Katalin Gyarmati

Measures of Pseudorandomness

Abstract: In the second half of the 1990s Christian Mauduit and András Sárközy [86] introduced a new quantitative theory of pseudorandomness of binary sequences. Since then numerous papers have been written on this subject and the original theory has been generalized in several directions. Here I give a survey of some of the most important results involving the new quantitative pseudorandom measures of finite binary sequences. This area has strong connections to finite fields, in particular, some of the best known constructions are defined using characters of finite fields and their pseudorandom measures are estimated via character sums.

Keywords: Pseudorandomness, Well Distribution, Correlation, Normality

2010 Mathematics Subject Classifications: 11K45

Katalin Gyarmati: Department of Algebra and Number Theory, Eötvös Loránd University, Budapest, Hungary, e-mail: gykati@cs.elte.hu

1 Introduction

In the twentieth and twenty-first centuries various pseudorandom objects have been studied in cryptography and number theory since these objects are widely used in modern cryptography, in applications of the Monte Carlo method and in wireless communication (see [39]). Different approaches and definitions of pseudorandomness can be found in several papers and books. Menezes, Oorschot and Vanstone [95] have written an excellent monograph about these approaches. The most frequently used interpretation of pseudorandomness is based on complexity theory; Goldwasser [38] has written a survey paper about this approach. However, recently the complexity theory approach has been widely criticized. One problem is that in this approach usually *infinite* sequences are tested while in the applications only *finite* sequences are used. Another problem is that most results are based on certain unproved hypotheses (such as the difficulty of factorization of integers). Finite pseudorandom $[0, 1)$ sequences have been studied by Niederreiter and others (see, for example, [103–106]). Niederreiter [107] also studied random number generation and quasi-Monte Carlo methods and their connections.

Research partially supported by ERC/AdG.228005, Hungarian National Foundation for Scientific Research, Grants No. K72731 and K100291 and the János Bolyai Research Fellowship.

In the second half of the 1990s, Christian Mauduit and András Sárközy [86] introduced a new constructive approach, in which the pseudorandomness of finite binary sequences is well characterized, and they also constructed binary sequences (and later other pseudorandom objects) with strong pseudorandom properties. In order to characterize the pseudorandomness of binary sequences Mauduit and Sárközy introduced new quantitative pseudorandom measures. Although earlier certain statistical tests (see, for example, [95]) already existed and one could determine whether a sequence passes these tests or not, the pseudorandom properties of the sequence were not classified. We also mention that by using these tests it was possible to test a sequence after generating it (*a posteriori testing*), but we did not have any *a priori* result which guaranteed the applicability of the sequence before generating it. There are two fundamental problems with a posteriori testing. Firstly, it could be quite lengthy to check whether or not a sequence passes these tests and it is much faster if certain properties of the construction guarantee that these tests are always passed for certain theoretical reasons (*a priori testing*). Secondly, in the case of a posteriori testing we always test only one certain, very special property of the sequence and nothing is known about the other pseudorandom properties. By using the pseudorandom measures of Mauduit and Sárközy it is possible to control several pseudorandom properties of sequences and it is also possible to *measure* their quality. In [118] Rivat and Sárközy estimated the outcome of certain basic statistical tests by the pseudorandom measures W and C_ℓ (see Section 2 below; the precise definitions of these tests can be found, for example, in [95]). In [122] Sárközy gave a survey of this new constructive theory of pseudorandomness. In the present survey we will focus mostly on pseudorandom measures; we will study the most important properties of these measures and their connections with other cryptographic tools.

2 Definition of the Pseudorandom Measures

In [86] Mauduit and Sárközy introduced the following pseudorandom measures in order to study the pseudorandom properties of *finite* binary sequences:

Definition 2.1. For a binary sequence $E_N = (e_1, \dots, e_N) \in \{-1, +1\}^N$ of length N, write

$$U(E_N, t, a, b) = \sum_{j=0}^{t} e_{a+jb} .$$

Then the *well-distribution measure of* E_N is defined as

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

where the maximum is taken over all a, b, t such that $a, b, t \in \mathbb{N}$ and $1 \le a \le a + tb \le N$.

The well-distribution measure studies how close are the frequencies of the $+1$'s and -1's in arithmetic progressions (for a binary sequence with strong pseudorandom properties these two quantities are expected to be very close). But often it is also necessary to study the connections between certain elements of the sequence. For example, if the subsequence $(+1,+1)$ occurs much more frequently than the subsequence $(-1,-1)$, it may cause problems in the applications, and we cannot say that our sequence has strong pseudorandom properties. In order to study connections of this type Mauduit and Sárközy [86] introduced the correlation and normality measures:

Definition 2.2. For a binary sequence $E_N = (e_1, \dots, e_N) \in \{-1,+1\}^N$ of length N and for $D = (d_1, \dots, d_\ell)$ with non-negative integers $0 \le d_1 < \cdots < d_\ell$, write

$$V(E_N, M, D) = \sum_{n=1}^{M} e_{n+d_1} \dots e_{n+d_\ell}\,.$$

Then the *correlation measure of order ℓ of E_N* is defined as

$$C_\ell(E_N) = \max_{M,D} \left| V(E_N, M, D) \right| = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} \dots e_{n+d_\ell} \right|,$$

where the maximum is taken over all $D = (d_1, \dots, d_\ell)$ and M such that $0 \le d_1 < \cdots < d_\ell < M + d_\ell \le N$.

Definition 2.3. For a binary sequence $E_N = (e_1, \dots, e_N) \in \{-1,+1\}^N$ of length N and for $X = (x_1, \dots, x_\ell) \in \{-1,+1\}^\ell$ write

$$T(E_N, M, X) = \left| \{n : 0 \le n < M,\ (e_{n+1}, e_{n+2}, \dots, e_{n+\ell}) = X\} \right|.$$

Then the *normality measure of order ℓ of E_N* is defined as

$$N_\ell(E_N) = \max_{M,X} \left| T(E_N, M, X) - M/2^\ell \right|,$$

where the maximum is taken over all $X = (x_1, \dots, x_\ell) \in \{-1,+1\}^\ell$, and M such that $0 < M \le N - \ell + 1$.

We remark that *infinite* analogs of the functions U, V and T have been studied before (see, for example, [19, 66] and [111]), but the quantitative analysis of pseudorandom properties of *finite* sequences started with the work of Mauduit and Sárközy [86].

The *combined* (well-distribution correlation) pseudorandom measure [86] is a common generalization of well-distribution and correlation measures. This measure has an important role in the multidimensional extension of the theory of pseudorandomness (see Section 9).

Definition 2.4. For a binary sequence $E_N = (e_1, \dots, e_N) \in \{-1, +1\}^N$ of length N and for $D = (d_1, \dots, d_\ell)$ with non-negative integers $0 \le d_1 < \dots < d_\ell$ write

$$Z(E_N, a, b, t, D) = \sum_{j=0}^{t} e_{a+jb+d_1} \dots e_{a+jb+d_\ell}.$$

Then the *combined (well-distribution correlation) measure of order ℓ of E_N* is defined as

$$Q_\ell(E_N) = \max_{a,b,t,D} \left| Z(E_N, a, b, t, D) \right| = \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} \dots e_{a+jb+d_\ell} \right|,$$

where the maximum is taken over all a, b, t and $D = (d_1, \dots, d_\ell)$ such that all the subscripts $a + jb + d_i$ belong to $\{1, 2, \dots, N\}$.

When introducing their quantitative pseudorandom measures, the starting point of Mauduit and Sárközy was to balance the requirements possibly optimally. They decided to introduce functions that are real-valued and positive, and the pseudorandom properties of the sequence are characterized by the sizes of the values of these functions. It was also an important requirement that one should be able to present constructions for which these measures can be estimated well. It turned out that the measures W and C_ℓ do not only satisfy these criteria, but later Rivat and Sárközy [118] showed that if the values of W and C_ℓ are "small", then the outcome of many (previously used a posteriori) statistical tests is guaranteed to be (nearly) positive.

