On the typical values of the cross-correlation measure

László Mérai

On the typical values of the cross-correlation measure

László Mérai

Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenbergerstr. 69, 4040 Linz, Austria
merai@cs.elte.hu

Abstract. In order to study the pseudorandomness of families of finite binary sequences $\mathcal{F} \subset \{-1,1\}^N$, Gyarmati, Mauduit and Sárközy introduced the *cross-correlation measure* $\Phi_k(\mathcal{F})$ *of order* k. In this paper we study the order of magnitude of the cross-correlation measure $\Phi_k(\mathcal{F})$ for typical families $\mathcal{F}$.

1 Introduction

Pseudorandom binary sequences play an important role in many applications, such as cryptography, Monte-Carlo integration, etc. The pseudorandomness of individual sequences is usually tested by complexity-theoretic (e.g. linear complexity) or statistical (e.g. discrepancy, poker test, runs test or other NIST tests) methods. Since these two types of tests are in a sense independent (see e.g. [18]), it is crucial to test the sequences both complexity-theoretically and statistically.

In [14], Mauduit and Sárközy introduced a new kind of measures to study the pseudorandom behavior of finite binary sequences which are related to both complexity-theoretic and statistical meaning of pseudorandomness. Namely, consider the binary sequence

$$E_N = (e_1, e_2, \ldots, e_N) \in \{-1,1\}^N.$$

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

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

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

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

where the maximum is taken over all $D = (d_1, d_2, \ldots, d_k)$ with non-negative integers $0 \le d_1 < d_2 < \cdots < d_k < N$ and $M \in \mathbb{N}$ with $M + d_k \le N$.

Cassaigne, Mauduit and Sárközy [6] studied the typical values of $C_k(E_N)$, when the binary sequences E_N are chosen equiprobable from $\{-1,1\}^N$. Later Alon, Kohayakawa, Mauduit, Moreira and Rödl [1] improved their result.

Theorem 1 (Alon, Kohayakawa, Mauduit, Moreira, Rödl). *For any given $\varepsilon > 0$, there exist N_0 and $\delta > 0$ such that if $N \geq N_0$, then,*

$$\delta\sqrt{N} < W(E_N) < \frac{1}{\delta}\sqrt{N}$$

with probability at least $1-\varepsilon$.

Theorem 2 (Alon, Kohayakawa, Mauduit, Moreira, Rödl). *For fixed $0 < \varepsilon_0 \leq 1/16$, there is a constant $N_0 = N_0(\varepsilon_0)$ such that if $N \geq N_0$, then, with probability at least $1-\varepsilon_0$, we have*

$$\frac{2}{5}\sqrt{N\log\binom{N}{k}} < C_k(E_N) < \sqrt{(2+\varepsilon_1)N\log\left(N\binom{N}{k}\right)}$$
$$< \sqrt{(3+\varepsilon_0)N\log\binom{N}{k}} < \frac{7}{4}\sqrt{N\log\binom{N}{k}}.$$

for every integer k with $2 \leq k \leq N/4$, where $\varepsilon_1 = \varepsilon_1(N) = (\log\log N)/\log N$.

Based on Theorems 1 and 2, the sequence E_N be said to have good pseudorandom property if both these measures $W(E_N)$ and $C_k(E_N)$ (up to sufficiently large k) are $o(N)$.

The measures $W(E_N)$ and $C_k(E_N)$ are strongly connected to statistical tests. In particular, Mauduit, Niederreiter and Sárközy studied the connection between these type of measures and the discrepancy [13], while Rivat and Sárközy showed that small well-distribution and correlation measures imply strong pseudorandomness in terms of many NIST tests [19].

On the other hand small correlation measure ensures large (linear) complexity, (see [5]).

Many sequences have been tested for pseudorandomness in terms of these measures (see, e.g. [7] [12] [14], [15], [16], [20] and the references therein). For example, it was shown in [14], that for the Legendre symbol sequence $E_N = (e_1, e_2, \ldots, e_p)$ defined by

$$e_n = \begin{cases} \left(\frac{f(n)}{p}\right) & \text{if } p \nmid f(n), \\ 1 & \text{otherwise,} \end{cases} \tag{1}$$

where p is a prime, $(\frac{\cdot}{p})$ is the Legendre symbol modulo p and $f \in \mathbb{F}_p[x]$, we have

$$W(E_p) < 10\deg f p^{1/2}\log p \quad \text{and} \quad C_k(E_p) < 10k\deg f p^{1/2}\log p,$$

if f satisfies certain conditions, for example if f is irreducible.

