Tatra Mt. Math. Publ. **37** (2007), 123–136

TATRA MOUNTAINS *Mathematical Publications*

ON FINITE PSEUDORANDOM BINARY SEQUENCES AND THEIR APPLICATIONS IN CRYPTOGRAPHY

András Sárközy

ABSTRACT. Finite pseudorandom binary sequences play a crucial role in cryptography. The pseudorandomness is usually characterized in terms of complexity theory. First the limitations of this approach will be analyzed. Then another, more constructive approach developed in the last decade by Mauduit, Sárközy and others will be described. Finally, constructions of large families of binary sequences with strong pseudorandom properties will be presented.

1. Introduction

Finite pseudorandom (=PR) binary sequences have many applications and, in particular, they play a role of basic importance in cryptography. The notion of pseudorandomness is usually interpreted in terms of *computational complexity*; an excellent survey of this approach was given by Goldwasser in [19]. However, this computational complexity approach has certain weak points which have been criticized recently widely. Thus in the last decade an other, more *constructive* approach has been developed. In this paper *my goal is to give a survey of this new approach.* To help to understand the underlying ideas better, first in this section I will give a short sketch of the computational complexity approach and its weak points.

The most important applications of finite PR binary sequences in cryptography are related to the classical stream cipher type encrypting algorithm called *Vernam cipher* which is the following: we consider the plaintext given in form of a bit sequence, then we take a bit sequence of identical length as key stream,

2000 Mathematics Subject Classification: 11K45.
Keywords: pseudorandom, binary sequence, correlation, complexity.
Research partially supported by Hungarian National Foundation for Scientific Research, Grant No. T043623.

and the encryption happens by bitwise modulo 2 addition (by "XORing") of the two bit sequences. If the bits of the key stream are generated independently and randomly, then the Vernam cipher is called a *one-time pad.* The bits of the key stream are usually generated by a physical device, however, the bit sequences obtained in this way must be tested by using statistical test (testing of this type is called "a posteriori testing" by Knuth [33]). As Menezes, van Oorschot and Vanstone write in their excellent monograph [44] (all the quotations in this paper will be taken from [44]):

"An obvious drawback of the one-time pad is that the key should be as long as the plaintext which increases the difficulty of key distribution and key management. This motivates the design of stream ciphers where *the key stream os pseudorandomly generated from a smaller secret key, with the intent that the keystream appears random to a computationally bounded adversary. Such stream ciphers do not offer unconditional security..., but the hope is that they are computationally secure". More precisely:*

Definition 1. A *pseudorandom bit generator* (=PRBG) is a deterministic *algorithm* which, given a truly random binary sequence of length k, outputs a binary sequence of length $1 \gg k$, which "appears" to be random. The input to the PRBG is called the *seed* (produced by, say, coin toss and passed the partner by public key cryptography) "while the output of the PRBG is called a *pseudorandom bit sequence*".

Thus for encrypting the plaintext we need *a "good" PRBG.* But *when is a PRBG good*? The usual answer to this question is formulated by using notions and tools of *computational complexity:*

Definition 2. A PRBG is said to *pass the next bit test* if there is no polynomial time algorithm which, on input of the first l bits of an output sequence S, can predict the $(l+1)^{st}$ bit of s with probability significantly greater than 1/2. (Briefly, we may call this requirement *unpredictability.*)

Definition 3. A PRGB that passes the next bit test (possibly *under some plausible but unproved mathematical assumption* such as the intractability of factoring integers) is called a *"cryptographically secure" PRBG.*

(Some of the most important "cryptographically secure" RGBG's are: the RSA [5], Blum-Blum-Shub [9] and Blum-Micali [10] PRBG's which are secure under the assumption that the factorization of integers, resp. computing the discrete logarithm is difficult.)

These definitions have several weakness:

1. In the practice one has to construct a PR sequence of a give length N; in the definitions above nothing is said on the dependence of the degree and

coefficients of the polynomial in the "polynomial time algorithm" on N, thus the definitions cannot be adopted to this situation, they are of asymptotic nature only.