Although by W, C_ℓ, N_ℓ and Q_ℓ many pseudorandom properties of the sequence can be characterized, obviously not all of them can. For example, in [45] the symmetry measure was introduced in order to study symmetry properties of finite binary sequences (later the symmetry measure was generalized by Sziklai [125]). In [135] Winterhof gave an excellent survey on different pseudorandom measures and certain constructions. This is a fast developing area and many papers have been published; there are too many to list all of them here. However, introducing more and more pseudorandom measures, can make it quite lengthy to handle all these measures. Thus it is important to determine a not too large set of certain basic pseudorandom measures, which can guarantee the adequate security in the applications. The present research shows that the measures described in this section satisfy these criteria. The most studied measures are W and C_ℓ, and many papers use only these measures.

In the next section we will show that for a *random-type* sequence (i.e. for a sequence with strong pseudorandom properties) the well-distribution and correlation measures are expected to be small.

3 Typical Values of Pseudorandom Measures

In [16] Cassaigne, Ferenczi, Mauduit, Rivat and Sárközy formulated the following principle: "The sequence E_N is considered a 'good' pseudorandom sequence if these

measures $W(E_N)$ and $C_\ell(E_N)$ (at least for 'small' ℓ) are 'small'." Indeed, the security of many cryptographic schemes is based on the property that the frequencies of the -1's and $+1$'s are about the same in certain "regular" subsequences of the used pseudorandom binary sequence $E_N \in \{-1,+1\}^N$.

In [18] Cassaigne, Mauduit and Sárközy proved that for the majority of the sequences $E_N \in \{-1,+1\}^N$ the measures $W(E_N)$ and $C_\ell(E_N)$ are around $N^{1/2}$ (up to some logarithmic factors). Later Alon, Kohayakawa, Mauduit, Moreira and Rödl [5] improved on these bounds:

Theorem 3.1. *Suppose that we choose each $E_N \in \{-1,+1\}^N$ with probability $1/2^N$. For all $\varepsilon > 0$ there exist $N_0 = N_0(\varepsilon)$ and $\delta = \delta(\varepsilon) > 0$ such that for $N > N_0$ we have*

$$P\left(\delta\sqrt{N} < W(E_N) < \tfrac{1}{\delta}\sqrt{N}\right) > 1-\varepsilon\,.$$

Theorem 3.2. *Suppose that we choose each $E_N \in \{-1,+1\}^N$ with probability $1/2^N$. Then for all $0 < \varepsilon < 1/16$ there is a constant $N_0 = N_0(\varepsilon)$ such that for $N > N_0$ we have*

$$P\left(\tfrac{2}{5}\sqrt{N\log\binom{N}{\ell}} < C_\ell(E_N) < \tfrac{7}{4}\sqrt{N\log\binom{N}{\ell}}\right) > 1-\varepsilon\,.$$

We remark that while it is important that for a binary sequence with strong pseudorandom properties these measures should be "small", lower bounds are not required (this will be justified by the results of Section 4, where the minimum values of these measures are studied). In many applications it is enough to guarantee that $W(E_N)$ and $C_\ell(E_N)$ are $o(N)$, but for the best constructions $E_N \in \{-1,+1\}^N$ *it is proved* that $W(E_N) \ll N^{1/2}\log N$, $C_\ell(E_N) \ll N^{1/2}(\log N)^{A_\ell}$ (see Section 6).

4 Minimum Values of Pseudorandom Measures

Write

$$m(N) = \min_{E_N\in\{-1,+1\}^N} W(E_N)\,, \qquad M_\ell(N) = \min_{E_N\in\{-1,+1\}^N} C_\ell(E_N)\,.$$

The estimate of $m(N)$ is a classical problem. In 1964 Roth [119] proved that $m(N) \gg N^{1/4}$. Upper bounds for $m(N)$ were given by Sárközy [32] and Beck [9]. Finally Matoušek and Spencer [78] showed that $m(N) \ll N^{1/4}$.

The value of $M_\ell(N)$ depends on the value of the order ℓ. Cassaigne, Mauduit and Sárközy [18] proved that $M_\ell(E_N) \ll (\ell N\log N)^{1/2}$. The results of [5] improved the implied constant factor (see Theorem 3.2 in the previous section). On the other hand, first Cassaigne, Mauduit and Sárközy [18] proved that $M_\ell(N) \gg \log(N/\ell)$ for even ℓ. This was improved considerably by Alon, Kohayakawa, Mauduit, Moreira and Rödl in [4] and [67], where the best lower bound is the following:

Theorem 4.1. *If ℓ is even then*

$$M_\ell(N) \geq \sqrt{\frac{1}{2}\left[\frac{N}{\ell+1}\right]}.$$

The proof of the theorem used deep linear algebraic tools, and later Anantharam [7] simplified the proof, but he obtained a slightly (by a constant factor) weaker result.

Cassaigne, Mauduit and Sárközy [18] noticed that the minimum values of correlation of odd order can be very small. Namely, for the sequence $E_N = (-1, +1, -1, +1, \ldots) \in \{-1, +1\}^N$ we have $C_\ell(E_N) = 1$ for odd ℓ, since

$$e_{n+1+d_1} \cdots e_{n+1+d_\ell} = (-e_{n+d_1}) \cdots (-e_{n+d_\ell}) = (-1)^\ell e_{n+d_1} \cdots e_{n+d_\ell}.$$

Thus

$$\left| \sum_{n=1}^{M} e_{n+d_1} \cdots e_{n+d_\ell} \right| = |1 - 1 + 1 - 1 + \cdots| = \begin{cases} 1 & \text{if } M \text{ is odd,} \\ 0 & \text{if } M \text{ is even.} \end{cases}$$

So $C_\ell(E_N) = 1$ and thus $M_\ell(N) = 1$ for odd ℓ. Cassaigne, Mauduit and Sárközy [18] also observed that although for the sequence $E_N = (-1, +1, -1, +1, \ldots)$, $C_3(E_N)$ is 1, the correlation measure of order 2 is large: $C_2(E_N) = \lceil \frac{N}{2} \rceil$. By solving problems of Cassaigne, Mauduit and Sárközy [18] and Mauduit [79], in [48] I proved that $C_2(E_N)C_3(E_N) \gg N^{2/3}$ always holds. Later Anantharam [8] proved that $C_2(E_N)C_3(E_N) \gg N$. By the methods of the proofs it is possible to compare correlation measures of odd and even order. With Mauduit we proved the following sharp result in [51]:

Theorem 4.2. *There is a constant $c_{k,\ell}$ depending only on k and ℓ such that if*

$$C_{2k+1}(E_N) < c_{k,\ell} N^{1/2},$$

then

$$C_{2k+1}(E_N)^{2\ell} C_{2\ell}(E_N)^{2k+1} \gg N^{2k+1},$$

where the implied constant factor depends only on k and ℓ.

This theorem has the following consequences:

Corollary 4.3. *If $C_{2k+1}(E_N) = O(1)$, then $C_{2\ell}(E_N) \gg N$, where the implied constant factor depends on k and ℓ.*

Corollary 4.4.

$$C_{2k+1}(E_N)C_{2\ell}(E_N) \gg N^{c(k,\ell)}$$

where the implied constant factor depends only on k and ℓ and where

$$c(k,\ell) = \begin{cases} 1 & \text{if } k \geq \ell, \\ \frac{1}{2} + \frac{2k+1}{4\ell} & \text{if } k < \ell. \end{cases}$$

The minimum of the normality measure was studied in [4] and [67], but there is a huge gap between the lower and upper bounds.

5 Connection between Pseudorandom Measures

It is a problem of basic importance to study the connections between the different pseudorandom measures. For example, Mauduit and Sárközy [86] proved that the normality measure can be bounded by the maximum of correlation measures:

Theorem 5.1.

$$N_\ell(E_N) \le \max_{1\le t\le \ell} C_t(E_N)\,.$$

Since the normality measures can be estimated by the correlation measures, most of the papers do not handle the normality measures separately, just they give non-trivial upper bounds for the well-distribution and correlation measures.