The well-distribution and the correlation measures concern only the pseudorandomness of an individual sequence. However, in applications one may need a whole family of sequences which contains "large" number of "independent" sequences with good pseudorandom properties. One of the notion appearing in the literature which is connected to such independence is the *avalanche effect* (see, e.g. [3], [8],[11],[21], [22]).

Definition 1. *If $N \in \mathbb{N}$, then the (Hamming) distance $d(E_N, E'_N)$ between the sequences $E_N = (e_1, e_2, \ldots, e_N) \in \{-1, 1\}^N$ and $E'_N = (e'_1, e'_2, \ldots, e'_N) \in \{-1, 1\}^N$ is defined as*

$$d(E_N, E'_N) = |\{n : \ 1 \le n \le N, \ e_n \ne e'_n\}|.$$

Moreover, the minimum distance $m(\mathcal{F})$ of a family $\mathcal{F} \subset \{1, -1\}^N$ is defined as

$$m(\mathcal{F}) = \min\{d(E_N, E'_N) : \ E_N, E'_N \in \mathcal{F}, \ E_N \ne E'_N\}.$$

The family $\mathcal{F} \subset \{1, -1\}^N$ possesses the strict avalanche property if

$$m(\mathcal{F}) \ge \left(\frac{1}{2} - o(1)\right) N. \tag{2}$$

2 The definition of the cross-correlation measure

In [10], Gyarmati, Mauduit and Sárközy introduced a new quantity for families $\mathcal{F} \subset \{-1, 1\}^N$.

Definition 2. *Let $N, k \in \mathbb{N}$, and for any k binary sequences $E_N^{(1)}, E_N^{(2)}, \ldots, E_N^{(k)}$ with*

$$E_N^{(i)} = (e_1^{(i)}, e_2^{(i)}, \ldots, e_N^{(i)}) \in \{-1, 1\}^N, \quad \text{for } i = 1, 2, \ldots, k,$$

and any $M \in \mathbb{N}$ and k-tuple $D = (d_1, \ldots, d_k)$ of non-negative integers with

$$0 \le d_1 \le d_2 \le \cdots \le d_k < M + d_k \le N, \tag{3}$$

write

$$V_k\left(E_N^{(1)}, E_N^{(2)}, \ldots, E_N^{(k)}, M, D\right) = \sum_{n=1}^{M} e_{n+d_1}^{(1)} e_{n+d_2}^{(2)} \ldots e_{n+d_k}^{(k)}.$$

Let

$$\widetilde{C}_k\left(E_N^{(1)}, E_N^{(2)}, \ldots, E_N^{(k)}\right) = \max_{M,D} \left|V_k\left(E_N^{(1)}, E_N^{(2)}, \ldots, E_N^{(k)}, M, D\right)\right|,$$

where the maximum is taken over all $D = (d_1, \ldots, d_k)$ and $M \in \mathbb{N}$ satisfying (3) with the additional restriction that if $E_N^{(i)} = E_N^{(j)}$ for some $i \ne j$, then we must not have $d_i = d_j$. Then the cross-correlation measure of order k *of the family $\mathcal{F}$ of binary sequences $E_N \in \{-1, 1\}^N$ is defined as*

$$\Phi_k(\mathcal{F}) = \max \widetilde{C}_k\left(E_N^{(1)}, E_N^{(2)}, \ldots, E_N^{(k)}\right),$$

where the maximum is taken over all k-tuples of binary sequences

$$\left(E_N^{(1)}, E_N^{(2)}, \ldots, E_N^{(k)}\right), \quad E_N^{(i)} \in \mathcal{F}, \quad \text{for } i = 1, \ldots, k.$$

Clearly, for the family $\mathcal{F} = \{E_N\}$ of size 1 we have

$$\Phi_k(\{E_N\}) = C_k(E_N).$$

On the other hand for general $\mathcal{F}$ we have

$$\Phi_k(\mathcal{F}) \geq \max_{E_N \in \mathcal{F}} C_k(E_N). \tag{4}$$

Moreover, families of small cross-correlation measure of order 2 posses the strict avalanche property [10].