2. What does it mean in Definition 2 that "probability significantly greater than 2"?

3. The non-existence of a polynomial time algorithm has never been shown *unconditionally* yet; thus there is no PRBG whose cryptographical security has been proved unconditionally. On the other hand, "plausible but unproved mathematical assumptions" can be disputed (even they may turn out to be wrong); e.g., the assumption on the "difficulty of factorization" used to be widely accepted but now, after the discovery of polynomial time primality testing, it becomes more and more disputed.

4. These definitions measure only *the quality of the PRBG's* but not that of *the output sequences* so that, even in case of "good" PRBG's one may get, e.g., an all zero output sequence. Thus to avoid the use of sequences which "are not of random type", one also needs "a posteriori" testing.

Based on all these facts, we may conclude that the notion of pseudorandomness needs a *new approach* which is more *constructive* than the one based on complexity theory, it does not use *unproved* assumptions, it studies pseudorandomness of *single sequences* instead of generators, and which also makes testing of *"a priori" type* possible. In the next sections we will present such a new approach.

2. A new, constructive approach

In case of *infinite* binary sequences there is a classical measure of pseudorandomness: *normality*, introduced by Borel [11] a century ago. In the *finite* case Golomb [20], then Knuth [33] made (not very satisfactory) attempts to define the pseudorandomness of (single) binary sequences. Then "Kolomogorov [35] and Chaitin [13] introduced the notion of so called Turning-Kolomogorov-Chaitin complexity...", however, "there is no algorithm known for computing *it and, hence, it has no apparent practical significance".*

The notion of *linear complexity* is more important: it measures an important PR property, and the linear complexity of *special* sequences can be computed by the so called Berlekamp-Massey algorithm. On the other hand, simple examples show that a sequence can have large linear complexity without being of random character. Moreover, it is difficult to compute the linear complexity of *general* sequences. Thus the linear complexity makes an important but far not satisfactory measure of pseudorandomness.

In 1997 Mauduit and I [39] introduced the following *new measures of pseudorandomness* of (single) finite binary sequences:

Let $E_N = (e_1, e_2, \dots, e_N) \in \{-1, +1\}^N$ be a finite binary sequence. (Clearly, instead of bit sequences we may study ± 1 sequences, and the latter case many formulas are simpler.) Then

Definition 4. The *well-distribution* measure of E_N is defined as

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

where the maximum is taken over all a, b, t with $a, b, t \in \mathbb{N}, a + (t-1)\, b \le N$. ($\mathbb{N}$ denotes the set of the positive integers.)

Definition 5. The *correlation measure of order* k of E_N is defined as

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

where the maximum is taken over all $D = (d_{1,} d_{2,} \dots, d_{k,})\, (d_1 < d_2 < \dots < d_k)$ are non-negative integers and $M \in \mathbb{N}$ with $M + d_k \le N$.

Then E_N is considered as a "good" PR sequence if both $W(E_N)$ and $C_k(E_N)$ (at least for "small" k) are "small" in terms of N. This terminology is justified by the fact that, as Cassaigne, Mauduit and I [12] showed, for a truly random $E_N \in \{-1, +1\}^N$ both W and C_k are $o\left(N/^{1/2}\,(\log N)\right)^c$.

A good candidate for testing these new PR measure is the Legendre symbol $\left(\frac{n}{p}\right)$ whose random type behaviour has been known since at least a century as the papers of Jacobstahl [32], Davenport [15], [16], Bach [8], Peralta [46] and Damgård [14] and my book [50] show. Indeed, in our paper [39] with Mauduit we proved:

Theorem 1. *There is a number* p_0 *so that if* $p > p_0$ *is a prime,* $k \in \mathbb{N}$, $k < p$ *and the sequence* $E_{p-1} = (e_1, \dots, e_{p-1})$ *is defined by*

$$e_n = \left(\frac{n}{p}\right) \qquad (for\ n = 1, 2, \dots, p-1)\ , \tag{1}$$

then we have

$$W(E_{p-1}) \le 9_{p^{1/2}}\ \log p$$

and

$$C_k(E_{p-1}) \le 9\, kp^{1/2}\ \log p\ .$$

The proof was based on the following theorem which we deduced from a theorem of Weil [54] by using an inequality of Vinogradov [53]:

Theorem 2. *If p is a prime, χ is a non-principal character modulo p of order d, $f(x) \in F_p[x]$ has degree k and a factorization $f(x) = b(x - x_1)^{d1} \dots (x - x_s)^{ds}$ (where $x_1 \neq x_j$ for $i \neq j$) in $\overline{F}_p$ (= the algebraic closure of F_p) with*

$$(d_1, d_2, \dots, d_s) = 1\,, \tag{2}$$

and X, Y are real numbers with $0 < Y \leq p$, then

$$\left| \sum_{X<n\leq Y} \chi\bigl(f(n)\bigr) \right| < 9\,kp^{1/2}\ \log p\,.$$

Later we showed [48] that (2) can be replaced by $f(x) \neq cg(x)^d$, where $C \in F_p$, $g(x) \in F_p[x]$, $d \in \mathbb{N}$; in this from Honkala and Tietäväinen [29] also proved the theorem one year later (in 1998).

Our paper with Mauduit was followed by nearly 50 papers written on this field. In these papers 5 subject are studied:

(i) a large family of PR sequences, f-complexity and its sharpening,
(ii) further good constructions,
(iii) the measures of pseudorandomness,
(iv) extensions, generalizations,
(v) applications in number theory.

In the applications (i) and (ii) are the most important thus here I will focus on these two subjects.

3. A large family of PR sequences, f-complexity and its sharpening

In the most applications and, in particular in cryptography it is not enough to construct "a few" "good" PR sequences, instead we need a large family of them. It is a natural idea to extend the construction $e_n \left(\frac{n}{p}\right)$ in (1) Theorem 1 so that we replace n by $f(n)$:

$$e_n = \left(\frac{f(n)}{p}\right) \qquad \bigl(\text{for}\, p \nmid f(n)\bigr) \tag{3}$$

where $f(n) \in F_p[x]$ belongs to a possibly large family of polynomials.

In (3) $f(x)$ cannot be any polynomial with $f(x) \in F_p[x]$. Indeed, if, e.g.,

$$f(x) = cg^2(x) \qquad \big(\text{with } c \in F_p,\ g(x) \in F_p[x]\big)\,,$$

then in (3) we have

$$e_n = \left(\frac{cg^2(n)}{p}\right) = \left(\frac{c}{p}\right) \quad \text{for all } n \text{ with } p \nmid g(n)\,,$$

so that e_n is constant apart from the n's with $p \mid g(n)$, thus $E_N = (e_1, e_2, \dots e_N)$ is certainly not of random type.

Hoffstein and Lieman [28] proposed the use of polynomials $f(x)$ in (3) such that they are squarefree and neither even, nor odd, but they did not prove anything on the PR properties of the corresponding sequences $E_N = (e_1, e_2, \dots e_N)$.

Later Goubin, Mauduit and I [21] showed further (nontrivial) examples for "bad" polynomials $f(x)$.

Mauduit and I [40] gave the first sufficient condition for a polynomials $f(x)$ being "good": we showed that the permutation polynomials $f(x)$ over F_p are "good". However, this result is of no practical use since very little is known on permutation polynomials.

Recently, Goubin, Mauduit and I [21] have extended the set of the "good" polynomials considerably:

Theorem 3. *If p is a prime, $f(x) \in F_p[x]$, $\deg f = d(> 0)$, f has no multiple zero in the algebraic closure of F_p, $E_p = (e_1, e_2, \dots e_p)$ is defined by*

$$e_n \begin{cases} \frac{\left(f(n)\right)}{p} & \text{for } \big(f(n),\, p\big) = 1 \\ +1 & \text{for } p \,|\, f(n)\,, \end{cases}$$

then we have

$$W(E_p) < 10\, dp^{\frac{1}{2}} \log p\,.$$

Moreover, assume that for $k \in \mathbb{N}$ one of the following conditions holds:

(i) *$k = 2$,*

(ii) *$k < p$ and 2 is a primitive root modulo p,*

(iii) *$(4d)^k < p$.*

Then we also have

$$C_k(E_p) < 10\, dkp^{1/2} \log p\,.$$

Perhaps, conditions (i)-(iii) can be relaxed slightly but examples show that they cannot be dropped completely. Condition (ii) is the most convenient one; both W and, for "not very large k", C_k are "small" if this condition holds, i.e., p

is such that 2 is a primitive root modulo p. This condition is easy to handle, a positive proportion of primes is expected to have this property, besides in the applications it suffices to have a possibly long sequence $p_1, p_2, p_3, \dots$ of primes of this property with $p_n < p_{n+1} < 2p_n$ for all n.