Cassaigne, Mauduit and Sárközy [18] compared correlation measures of different orders:

Theorem 5.2. *Suppose that* $2 \le k \mid \ell$ *and* $E_N \in \{-1,+1\}^N$. *Then*

$$C_k(E_N) \ll N^{1-k/\ell}\left(C_\ell(E_N)\right)^{k/\ell}\,.$$

If $k \nmid \ell$, it is possible to construct a sequence E_N for which $C_k(E_N)$ is large but $C_\ell(E_N)$ is small:

Theorem 5.3. *Suppose that* $2 \le k, \ell$ *and* $k \nmid \ell$. *Then there is a sequence* $E_N \in \{-1,+1\}^N$ *for which*

$$C_k(E_N) > \frac{N}{k} - 1 - 54k^2 \log N\,,$$
$$C_\ell(E_N) < 27k^2\ell N^{1/2}\log N\,.$$

Indeed in [18], Theorem 5.2 and Theorem 5.3 were proved in a sharper form.

The well-distribution measure can be estimated by the correlation measures of even order. In [92] Mauduit and Sárközy proved that for all sequences $E_N \in \{-1,+1\}^N$ we have

$$W(E_N) \le \sqrt{NC_2(E_N)}\,.$$

Later in [42] and [44] this inequality was generalized by me to correlation measures of any even order.:

Theorem 5.4. *For all sequences* $E_N \in \{-1,+1\}^N$ *we have*

$$W(E_N) \ll N^{1-1/(2\ell)}\left(C_{2\ell}(E_N)\right)^{1/(2\ell)}\,. \tag{5.1}$$

In [42] I also proved that (5.1) is sharp apart from the implied constant factor.

6 Constructions

First Mauduit and Sárközy [86] studied the well-distribution and correlation measures of a finite binary sequence. Their construction was the following:

Construction 6.1. *Let p be a prime number, $N = p - 1$ and define the Legendre-sequence $E_N = (e_1, e_2, \dots, e_N) \in \{-1, +1\}^N$ by*

$$e_n = \left(\frac{n}{p}\right),$$

where $(\frac{\cdot}{p})$ denotes the Legendre symbol.

Then by Theorem 1 in [86] for the sequence E_N defined in Construction 6.1 we have

$$W(E_N) \ll N^{1/2} \log N \quad \text{and} \quad C_\ell(E_N) \ll N^{1/2} \log N .$$

After their first paper [86] on pseudorandomness, Mauduit and Sárközy continued with a series of papers ([16–18, 87–89]) in which they tested several constructions. Since then numerous constructions have been given, see, for example, [21, 23, 26, 28, 29, 36, 41, 71–73, 75, 82, 109, 112, 113, 116, 121]. We remark that the majority of these constructions are of modular type. It would be interesting to give a construction which is not of modular type, but (nearly) optimal bounds can be proved for its pseudorandom measures.

First for fixed N most constructions produced only a single sequence of length N; however, in many applications one needs many pseudorandom binary sequences. In 2004 Goubin, Mauduit and Sárközy [40] succeeded in constructing large families of pseudorandom binary sequences based on the Legendre symbol. Their construction was the following:

Construction 6.2. *Let $K \in \mathbb{N}$, p be a prime number and denote by $\mathcal{P}$ the set of polynomials $f(x) \in \mathbb{F}_p[x]$ of degree k, where $0 < k \le K$ and which have no multiple zero in $\overline{\mathbb{F}}_p$ (=the algebraic closure of $\mathbb{F}_p$). For $f \in \mathcal{P}$ define the binary sequence $E_p(f) = (e_1, \dots, e_p)$ by*

$$e_n = \begin{cases} \left(\frac{f(n)}{p}\right) & \text{for } (f(n), p) = 1 , \\ +1 & \text{for } p \mid f(n) . \end{cases} \tag{6.1}$$

Let $\mathcal{F} = \{E_p(f) : f \in \mathcal{P}\}$.

Clearly $\mathcal{F}$ is a large family of pseudorandom binary sequences. Goubin, Mauduit and Sárközy [40] proved that, under some not too restrictive conditions on the polynomials f, the sequences $E_p(f)$ have strong pseudorandom properties:

Theorem 6.3. *Let p, $\mathcal{P}$ and $\mathcal{F}$ be defined as in Construction 6.2 and for $f \in \mathcal{P}$ define $E_p = E_p(f) \in \mathcal{F}$ by (6.1). Let k be the degree of f. Then*

$$W(E_p) \ll k p^{1/2} \log p .$$

Moreover, assume that for $\ell \in \mathbb{N}$ one of the following assumptions holds:
(i) $\ell = 2$;
(ii) $\ell < p$ *and 2 is a primitive root modulo* p;
(iii) $(4k)^{\ell} < p$.
Then we also have

$$C_{\ell}(E_p) \ll k\ell p^{1/2} \log p \, .$$

We remark that several important a posteriori tests (indicated by the 1.4-sts. package of the National Institute of Standards and Technology) were checked by Rivat and Sárközy [118] by computer for many sequences generated by Construction 6.2. In each case they obtained that the sequence passes all these tests.

The next construction was based on the discrete logarithm [43]:

Construction 6.4. *Let $K \in \mathbb{N}$, p be an odd prime number, and denote by $\mathcal{P}'$ the set of polynomials $f(x) \in \mathbb{F}_p[x]$ of degree k, where $0 < k \le K$. Let g be a primitive root modulo p and define* $\operatorname{ind} n$ *by* $n \equiv g^{\operatorname{ind} n} \pmod{p}$ *and* $1 \le \operatorname{ind} n \le p-1$. *For $f \in \mathcal{P}'$ define the binary sequence $E_{p-1}(f) = (e_1, \dots, e_{p-1})$ by*

$$e_n = \begin{cases} +1 & \text{if } 1 \le \operatorname{ind} f(n) \le (p-1)/2 \\ -1 & \text{if } (p+1)/2 \le \operatorname{ind} f(n) \le p-1 \text{ or } p \mid f(n) \, . \end{cases}$$

Let $\mathcal{F}' = \{E_p(f) : f \in \mathcal{P}'\}$.

This construction is nearly as good as Construction 6.2, the only problem is that it is slow to compute e_n, since no fast algorithm is known to compute $\operatorname{ind} n$. In [44] this construction was slightly modified such that the sequences in the new construction can be generated faster. Since then many other constructions of large families of pseudorandom sequences have been given (see, for example, [22, 24, 34, 35, 40, 43, 44, 59, 69, 74, 81, 84, 96–98, 117, 123, 127]).

Most constructions use finite fields and character sums over it (see the survey paper [127] for the most frequently used character sum estimates). One of the main tools in estimating the pseudorandom measures is Weil's theorem [133]:

Lemma 6.5. *Suppose that $\mathbb{F}_q$ is a finite field, χ is a non-principal character of order d over it, $f \in \mathbb{F}_q[x]$ has s distinct roots in $\overline{\mathbb{F}}_q$ and it is not a constant multiple of the d-th power of a polynomial over $\mathbb{F}_q$. Then:*

$$\left| \sum_{n \in \mathbb{F}_q} \chi(f(n)) \right| \le (s-1)p^{1/2} \, .$$

More precisely, the proofs of Theorem 6.3 and several other theorems (involving estimates of pseudorandom measures of different modular type constructions) are based on incomplete sums of multiplicative and additive characters. Such results can be derived from Weil's theorems on complete character sums (see, e.g. Lemma 6.5) by using a method of Vinogradov [131] (see also [64, 114, 126]).

Although many constructions exist, Construction 6.2 is one of the best: we have optimally good bounds for the pseudorandom measures and the elements of the sequences can be generated fast. In the next section we will analyze structural properties of large families of pseudorandom binary sequences.