Proposition 1 (Gyarmati, Mauduit, Sárközy). *If $N \in \mathbb{N}$, $\mathcal{F} \subset \{1, -1\}^N$, then we have*

$$m(\mathcal{F}) \geq \frac{N}{2} - \frac{1}{2}\Phi_2(\mathcal{F})$$

3 Typical values of $\Phi_k(\mathcal{F})$

In this paper we estimates $\Phi_k(\mathcal{F})$ for "random" families $\mathcal{F}$ of sequences E_N with given length N and family size $|\mathcal{F}|$, i.e. we choose a family $\mathcal{F}$ from all subsets of $\{-1, 1\}^N$ of size $|\mathcal{F}|$ with the same probability.

We expect, that for a "random" family $\mathcal{F} \subset \{-1, 1\}^N$ the cross-correlation measure is "small" in terms of N (in particular $o(N)$ as $N \to \infty$). However, the value of $\Phi_k(\mathcal{F})$ strongly depends on the size of the family $\mathcal{F}$. If $\mathcal{F}$ is large: $|\mathcal{F}| > 2^{cN}$ with some $0 < c < 1/2$, then it follows from results of coding theory, that (2) cannot hold (see, e.g. [23]), thus by Proposition 1 $\Phi_2(\mathcal{F})$ is large: $\Phi_2(\mathcal{F}) = c'N$ for a constant c' (here $c = 0.18$ can be taken).

On the other hand, if $|\mathcal{F}| < 2^{cN}$ with $c \leq 1/12 = 0.0833\ldots$, then the behavior of $\Phi_k(\mathcal{F})$ can be controlled.

Theorem 3. *For a given $\varepsilon > 0$, there exists N_0, such that if $N > N_0$ and $1 \leq \log_2 |\mathcal{F}| < N/12$, then we have with probability at least $1 - \varepsilon$, that*

$$\frac{2}{5}\sqrt{N\left(\log\binom{N}{k} + k \log |\mathcal{F}|\right)} < \Phi_k(\mathcal{F}) < \frac{5}{2}\sqrt{N\left(\log\binom{N}{k} + k \log |\mathcal{F}|\right)}$$

for every integer k with $2 \leq k \leq N/(6 \log_2 |\mathcal{F}|)$.

(Here $\log_2$ is the logarithm to base 2: $\log_2 = \log / \log 2$.)

In Appendix we sketch the proof. For details, see the full version of this abstract [17].

4 An example for a family of pseudorandom binary sequences

Based on Theorems 1, 3 and (4), a family $\mathcal{F} \subset \{-1,1\}^N$ said to have good pseudorandom properties if for all individual sequence $E_N \in \mathcal{F}$ we have $W(E_N) = o(N)$ and $\Phi_k(\mathcal{F}) = o(N)$ (at least for small k). In [10], it was shown by an example, that such a family can be constructed by the Legendre symbol.

Theorem 4 (Gyarmati, Mauduit, Sárközy). *Let $d \in \mathbb{N}$, p a prime number, $d < p$, and consider all the irreducible polynomials $f(x) \in \mathbb{F}_p[x]$ of the form*

$$f(x) = x^d + a_2 x^{d-2} + a_3 x^{d-3} + \cdots + a_d$$

(so that there is no x^{d-1} term) and let $\mathcal{F}$ denote the family of sequences $E_p = E_p(f)$ assigned to these polynomials f by the formula (1). Then

1. *for all $E_p(f) \in \mathcal{F}$, we have*

$$W(E_p(f)) < 10kp^{1/2}\log p;$$

2. *for all $1 < k < p$ we have*

$$\Phi_k(\mathcal{F}) < 10kdp^{1/2}\log p;$$

3. *if $d < p^{1/2}/20\log p$, then*

$$|\mathcal{F}| \geq p^{\lfloor d/3 \rfloor - 1}.$$

Acknowledgment The author is partially supported by the Austrian Science Fund FWF Project F5511-N26 which is part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications".

Appendix

In this section we sketch the proof. For more details, see the full version of this abstract [17].

To prove the theorem it is more convenient to work *generators* instead of families of sequences. Namely, let $\mathcal{S}$ be a given set and $N \in \mathbb{N}$ be an integer. Consider the map $G : \mathcal{S} \to \{-1,1\}^N$ where

$$s \mapsto E_N(s) = (e_1(s), e_2(s), \ldots, e_N(s)) \in \{-1,1\}^N.$$

The cross-correlation measure $\widetilde{\Phi}_k(G)$ of the generator $G : \mathcal{S} \to \{-1,1\}^N$ can be defined in the following way.

