sum_{i=a}^{a+b-1} \left(\sum_{j=0}^{t-1} e_{i+jb+d_1} e_{i+jb+d_2} \right)^2 \\ &< 2N + 2(t-2) C_4(E_N) + 2 C_2(E_N) \\ &\leq 2N C_4(E_N) + 2(N-2) C_4(E_N) + 2 \cdot 7 \sqrt{N C_4(E_N)} \\ &\leq 2N C_4(E_N) + 2(N-2) C_4(E_N) + 14 N C_4(E_N) \\ &< 18 N C_4(E_N). \end{aligned} \tag{17}$$

In the case $b \nmid d$

$$\begin{aligned} (Z(a,b,t,D))^2 &= \left(\sum_{j=0}^{t-1} e_{i+jb+d_1} e_{i+jb+d_2} \right)^2 \leq \sum_{i=a}^{a+b-1} \left(\sum_{j=0}^{t-1} e_{i+jb+d_1} e_{i+jb+d_2} \right)^2 \\ &< 2N + 2 \sum_{f=1}^{t-1} C_4(E_N) = 2N + 2(t-1) C_4(E_N) \\ &\leq 2N C_4(E_N) + 2(N-1) C_4(E_N) \\ &< 4N C_4(E_N) \end{aligned} \tag{18}$$

which proves the corollary. □

Remark

One would like to know if there is a stronger form of Theorem 1:

$$Q_k(E_N) \ll \sqrt{NC_{2k}(E_N)},$$

but so far I did not manage to answer this question. If there is such a sequence E_N, where $Q_k(E_N)$ cannot be bounded by a constant times $\sqrt{NC_{2k}(E_N)}$, then by [1] and [5] we know that for every even l,

$$\min_{E_N \in \{-1,+1\}^N} C_l(E_N) \geq \sqrt{\frac{1}{2}\left[\frac{N}{l+1}\right]},$$

thus

$$Q_k(E_N) \gg N^{\frac{3}{4}}$$

holds for this sequence.

I would like to thank Professor C. Mauduit for asking this important question.

REFERENCES

[1] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira, and V. Rödl. *Measures of pseudorandomness for finite sequences: minimal values*, Combin., Probab. Comput 15. (2005), 1-29.

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

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

[4] K. Gyarmati, *Measures of pseudorandomness*, P. Charpin, A. Pott, A. Winterhof (eds.), Radon Series in Computational and Applied Mathematics, de Gruyter (2013), 43-64.

[5] Y. Kohayakawa, C. Mauduit, C. G. Moreira, and V. Rödl, *Measures of pseudorandomness for finite sequences: minimal and typical values*, Proceeding of WORDS'03, TUCS Gen. Publ. 27, Turku Cent. Comput. Sci., Turku, (2003) 159-169.

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

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

Received August 26, 2014
Accepted October 23, 2014

Eötvös Loránd University
Department of Algebra and Number Theory
H-1117 Budapest, Pázmány Péter sétány 1/C
E-mail: sebokr@cs.elte.hu