7 Family Measures

In many applications it is not enough if our family $\mathcal{F}$ is large. For example, if $\mathcal{F}$ contains many sequences but they differ only in the last few bits, then one cannot use more than one sequence from the family. So it is very important to guarantee that the family $\mathcal{F}$ has a "rich", "complex" structure, there are many "independent" sequences in it which are "far apart." Thus one needs quantitative measures to study the structural properties of families of binary sequences. The first family measure was introduced by Ahlswede, Khachatrian, Mauduit and Sárközy in [1]:

Definition 7.1. Suppose that $\mathcal{F}$ is a family of binary sequences $E_N = (e_1, e_2, \ldots, e_N) \in \{-1, +1\}^N$ and $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_j) \in \{-1, +1\}^j$ is a fixed binary sequence of length j (for some $j \le N$), and let $1 \le i_1 < i_2 < \cdots < i_j \le N$. If we consider binary sequences $E_N = (e_1, e_2, \ldots, e_N) \in \{-1, +1\}^N$ with

$$e_{i_1} = \varepsilon_1\,, \quad e_{i_2} = \varepsilon_2\,, \quad \ldots\,, \quad e_{i_j} = \varepsilon_j\,, \tag{7.1}$$

then (7.1) is said to be a *specification of length* j (of the binary sequence E_N).

Definition 7.2. The *family complexity* or briefly f*-complexity* of a family $\mathcal{F}$ of binary sequences $E_N \in \{-1, +1\}^N$ is defined as the greatest integer j such that for any specification (7.1) (of length j) there is at least one $E_N \in \mathcal{F}$ which satisfies it. The f-complexity of $\mathcal{F}$ is denoted by $\Gamma(\mathcal{F})$. (If there is no $j \in \mathbb{N}$ with the property above, we set $\Gamma(\mathcal{F}) = 0$.)

Note that an easy consequence of the definition is

Proposition 7.3.

$$\Gamma(\mathcal{F}) \le \frac{\log |\mathcal{F}|}{\log 2}\,. \tag{7.2}$$

Ahlswede, Khachatrian, Mauduit and Sárközy [1] showed that for the family $\mathcal{F}$ defined in Construction 6.2, the f-complexity $\Gamma(\mathcal{F})$ is large. Later Gyarmati [47] improved on their lower bound by showing that $\Gamma(\mathcal{F}) > c \log |\mathcal{F}|$ with some explicit constant c; we note that by (7.2), this estimate is best possible apart from the value of this constant c, and thus the f-complexity of this family is optimally large (apart from the constant factor). Since then the family complexity of many other constructions were also studied by several authors. In [85] Mauduit and Sárközy gave a survey paper on family complexity.

Another important tool for studying the pseudorandomness of families of binary sequences is the notion of *collision* (see, for example, [10, 95, 129, 130]):

Assuming that $N \in \mathbb{N}$, S is a given set (e.g. a set of certain polynomials or the set of all the binary sequences of a given length much less than N), to each $s \in S$ we assign a unique binary sequence

$$E_N = E_N(s) = (e_1, \dots, e_N) \in \{-1, +1\}^N ,$$

and let $\mathcal{F} = \mathcal{F}(S)$ denote the family of the binary sequences obtained in this way:

$$\mathcal{F} = \mathcal{F}(S) = \{E_N(s) : s \in S\} . \tag{7.3}$$

Definition 7.4. If $s \in S$, $s' \in S$, $s \neq s'$ and

$$E_N(s) = E_N(s') , \tag{7.4}$$

then (7.4) is said to be a *collision* in $\mathcal{F} = \mathcal{F}(S)$. If there is no collision in $\mathcal{F} = \mathcal{F}(S)$, then $\mathcal{F}$ is said to be *collision free*.

In other words, $\mathcal{F} = \mathcal{F}(S)$ is collision free if we have $|\mathcal{F}| = |S|$. It turns out that in the best constructions, the families of pseudorandom binary sequences are collision free. If $\mathcal{F}$ is not collision free but the number of collisions is "small", then they may cause only minor problems in the applications. A good measure of the number of collisions is the following:

Definition 7.5. The *collision maximum* $M = M(\mathcal{F}, S)$ is defined by

$$M = M(\mathcal{F}, S) = \max_{E_N \in \mathcal{F}} |\{s : s \in S, E_N(s) = E_N\}|$$

(i.e. M is the maximal number of elements of S representing the same binary sequence E_N, and $\mathcal{F} = \mathcal{F}(S)$ is collision free if and only if $M(\mathcal{F}, S) = 1$).

Another important family requirement is the avalanche effect (see, e.g. [10, 33, 65, 129, 130]) which studies that by changing a few bits of the *seed* how many elements of the output sequence will change.

Definition 7.6. If in (7.3) we have $S = \{-1, +1\}^\ell$, and for any $s \in S$, changing any element of s changes "many" elements of $E_N(s)$ (i.e. for $s \neq s'$ many elements of the sequences $E_N(s)$ and $E_N(s')$ are different), then we speak about an *avalanche effect*, and we say that $\mathcal{F} = \mathcal{F}(S)$ *possesses the avalanche property*. If $N \to \infty$ and for any $s \in S$, $s' \in S$, $s \neq s'$ at least $(\frac{1}{2} - o(1))N$ elements of $E_N(s)$ and $E_N(s')$ are different, then $\mathcal{F}$ is said to *possess the strict avalanche property*.

To study the avalanche property, one may introduce the following quantitative measure:

Definition 7.7. If $N \in \mathbb{N}$, $E_N = (e_1, \dots, e_N) \in \{-1, +1\}^N$ and $E'_N = (e'_1, \dots, e'_N) \in \{-1, +1\}^N \in \{-1, +1\}^N$, then the *distance* $d(E_N, E'_N)$ between E_N and E'_N is defined by

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

(a similar notion is introduced in [10]; this is a variant of the Hamming distance). Moreover, if $\mathcal{F}$ is a family of the form (7.3), then the *distance minimum* $m(\mathcal{F})$ of $\mathcal{F}$ is defined by

$$m(\mathcal{F}) = \min_{\substack{s,s' \in S \\ s \ne s'}} d(E_N(s), E_N(s'))\,.$$

Thus the family $\mathcal{F}$ in (7.3) is collision free if and only if $m(\mathcal{F}) > 0$, and $\mathcal{F}$ possesses the strict avalanche property if

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

In [129] Tóth studied the Legendre symbol construction described in Construction 6.2 and she showed that a variant of the family defined there (she replaced the condition $\deg f(x) \le K$ by $\deg f(x) = K$) is collision free if $K < p^{1/2}/2$ and it possesses the strong avalanche effect for $p \to \infty$, $K = o(p^{1/2})$. In [130] she also studied a further construction using additive characters and she showed that there are many collisions in it, but a large subfamily of it possesses the strong avalanche property.

8 Linear Complexity

Cryptographic applications require pseudorandom sequences which are "unpredictable" in a certain sense. Kolmogorov [68] and Chaitin [20] introduced the notion of Kolmogorov complexity, which is roughly speaking the length of the shortest computer program which generates the given sequence in a fixed Turing machine. From this point of view, a sequence can be considered a bad pseudorandom sequence if its Kolmogorov complexity is "small". Unfortunately, in practice, it is usually hopeless to compute the Kolmogorov complexity for a fixed sequence, thus this definition cannot be used in the applications. In this section we analyze a related measure, linear complexity, which is a computable measure. Mainly we will study the connection between linear complexity and other pseudorandom measures.

Feedback shift registers, in particular linear feedback shift registers are used in many cryptographic stream ciphers (see, e.g. [95]). The linear feedback shift registers (LFSR) have many equivalent definitions, here I use one from [132]:

Definition 8.1. The *linear feedback shift register* is a sequence of 0–1 bits $(s_1, s_2, \dots, s_\ell, c_1, \dots, c_\ell)$ with $c_1 = 1$. The output of the LFSR is the infinite sequence $(s_1, s_2, \dots)$

where $s_i (\in \{0,1\})$ for $i > \ell$ is defined by the following equation:

$$s_i = \sum_{j=1}^{\ell} c_j s_{i-\ell-1+j} \pmod 2 .$$

An LFSR $L(s_1, s_2, \ldots, s_\ell, c_1, \ldots, c_\ell)$ is said to *generate* an infinite sequence $s = (s_1, s_2, \ldots)$ if s is the output sequence of $L(s_1, s_2, \ldots, s_\ell, c_1, \ldots, c_\ell)$. The *linear complexity* of an infinite sequence s, denoted by $L(s)$, is defined as follows:

(1) If s is the zero sequence $(0, 0, 0, \ldots)$, then $L(s) = 0$.
(2) If no LFSR generates s, then $L(s) = \infty$.
(3) Otherwise $L(s)$ is the length of the shortest LFSR that generates s.