Let $M, k_1, \ldots, k_\ell \geq 1$ be integers with the restriction $k = k_1 + \cdots + k_\ell \geq 2$. Let $D = (d_1^1, \ldots, d_{k_1}^1, \ldots, d_1^\ell, \ldots, d_{k_\ell}^\ell)$ be a k-tuple such that

$$0 \leq d_1^i < \cdots < d_{k_i}^i < M + d_{k_i}^i \leq N, \quad \text{for } i = 1, \ldots, \ell. \tag{5}$$

Then for distinct $s_1, \dots, s_\ell \in \mathcal{S}$ write

$$V_{k_1,\dots,k_\ell}\left(E_N(s_1), \dots, E_N(s_\ell), M, D\right) = \sum_{n=1}^{M} e_{n+d_1^1}(s_1) \dots e_{n+d_{k_1}^1}(s_1) \dots e_{n+d_1^\ell}(s_\ell) \dots e_{n+d_{k_\ell}^\ell}(s_\ell).$$

The *cross-correlation measure of order* k of the generator G is defined as

$$\widetilde{\Phi}_k(G) = \max \left| V_{k_1,\dots,k_\ell}\left(E_N(s_1), \dots, E_N(s_\ell), M, D\right) \right|,$$

where the maximum is taken over all integers $k_1, \dots, k_\ell \geq 1$ such that $k = k_1 + \dots + k_\ell$, all $s_1, \dots, s_\ell \in \mathcal{S}$, and all M and D satisfying (5).

If the generator G is collision free (injection), then $\widetilde{\Phi}_k(G) = \Phi_k(\mathcal{F})$ with the family

$$\mathcal{F} = \mathcal{F}(G) = \{E_N(s) : s \in \mathcal{S}\}.$$

On the other hand, if there is a collision: $E_N(s) = E_N(s')$ for $s \neq s'$, then $\widetilde{\Phi}_k(G) = N$.

Since if $\log_2 |\mathcal{S}| < cN$ with $c < 1/2$, then for a random generator G, the probability of collision is small, thus it is enough to estimate the typical values of $\widetilde{\Phi}_k(G)$.

The proof falls naturally into two parts. For the upper bound let

$$S^{\pm}(n) = \sum_{1 \leq i \leq n} X_i,$$

where X_i $(1 \leq i \leq n)$ are independent random variables with mean 0, that is,

$$\mathbb{P}(X_i = -1) = \mathbb{P}(X_i = +1) = 1/2.$$

Clearly, $V_{k_1,\dots,k_\ell}\left(E_N(s_1), \dots, E_N(s_\ell), M, D\right)$ has the same distribution as $S^{\pm}(M)$.

The following lemma states a well-known estimate for large deviation of $S^{\pm}(n)$ (see, e.g. [2, Appendix 2])

Lemma 1. *Let X_i $(1 \leq i \leq n)$ are independent ± 1 random variables with mean 0. Let $S^{\pm}(n) = \sum_{1 \leq i \leq n} X_i$. For any real number $a > 0$, we have*

$$\mathbb{P}(S^{\pm}(n) > a) < e^{-a^2/2n}.$$

The following lemma gives an upper bound of the maximum of random variables having the same distribution as $S^{\pm}(n)$ for some n.

Lemma 2. *For $1 \leq \log_2 |\mathcal{S}| < \log_2 N$ we have*

$$\widetilde{\Phi}_k(G) < 2\sqrt{N\left(\log \binom{N}{k} + k \log |\mathcal{S}|\right)},$$

and for $\log_2 N \le \log_2 |\mathcal{S}| < N/12$ *we have*

$$\widetilde{\Phi}_k(G) < 2\sqrt{N\left(k\log N + \log\binom{|\mathcal{S}|}{k}\right)}$$
$$< 2\sqrt{N\left(\log\binom{N}{k} + (1+o(1))k\log|\mathcal{S}|\right)}$$

with probability tending to 1 as $N \to \infty$ *for every integer* k *with* $2 \le k \le N/(6\log_2|\mathcal{S}|)$.