For finite sequence $s \in \{0,1\}^N$, the linear complexity $L(s)$ is the length of the shortest LFSR that generates an infinite sequence whose first N bits form the finite sequence s.

The relationship between linear complexity and Kolmogorov complexity was studied in [13, 132]. The linear complexity is an important cryptographic characteristic of sequences (see the monographs and surveys [27, 93, 95, 102, 108, 128, 134]). An excellent historical survey on the linear complexity is given in [115]. Here I mention only some of the most important properties of the linear complexity: It is known [120] that the linear complexity of a truly random bit sequence $s = (s_1, s_2, \ldots, s_N) \in \{0,1\}^N$ is $(1 + o(1))\frac{N}{2}$. Based on this fact a sequence with low linear complexity is usually considered a "bad" pseudorandom sequence.

Using the Berlekamp–Massey algorithm (which is due to Massey [77] and based on an earlier algorithm of Berlekamp [12]), it is possible to calculate the value of the linear complexity of a fixed finite sequence. The linear complexity is usually defined for $0-1$ sequences (note that it can be defined similarly in the case of sequences of elements of $\mathbb{F}_q$ or $\mathbb{Z}_m$), but in this survey we study mostly ± 1 sequences. This problem can be easily avoided: there is a natural bijection $\varphi : \{-1,+1\}^N \to \{0,1\}^N$. Namely, if the sequence $E_N \in \{-1,+1\}^N$ is given, then $\varphi(E_N)$ can be defined by

$$\varphi(E_N) = \varphi((e_1, e_2, \ldots, e_N)) = S_N = (s_0, s_1, \ldots, s_{N-1}) \in \{0,1\}^N$$
$$\text{with } s_i = \frac{1 - e_{i+1}}{2} \text{ (or equivalently } (-1)^{s_i} = e_{i+1}) \text{ for } i = 0, 1, \ldots, N-1 .$$

Hence we may define the linear complexity of the binary sequence $E_N \in \{+1,-1\}^N$ by

$$L(E_N) = L(\varphi(E_N)) .$$

Brandstätter and Winterhof [14] showed that the linear complexity of a binary sequence E_N can be estimated in terms of the correlation measures of the sequence:

Theorem 8.2. *If $N \geq 2$ and E_N is a binary sequence then we have*

$$L(E_N) \geq N - \max_{1 \leq k \leq L(E_N)+1} C_k(E_N) .$$

Using this inequality they were able to give (in some cases quite strong) lower estimates for the linear complexity of binary sequences occurring in certain constructions. While this theorem may give quite good estimates for linear complexity, it has the disadvantage that it also uses correlations of high order which can be very difficult to estimate. Thus Andics [8] proved another inequality which uses the correlation of order 2 only (but it usually gives a weak lower bound):

Theorem 8.3. *If $N \in \mathbb{N}$ and E_N is a binary sequence then we have*

$$2^{L(E_N)} \geq N - C_2(E_N) .$$

Further results related to the pseudorandom measures and linear complexity can be found in several works (see, e.g. the papers of Winterhof and co-authors [6, 14, 15, 25, 37, 93, 94, 124, 128, 134]).

9 Multidimensional Theory

In the recent years, the one-dimensional theory of pseudorandomness has been extended to several dimensions. For example, when we would like to encrypt a digital map or image by the multidimensional analog of the Vernam cipher, then instead of a pseudorandom binary sequence we need a *two or more dimensional pseudorandom binary lattice* as a keystream. The multidimensional theory of pseudorandomness was developed by Hubert, Mauduit and Sárközy [62]. They introduced the following definitions:

Denote by I_N^n the set of n-dimensional vectors whose coordinates are integer numbers between 0 and $N-1$:

$$I_N^n = \{\mathbf{x} = (x_1, \dots, x_n) : x_1, \dots, x_n \in \{0, 1, \dots, N-1\}\} .$$

This set is called an *n-dimensional N-lattice* or briefly *N-lattice*. Next they extended this definition to more general lattices in the following way: Let $\mathbf{u_1}, \mathbf{u_2}, \dots, \mathbf{u_n}$ be n linearly independent vectors, where the i-th coordinate of $\mathbf{u_i}$ is a non-zero integer, and the other coordinates of $\mathbf{u_i}$ are 0, so $\mathbf{u_i}$ is of the form $(0, \dots, 0, z_i, 0, \dots, 0)$. Let $t_1, t_2, \dots, t_n$ be integers with $0 \leq t_1, t_2, \dots, t_n < N$. Then we will call the set

$$B_N^n = \{\mathbf{x} = x_1\mathbf{u_1} + \cdots + x_n\mathbf{u_n} : x_i \in \mathbb{N} \cup \{0\},\ 0 \leq x_i\,|\mathbf{u_i}| \leq t_i (< N) \text{ for } i = 1, \dots, n\}$$

an *n-dimensional box N-lattice* or briefly a *box N-lattice*.

In [62] the definition of binary sequences is extended to more dimensions by considering functions of type

$$e_{\mathbf{x}} = \eta(\mathbf{x}) : I_N^n \to \{-1, +1\} .$$

If $\mathbf{x} = (x_1, \dots, x_n)$ so that $\eta(\mathbf{x}) = \eta((x_1, \dots, x_n))$ then we will slightly simplify the notation by writing $\eta(\mathbf{x}) = \eta(x_1, \dots, x_n)$. These functions are called *bina-*

ry N-lattices or briefly *binary lattices*. One may visualize a binary lattice as the lattice points of the N-lattice replaced by the two symbols $+$ and $-$.

In [62] Hubert, Mauduit and Sárközy introduced the following pseudorandom measure of binary lattices (here we will present the definition in a slightly modified but equivalent form):

Definition 9.1. Let

$$\eta\colon I_N^n \to \{-1,+1\}$$

be a binary lattice. Define the *pseudorandom measure of order ℓ of η* by

$$Q_\ell(\eta) = \max_{B,\mathbf{d_1},\dots,\mathbf{d_k}} \left| \sum_{\mathbf{x}\in B} \eta(\mathbf{x}+\mathbf{d_1})\cdots\eta(\mathbf{x}+\mathbf{d}_\ell) \right|,$$

where the maximum is taken over all distinct $\mathbf{d_1},\dots,\mathbf{d}_\ell \in I_N^n$ and box N-lattice B such that $B+\mathbf{d_1},\dots,B+\mathbf{d}_\ell \subseteq I_N^n$.

Then η is said to have strong pseudorandom properties, or briefly, it is considered a "good" pseudorandom lattice if for fixed n and ℓ and "large" N the measure $Q_\ell(\eta)$ is "small" (much smaller than the trivial upper bound N^n). This terminology is justified by the fact that, as it was proved in [62], for a truly random binary lattice defined on I_N^n and for fixed ℓ the measure $Q_\ell(\eta)$ is "small" (less than $N^{n/2}$ multiplied by a logarithmic factor).

Recently several multidimensional constructions have been given for lattices with strong pseudorandom properties, see, for example, [52, 60–62, 70, 83, 91, 99, 100].

Some one-dimensional theorems can be generalized to the multidimensional case. For example, we studied the properties of the multidimensional pseudorandom measures in [53–58]. In particular, in [58] we compared the one-dimensional pseudorandom measures with the two or more dimensional pseudorandom measures and we showed that the study of the multidimensional measures cannot be reduced to one-dimensional ones, so indeed it was necessary to develop the multidimensional theory. In [55–57] we introduced the multidimensional analog of the normality, correlation and symmetry measures. We studied the connection between multidimensional pseudorandom measures of different orders and we proved the multidimensional analog of Theorem 5.1. We also studied the minimal values of the multidimensional pseudorandom measures. In [46] further multidimensional pseudorandom measures were introduced. In [53] and [54] the notions of family complexity, collision and avalanche effect were extended and studied in the multidimensional case.

10 Extensions

Pseudorandom binary sequences have many further generalizations. For example, Mauduit and Sárközy [90], Ahlswede, Mauduit and Sárközy [2, 3], Bérczi [11], Marzouk and Winterhof [76] and Mérai [101] studied the case of sequences of k symbols.

Hubert and Sárközy [63] studied the case of p-pseudorandom binary sequences, i.e. the case when the binary sequences simulate the binomial distribution of parameter p. Niederreiter, Rivat and Sárközy [110] studied pseudorandom sequences of binary vectors. In [30] and [31] Dartyge and Sárközy started to study pseudorandom subsets of $\{1, 2, \dots, N\}$ and $\mathbb{Z}_n$. In [49] and [50] we studied pseudorandom binary functions on rooted plane trees. The connection between pseudorandom binary and $[0, 1)$ sequences was analyzed in [80] by Mauduit, Niederreiter and Sárközy.

References

[1] R. Ahlswede, L. H. Khachatrian, C. Mauduit, and A. Sárközy, *A complexity measure for families of binary sequences*, Period. Math. Hungar. **46** (2003), 107–118.

[2] R. Ahlswede, C. Mauduit, and A. Sárközy, *Large families of pseudorandom sequences of k symbols and their complexity. I*, Lecture Notes in Comput. Sci. 4123, General theory of information transfer and combinatorics, pp. 293–307, Springer, Berlin, Heidelberg, 2006.

[3] R. Ahlswede, C. Mauduit, and A. Sárközy, *Large families of pseudorandom sequences of k symbols and their complexity. II*, Lecture Notes in Comput. Sci. 4123, General theory of information transfer and combinatorics, pp. 308–325, Springer, Berlin, Heidelberg, 2006.

[4] 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.

[5] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira, and V. Rödl, *Measures of pseudorandomness for finite sequences: typical values*, Proc. London Math. Soc. **95** (2007), 778–812.

[6] H. Aly and A. Winterhof, *On the k-error linear complexity over $\mathbb{F}_p$ of Legendre and Sidelnikov sequences*, Des. Codes Cryptogr. **40** (2006), 369–374.

[7] V. Anantharam, *A technique to study the correlation measures of binary sequences*, Discrete Math. **308(24)** (2008), 6203–6209.

[8] Á. Andics, *On the linear complexity of binary sequences*, Annales Univ. Sci. Budapest. **48** (2005), 173–180.

[9] J. Beck, *Roth's estimate on the discrepancy of integer sequences is nearly sharp*, Combinatorica **1** (1981), 319–325.

[10] A. Bérczes, J. Ködmön, and A. Pethő, *A one-way function based on norm form equations*, Period. Math. Hungar. **49** (2004), 1–13.

[11] G. Bérczi, *On finite pseudorandom sequences of k symbols*, Period. Math. Hungar. **47(1–2)** (2003), 29–44.

[12] E. R. Berlekamp, *Algebraic Coding Theory*, McGraw Hill, New York, 1968.

[13] T. Beth and Z. D. Dai, *On the complexity of pseudo-random sequences – or: if you can describe a sequence it can't be random*, Advances in Cryptology – EUROCRYPT '89 (Houthalen 1989), Lecture Notes in Computer Science 434, pp. 533–543, Springer, Berlin, 1990.

[14] N. Brandstätter and A. Winterhof, *Linear complexity profile of binary sequences with small correlation measure*, Period. Math. Hungar. **52** (2006), 1–8.

[15] N. Brandstätter and A. Winterhof, *k-error linear complexity over $\mathbb{F}_p$ of subsequences of Sidelnikov sequences of period $(p^r - 1)/3$*, J. Math. Cryptol. **3** (2009), 215–225.

[16] J. Cassaigne, S. Ferenczi, C. Mauduit, J. Rivat, and A. Sárközy, *On finite pseudorandom binary sequences III: The Liouville function, I*, Acta Arith. **87** (1999), 367–384.

[17] J. Cassaigne, S. Ferenczi, C. Mauduit, J. Rivat, and A. Sárközy, *On finite pseudorandom binary sequences. IV*, Acta Arith. **95**, 343–359 (2000).

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

[19] J. W. S. Cassels, *On a paper of Niven and Zuckerman*, Pacific J. Math. **2** (1952), 555–557.
[20] G. J. Chaitin, *On the length of programs for computing finite binary sequences*, J. Assoc. Comput. Mach. **13** (1966), 547–569.
[21] Z.-X. Chen, *Elliptic curve analogue of Legendre sequences*, Monatsh. Math. **154** (2008), 1–10.
[22] Z. X. Chen, X. N. Du, and G. Z. Xiao, *Sequences related to Legendre/Jacobi sequences*, Inform. Sci. **177** (2007), 4820–4831.
[23] Z. Chen and S. Li, *Some notes on generalized cyclotomic sequences of length* pq, J. Comput. Sci. Technology **23** (2008), 843–850.
[24] Z. Chen, S. Li and G. Xiao, *Construction of pseudorandom binary sequences from elliptic curves by using the discrete logarithms*, in: Sequences and their applications – SETA 2006, LNCS 4086, pp. 285–294, Springer, 2006.
[25] Z. Chen and A. Winterhof, *Linear complexity profile of* m*-ary pseudorandom sequences with small correlation measure* Indag. Math. (N. S.) **20(4)** (2009), 631–640.
[26] Z. Chen, Zhixiong, A. Ostafe, and A. Winterhof, *Structure of pseudorandom numbers derived from Fermat quotients*, Lecture Notes in Comput. Sci., 6087, Arithmetic of finite fields, pp. 73–85, Springer, Berlin, 2010.
[27] T. W. Cusick, C. Ding, and A. Renwall, *Stream Ciphers and Number Theory*, revised ed., North-Holland Mathematical Library 66, Elsevier Science B. V., Amsterdam, 2004.
[28] H. Daboussi, *On pseudorandom properties of multiplicative functions*, Acta Math. Hungar. **98** (2003), 273–300.
[29] H. Daboussi, *On the correlation of the truncated Liouville function*, Acta Arith. **108** (2003), 61–76.
[30] C. Dartyge and A. Sárközy, *On pseudo-random subsets of the set of the integers not exceeding N*, Period. Math. Hung. **54(2)** (2007), 183–200.
[31] C. Dartyge and A. Sárközy, *On pseudo-random subsets of* $\mathbb{Z}_n$, Monatsh. Math. **157(1)** (2009), 13–35.
[32] P. Erdős and A. Sárközy, *Some solved and unsolved problems in combinatorial number theory*, Math. Slovaca **28** (1978), 407–421 (p. 415).
[33] H. Feistel, W. A. Notz, and J. L. Smith, *Some cryptographic techniques for machine-to-machine data communications*, Proc. IEEE **63** (1975), 1545–1554.
[34] J. Folláth, *Construction of pseudorandom binary sequences using additive characters over* $GF(2^k)$, Period. Math. Hungar. **57** (2008), 73–81.
[35] J. Folláth, *Construction of pseudorandom binary sequences using additive characters over* $GF(2^k)$. *II*, Period. Math. Hungar. **60** (2010), 127–135.
[36] E. Fouvry, P. Michel, J. Rivat, and A. Sárközy, *On the pseudorandomness of the signs of Kloosterman sums*, J. Australian Math. Soc. **77** (2004), 425–436.
[37] M. Z. Garaev, F. Luca, Florian, I. E. Shparlinski, and A. Winterhof, *On the lower bound of the linear complexity over* $\mathbb{F}_p$ *of Sidelnikov sequences*, IEEE Trans. Inform. Theory **52(7)** (2006), 3299–3304.
[38] S. Goldwasser, *Mathematical Foundations of Modern Cryptography: Computational Complexity Perspective*, ICM 2002, vol. I, 245–272.
[39] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*, University Press, Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo, 2005.
[40] L. Goubin, C. Mauduit, and A. Sárközy, *Construction of large families of pseudorandom binary sequences*, J. Number Theory **106** (2004), 56–69.
[41] E. Grant, J. Shallit, and T. Stoll, *Bounds for the discrete correlation of infinite sequences on* k *symbols and generalized Rudin–Shapiro sequences*, Acta Arith. **140** (2009), 345–368.