For the lower bound let us define $S(n,p)$ as the sum of n independent Bernoulli random variables with mean p. Clearly, $(S^{\pm}(n)+n)/2$ has the same distribution as $S(n,1/2)$. We use the following bounds on the symmetric binomial distribution (see e.g. [4, Chapter 1, Theorem 6] and [1, Fact 10] resp.).

Lemma 3. *(i) For any* $c = c(n) > 0$ *with* $c = o(n^{1/6})$, *we have*

$$\mathbb{P}\left(S(n,1/2) \ge \left\lfloor\frac{n}{2}\right\rfloor + c\sqrt{n}\right) = \sum_{\ell \ge c\sqrt{n}} \frac{1}{2^n}\binom{n}{\lfloor n/2\rfloor + \ell}$$
$$= \left(\sqrt{\frac{2}{\pi}+o(1)}\right)\left(\int_c^\infty e^{-2x^2}dx\right). \qquad (6)$$

In particular, if we further have that $c \to \infty$, *then*

$$\mathbb{P}\left(S(n,1/2) \ge \left\lfloor\frac{n}{2}\right\rfloor + c\sqrt{n}\right) = \frac{e^{-2c^2}}{2c\sqrt{2\pi}}(1+o(1)). \qquad (7)$$

(ii) The estimates (6) and (7) hold for the lower tail

$$\mathbb{P}\left(S(n,1/2) \le \left\lfloor\frac{n}{2}\right\rfloor - c\sqrt{n}\right)$$

as well.

Let $\{x\} = x - \lfloor x\rfloor$. We have the following lower estimate for the symmetric binomial distribution (see [1, Fact 10])

Lemma 4. *Let* n *and* c *be integers with*

$$-\left\lfloor\frac{n}{2}\right\rfloor \le c \le \left\lceil\frac{n}{2}\right\rceil.$$

If n *is sufficiently large, then*

$$\mathbb{P}\left(S(n,1/2) = \left\lfloor\frac{n}{2}\right\rfloor + c\right) = \frac{1}{2^n}\binom{n}{\lfloor n/2\rfloor + c}$$
$$\ge (1+o(1))2^{-4(c+\{n/2\})^2/n}\sqrt{\frac{2}{\pi n}}.$$

The following lemma gives a lower bound of maximum of random variable having the same distribution as $S^{\pm}(n)$ for some n.

Lemma 5. *For* $1 \le \log_2 |\mathcal{S}| \le m^{1/4}$ *we have*

$$\widetilde{\Phi}_k(G) > \frac{4}{9}\sqrt{N\left(\log\binom{N}{k} + k\log|\mathcal{S}|\right)},$$

and for $m^{1/4} < \log_2 |\mathcal{S}| < N/12$ *we have*

$$\begin{aligned}\widetilde{\Phi}_k(G) &> \frac{4}{9}\sqrt{N\left(k\log N + \log\binom{|\mathcal{S}|}{k}\right)} \\ &> \frac{4}{9}\sqrt{N\left(\log\binom{N}{k} + (1-o(1))k\log|\mathcal{S}|\right)},\end{aligned}$$

with probability tending to 1 as $N \to \infty$ *for every integer* k *with* $2 \le k \le N/(6\log_2|\mathcal{S}|)$.

Proof (Lemma 5). We briefly sketch the proof of the first part, when $\mathcal{S}$ is small $1 \le \log_2|\mathcal{S}| \le m^{1/4}$. Let $m = \lfloor N/3 \rfloor$ and for $1 \le \log_2|\mathcal{S}| \le m^{1/4}$ consider the maximal $r = r_k(m,\mathcal{S}) \in \mathbb{N}$ such that

$$\mathbb{P}\left(S(m,1/2) \ge \frac{1}{2}(m+r)\right) \ge \frac{k^2\log N}{\binom{m+1}{k-1}|\mathcal{S}|^k}$$

holds. Then, it can be shown (Lemma 7 in [17]) that

$$r(m) \ge \frac{4}{9}\sqrt{N\left(\log\binom{N}{k} + k\log|\mathcal{S}|\right)}.$$

On the other hand

$$\widetilde{\Phi}_k(G) \le r_k(m,\mathcal{S}) \tag{8}$$

holds with probability at most $O(1/k^2\log N)$ (see the proof of Lemma 5 in [17]). Then, summing over all $2 \le k \le N/(6\log_2|\mathcal{S}|)$ we get that (8) holds for *some* k with $2 \le k \le N/(6\log_2|\mathcal{S}|)$ with probability $O(1/\log N) = o(1)$. Whence (8) does not hold for all $2 \le k \le N/(6\log_2|\mathcal{S}|)$ with probability $1 - o(1)$, which proves the lemma.