[42] K. Gyarmati, *An inequality between the measures of pseudorandomness*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **46** (2003), 157–166.
[43] K. Gyarmati, *On a family of pseudorandom binary sequences*, Period. Math. Hungar. **49** (2004), 45–63.
[44] K. Gyarmati, *On a fast version of a pseudorandom generator*, Lecture Notes in Comput. Sci. 4123, General theory of information transfer and combinatorics, pp. 326–342, Springer, Berlin, Heidelberg, 2006.
[45] K. Gyarmati, *On a pseudorandom property of binary sequences*, Ramanujan J. **8** (2004), 289–302.
[46] K. Gyarmati, *On new measures of pseudorandomness of binary lattices*, Acta Math. Hung. **131** (2011), 346–359.
[47] K. Gyarmati, *On the complexity of a family related to the Legendre symbol*, Period. Math. Hungar. **58** (2009), 209–215.
[48] K. Gyarmati, *On the correlation of binary sequences*, Studia Sci. Math. Hungar. **42** (2005), 59–75.
[49] K. Gyarmati, P. Hubert, and A. Sárközy, *Pseudorandom binary functions on almost uniform trees*, J. Combin. Number Theory **2** (2010), 1–24.
[50] K. Gyarmati, P. Hubert, and A. Sárközy, *Pseudorandom binary functions on rooted plane trees*, J. Combin. Number Theory, to appear.
[51] K. Gyarmati and C. Mauduit, *On the correlation of binary sequences, II*, Discrete Math. **312** (2012), 811–818.
[52] K. Gyarmati, C. Mauduit, and A. Sárközy, *Constructions of pseudorandom binary lattices*, Uniform Distribution Theory **4** (2009), 59–80.
[53] K. Gyarmati, C. Mauduit, and A. Sárközy, *Measures of pseudorandomness of families of binary lattices, I (Definitions, a construction using quadratic characters.)*, Publ. Math. Debrecen **79** (2011), 445–460.
[54] K. Gyarmati, C. Mauduit, and A. Sárközy, *Measures of pseudorandomness of families of binary lattices, II (A further construction.)*, Publ. Math. Debrecen **80** (2012), 481–504.
[55] K. Gyarmati, C. Mauduit, and A. Sárközy, *Measures of pseudorandomness of finite binary lattices, I (The measures Q_k, normality.)*, Acta Arith. **144** (2010), 295–313.
[56] K. Gyarmati, C. Mauduit, and A. Sárközy, *Measures of pseudorandomness of finite binary lattices, II (The symmetry measures.)*, Ramanujan J. **25** (2011), 155–178.
[57] K. Gyarmati, C. Mauduit, and A. Sárközy, *Measures of pseudorandomness of finite binary lattices, III (Q_k, correlation, normality, minimal values.)*, Unif. Distrib. Theory **5** (2010), 183–207.
[58] K. Gyarmati, C. Mauduit, and A. Sárközy, *Pseudorandom binary sequences and lattices*, Acta Arith. **135(2)** (2008), 181–197.
[59] K. Gyarmati, A. Pethő, and A. Sárközy, *On linear recursion and pseudorandomness*, Acta Arith. **118** (2005), 359–374.
[60] K. Gyarmati, A. Sárközy, and C. L. Stewart, *On Legendre symbol lattices*, Uniform Distribution Theory **4** (2009), 81–95.
[61] K. Gyarmati, A. Sárközy, and C. L. Stewart, *On Legendre symbol lattices, II*, to appear.
[62] P. Hubert, C. Mauduit, and A. Sárközy, *On pseudorandom binary lattices*, Acta Arith. **125** (2006), 51–62.
[63] P. Hubert and A. Sárközy, *On p-pseudorandom binary sequences*, Period. Math. Hungar. **49** (2004), 73–91.
[64] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Colloquium Publications 53, American Mathematical Society, 2004.

[65] J. Kam and G. Davida, *Structured design of substitution-permutation encryption networks*, IEEE Transactions on Computers **28** (1979), 747–753.
[66] D. E. Knuth, *The Art of Computer Programming*, Vol. 2, 2nd ed., Addison-Wesley, Reading, Mass., 1981.
[67] Y. Kohayakawa, C. Mauduit, C. G. Moreira, and V. Rödl, *Measures of pseudorandomness for finite sequences: minimum and typical values*, Proceedings of WORDS'03, TUCS Gen. Publ. 27, Turku Cent. Comput. Sci., Turku, 2003, 159–169.
[68] A. N. Kolmogorov, *Three approaches to the definition of the concept "quantity of information"*, Problemy Inform. Transmission **1(1)** (1965), 3–7.
[69] H. N. Liu, *A family of pseudorandom binary sequences constructed by the multiplicative inverse*, Acta Arith. **130** (2007), 167–180.
[70] H. Liu, *A large family of pseudorandom binary lattices*, Proc. Amer. Math. Soc. **137** (2009), 793–803.
[71] H. Liu, *New pseudorandom sequences constructed by quadratic residues and Lehmer numbers*, Proc. Amer. Math. Soc. **135** (2007), 1309–1318.
[72] H. Liu, *New pseudorandom sequences constructed using multiplicative inverses*, Acta Arith. **125** (2006), 11–19.
[73] H. N. Liu and W. G. Zhai, *A note on the pseudorandomness of the Liouville function*, Acta Arith. **136** (2009), 101–121.
[74] H. N. Liu, T. Zhan, and X. Y. Wang, *On the correlation of pseudorandom binary sequences with composite moduli*, Publ. Math. Debrecen **74** (2009), 195–214.
[75] S. Louboutin, J. Rivat, and A. Sárközy, *On a problem of D. H. Lehmer*, Proc. Amer. Math. Soc. **135** (2007), 969–975.
[76] R. Marzouk and A. Winterhof, *On the pseudorandomness of binary and quaternary sequences linked by the Gray mapping*, Period. Math. Hungar. **60** (2010), 13–23.
[77] J. L. Massey, *Shift register synthesis and BCH decoding*, IEEE Transactions on Information Theory **15** (1969), 122–127.
[78] J. Matoušek and J. Spencer, *Discrepancy in arithmetic progressions*, J. Amer. Math. Soc. **9** (1996), 195–204.
[79] C. Mauduit, *Construction of pseudorandom finite sequences*, unpublished lecture notes to the conference, Information Theory, and Some Friendly Neighbours – ein Wunschkonzert, Bielefeld, 2003.
[80] C. Mauduit, H. Niederreiter, and A. Sárközy, *On pseudorandom* $[0, 1)$ *and binary sequences*, Publ. Math. Debrecen **71** (2007), 305–327.
[81] C. Mauduit, J. Rivat, and A. Sárközy, *Construction of pseudorandom binary sequences using additive characters*, Monatsh. Math. **141** (2004), 197–208.
[82] C. Mauduit, J. Rivat, and A. Sárközy, *On the pseudo-random properties of* n^c, Illinois J. Math. **46** (2002), 185–197.
[83] C. Mauduit, and A. Sárközy, *Construction of pseudorandom binary lattices by using the multiplicative inverse*, Monatsh. Math. **153** (2008), 217–231.
[84] C. Mauduit and A. Sárközy, *Construction of pseudorandom binary sequences by using the multiplicative inverse*, Acta Math. Hungar. **108** (2005), 239–252.
[85] C. Mauduit and A. Sárközy, *Family Complexity and VC-dimension*, Lecture Notes in Computer Science, Springer, to appear.
[86] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences I: Measures of pseudorandomness, the Legendre symbol*, Acta Arith. **82** (1997), 365–377.
[87] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences. II: The Champernowne, Rudin–Shapiro, and Thue–Morse sequences, a further construction*, J. Number Theory **73(2)** (1998), 256–276.

[88] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences. V: On $(n\alpha)$ and $(n^2\alpha)$ sequences*, Monatsh. Math. **129(3)** (2000), 197–216.
[89] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences. VI: On $(n^k\alpha)$ sequences*, Monatsh. Math. **130(4)** (2000), 281–298.
[90] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences of k symbols*, Indag. Math **13** (2002), 89–101.
[91] C. Mauduit and A. Sárközy, *On large families of pseudorandom binary lattices*, J. Uniform Distribution Theory **2** (2007), 23–37.
[92] C. Mauduit and A. Sárközy, *On the measures of pseudorandomness of binary sequences*, Discrete Math. **271** (2003), 195–207.
[93] W. Meidl and A. Winterhof, *Linear complexity of sequences and multisequences*, in: G. Mullen, D. Panario (eds.), Handbook of Finite Fields, Boca Raton, London, New York, CRC Press, to appear.
[94] W. Meidl and A. Winterhof, *Some notes on the linear complexity of Sidel'nikov–Lempel–Cohn-Eastman sequences*, Des. Codes Cryptogr. **38(2)** (2006), 159–178.
[95] A. Menezes, P. C. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRS Press, Boca Raton, 1997.
[96] L. Mérai, *A construction of pseudorandom binary sequences using both additive and multiplicative characters*, Acta Arith. **139** (2009), 241–252.
[97] L. Mérai, *A construction of pseudorandom binary sequences using rational functions*, Unif. Distrib. Theory **4** (2009), 35–49.
[98] L. Mérai, *Construction of large families of pseudorandom binary sequences*, Ramanujan J. **18** (2009), 341–349.
[99] L. Mérai, *Construction of pseudorandom binary lattices based on multiplicative characters*, Period. Math. Hungar. **59** (2009), 43–51.
[100] L. Mérai, *Construction of pseudorandom binary lattices using elliptic curves*, Proc. Amer. Math. Soc. **139** (2011), 407–420.
[101] L. Mérai, *On finite pseudorandom lattices of k symbols*, Monatsh. Math. **161(2)** (2010), 173–191.
[102] H. Niederreiter, *Linear complexity and related complexity measures for sequences*, Progress in Cryptology – INDOCRYPT 2003, Lecture Notes in Computer Science, Vol. 2904, pp. 1–17, Springer, Berlin, 2003.
[103] H. Niederreiter, *On the distribution of pseudo-random numbers generated by the linear congruential method.*, Math. Comp. **26** (1972), 793–795.
[104] H. Niederreiter, *On the distribution of pseudo-random numbers generated by the linear congruential method. II*, Math. Comp. **28** (1974), 1117–1132.
[105] H. Niederreiter, *On the distribution of pseudo-random numbers generated by the linear congruential method. III*, Math. Comp. **30** (1976), 571–597.
[106] H. Niederreiter, *Quasi-Monte Carlo methods and pseudorandom numbers*, Bull. Amer. Math. Soc. **84** (1978), 957–1041.
[107] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, CBMS-NSF Regional Conference Series in Applied Math., Vol. 63, Soc. Industr. Applied Math., Philadelphia, 1992.
[108] H. Niederreiter, *Some computable complexity measures for binary sequences*, Sequences and their Applications, Singapore, 1998, Springer Ser. Discrete Math. Theor. Comput. Sci., pp. 67–78, Springer, London, 1999.
[109] H. Niederreiter and J. Rivat, *On the correlation of pseudorandom numbers generated by inversive methods*, Monatsh. Math. **153** (2008), 251–264.

[110] H. Niederreiter, J. Rivat, and A. Sárközy, *Pseudorandom sequences of binary vectors*, Acta Arith. **133(2)** (2008), 109–125.
[111] I. Niven and H. S. Zuckerman, *On the definition of normal numbers*, Pacific J. Math. **1** (1951), 103–109.
[112] S.-M. Oon, *On pseudo-random properties of some Dirichlet characters*, Ramanujan J. **15** (2008), 19–30.
[113] S.-M. Oon, *Pseudorandom properties of prime factors*, Period. Math. Hungar. **49** (2004), 107–118.
[114] A. Ostafe and A. Winterhof, *Some applications of character sums*, in: G. Mullen and D. Panario (eds.), Handbook of Finite Fields, Boca Raton, London, New York, CRC Press, to appear.
[115] T. Ritter, *Linear Complexity: A Literature Survey*, http://www.ciphersbyritter.com/RES/LINCOMPL.HTM.
[116] J. Rivat, *On pseudo-random properties of* $P(n)$ *and* $P(n+1)$, Period. Math. Hungar. **43** (2001), 121–136.
[117] J. Rivat and A. Sárközy, *Modular constructions of pseudorandom binary sequences with composite moduli*, Period. Math. Hungar. **51** (2005), 75–107.
[118] J. Rivat and A. Sárközy, *On pseudorandom sequences and their application*, Lecture Notes in Comput. Sci. 4123, General theory of information transfer and combinatorics, pp. 343–361, Springer, Berlin, Heidelberg, 2006.
[119] K. F. Roth, *Remark concerning integer sequences*, Acta Arith. **9** (1964), 257–260.
[120] R. A. Rueppel, *Linear complexity and Random Sequences*, Proc. Advances in Cryptology – EUROCRYPT '85, Linz, Austria, April 9–12, 1985, LNCS 219, pp. 167–188.
[121] A. Sárközy, *A finite pseudorandom binary sequence*, Studia Sci. Math. Hungar. **38** (2001), 377–384.
[122] A. Sárközy, *On finite pseudorandom binary sequences and their applications in cryptography*, Tatra Mt. Math. Publ. **37** (2007), 123–136.
[123] A. Sárközy and C. L. Stewart, *On pseudorandomness in families of sequences derived from the Legendre symbol*, Period. Math. Hungar. **54** (2007), 163–173.
[124] I. E. Shparlinski and A. Winterhof, *On the discrepancy and linear complexity of some counter-dependent recurrence sequences*, Lecture Notes in Comput. Sci., 4086, pp. 295–303, Springer, Berlin, 2006 Sequences and their applications – SETA 2006.
[125] B. Sziklai, *On the symmetry of finite pseudorandom binary sequences*, Uniform Distribution Theory **6** (2011), 143–156.
[126] A. Tietäväinen, *Vinogradov's method and some applications*, in: C. Yildirim and S. A. Stepanov (eds.), Number theory and its applications, Lecture Notes in Pure and Applied Math., Vol. 204, Dekker, New York, 1998, 261–282.
[127] A. Topuzoğlu and A. Winterhof, *Pseudorandom numbers: Uniform distribution and exponential sums*, in: S. Boztas (ed.), CRC Handbook of Sequences, Codes, and Applications: Chapman and Hall/CRC Press, to appear.
[128] A. Topuzoğlu and A. Winterhof, *Pseudorandom sequences*, in: G. Mullen and D. Panario (eds.), Handbook of Finite Fields, Boca Raton, London, New York, CRC Press, to appear.
[129] V. Tóth, *Collision and avalanche effect in families of pseudorandom binary sequences*, Period. Math. Hungar. **55** (2007), 185–196.
[130] V. Tóth, *The study of collision and avalanche effect in a family of pseudorandom binary sequences*, Period. Math. Hungar. **59** (2009), 1–8.
[131] I. M. Vinogradov, *Elements of Number Theory*, Dover 1954.
[132] Y. Wang, *Linear Complexity versus Pseudorandomness: On Beth and Dai's result*, Advances in Cryptology – ASIACRYPT'99 (Singapore), Lecture Notes in Computer Science, Vol. 1716, pp. 288–298, Springer, Berlin, 1999.

[133] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Act. Sci. Ind. 1041, Hermann, Paris, 1948.
[134] A. Winterhof, *Linear complexity and related complexity measures*, in: I. Woungang, S Misra, and S. C. Misra (eds.), Selected Topics in Information and Coding Theory, Vol. 7, Singapore: World Scientific, 2010, 3–40.
[135] A. Winterhof, *Measures of pseudorandomness*, in: S. Boztas, (ed.), CRC Handbook of Sequences, Codes and Applications: Chapman and Hall/CRC Press, to appear.