References

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

2. N. Alon and J. H. Spencer, The probabilistic method, second ed., Wiley-Interscience Series in Discrete Mathematics and Optimization, Wiley-Interscience [John Wiley & Sons], New York, 2000, With an appendix on the life and work of Paul Erdős
3. A. Bérczes, J. Ködmön and A. Pethő, A one-way function based on norm form equations, Period. Math. Hungar. 49 (2004), 1–13.
4. B. Bollobás, Random graphs, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London, 1985.
5. N. Brandstätter, A. Winterhof, Linear complexity profile of binary sequences with small correlation measure. Period. Math. Hungar. 52 (2006), no. 2, 1–8.
6. J. Cassaigne, C. Mauduit and A. Sárközy, On finite pseudorandom binary sequences VII: The measures of pseudorandomness, Acta Arith. 103 (2002), no. 2, 97–118.
7. Z. Chen, Elliptic curve analogue of Legendre sequences. Monatsh. Math. 154 (2008), no. 1, 1–10.
8. H. Feistel, W. A. Notz and J. L. Smith, Some cryptographic techniques for machine-to-machine data communications, Proc. IEEE 63 (1975), 1545–1554.
9. K. Gyarmati, Measures of pseudorandomness, P. Charpin, A. Pott, A. Winterhof (eds.), Radon Series in Computational and Applied Mathematics, de Gruyter 2013, 43-64.
10. K. Gyarmati, C. Mauduit, A. Sárközy, The cross-correlation measure for families of binary sequences, Applications of Algebra and Number Theory (Lectures on the occasion of Harald Niederreiter's 70th Birthday) (edited by G. Larcher, F. Pillichshammer, A. Winterhof, and C. Xing), 126–143, Cambridge University Press (2014).
11. J. Kam, G. Davida, Structured design of substitution-permutation encryption networks, IEEE Transactions on Computers 28 (1979), 747–753.
12. H. Liu, New pseudorandom sequences constructed by quadratic residues and Lehmer numbers. Proc. Amer. Math. Soc. 135 (2007), no. 5, 1309–1318.
13. C. Mauduit, H. Niederreiter, A. Sárközy, On pseudorandom $[0, 1)$ and binary sequences, Publ. Math. Debrecen 71 (2007), no. 3-4, 305–324.
14. C. Mauduit, A. Sárközy, On finite pseudorandom binary sequences I: Measures of pseudorandomness, the Legendre symbol, Acta Arith. 82 (1997) 365–377.
15. L. Mérai, A construction of pseudorandom binary sequences using both additive and multiplicative characters. Acta Arith. 139 (2009), no. 3, 241–252
16. L. Mérai, Construction of pseudorandom binary sequences over elliptic curves using multiplicative characters. Publ. Math. Debrecen 80 (2012), no. 1-2, 199–213
17. L. Mérai, On the typical values of the cross-correlation measure, submitted, `http://compalg.inf.elte.hu/~merai/pub/merai_crossCorrelation.pdf`
18. H. Niederreiter, The independence of two randomness properties of sequences over finite fields. J. Complexity 28 (2012), no. 2, 154–161.
19. J. Rivat, A. Sárközy, On pseudorandom sequences and their application, in: General Theory of Information Transfer and Combinatorics, eds. R. Ahlswede et al., LNCS 4123, Springer, 2006; pp. 343–361.
20. A. Sárközy, A. Winterhof, Measures of pseudorandomness for binary sequences constructed using finite fields. Discrete Math. 309 (2009), no. 6, 1327–1333
21. V. Tóth, Collision and avalanche effect in families of pseudorandom binary sequences, Period. Math. Hungar. 55 (2007), 185–196.
22. V. Tóth, The study of collision and avalanche effect in a family of pseudorandom binary sequences, Period. Math. Hungar. 59 (2009), 1–8.

23. M. Tsfasman, S. Vlăduţ and D. Nogin, Algebraic Geometric Codes: Basic Notions, in: Mathematical Surveys and Monographs, Vol. 139, AMS, 2007.