The proof of Theorem 3 was based on Theorem 2 and a new addition theorem from combinatorial number theory, and the theory of finite fields was also used.

In a recent paper Rivat and I [47] also studied the computational aspects of the construction described in Theorem 3. First we pointed out that the construction is fast. We also showed that the statistics to be computed in certain standard mathematical statistical test can be estimated in terms of W and the C_k's so that *the estimate of W and the C_k's can be considered as "a priori" testing* which can replace the "a posteriori" testing in many situations.

Theorem 3 describes a *"large"* family of *"good"* PR sequences. However, in the applications the "richness", the "complexity" of the structure of the family can be more important than the size of it. Thus in a recent paper Ahlswede, Khachatrian, Mauduit and I [2] introduced the following measure of complexity of families of binary sequences:

Definition 6. The *f-complexity* ("*f*" for family) *of a family $\mathcal{E}$ of binary* sequences $E_N = (e_1, \dots, e_N) \in \{-1,+1\}^N$, denoted by $\Gamma(\mathcal{E})$, is defined as the greatest k so that whenever $1 \le i_1 < i_2 < \dots < i_k \le N$ and $(\mathcal{E}_1, \mathcal{E}_2, \dots, \mathcal{E}_k) \in \{-1,+1\}^k$, there is an $E_N = (e_1, e_2, \dots, e_N) \in \mathcal{E}$ so that

$$e_{i_1} = \mathcal{E}_1,\ e_{i_2} = \mathcal{E}_2, \dots, e_{i_k} = \mathcal{E}_k\,. \tag{4}$$

((4) is called a specification of length k of E_N.)

Note that if the f-complexity is, say, K, if the adversary determines $K/2$ bits of the keystream, then there are at least $2^{K/2}$ extensions of this specification within $\mathcal{E}$. It follows that an exhaustive search must cover at least $2^{K/2}$, i.e., exponentially many sequences. Thus the f-complexity of a family $\mathcal{E} = \{-1,+1\}^N$ can be considered as a measure of cryptographical security of using sequences $E_N \in \mathcal{E}$ as keystream (more exactly, of using the bit sequences obtained from the $E_N's$ by replacing the $-1's$ in them by $0's$).

If $\mathcal{F}$ is the family of the output sequences of a PRBG with seed (input) length l, then clearly $|\mathcal{F}| = 2^l$ whence it follows that

$$\Gamma(\mathcal{F}) \le l.$$

Thus $\mathcal{F}$ can be considered of *high f-complexity* if its f-complexity is not much (say, by a power of $\log l$) smaller than the seed length l. Ahlswede, Khachatrian, Mauduit and I [2] showed that by a slight modification of the Legendre symbol construction in Theorem 3 one can obtain a PRBG *which has high* *f-complexity* in this sense. I will skip the details of this result since S t e w a r t and I [52] sharpened the result further. We showed that not only every "long" specification occurs in at least one $E_N \in \mathcal{F}$ but more is true: there is a "large" k so that every specification of length k is "nearly uniformly" covered, i.e., there are $(1+o(1))\,\frac{|\mathcal{F}|}{2^k}$ extensions of it to the family $\mathcal{F}$:

Theorem 4. *Let p be a prime, $l \in \mathbb{N}$, $l \le p$. For $\mathcal{A} \subset \{1,\dots,p\}$ let*

$$f_{\mathcal{A}}(x) = \prod_{a\in\mathcal{A}} (x-a),$$

and define the sequence $E_{p,l}\,(f_{\mathcal{A}}) = (e_1,\dots,e_l)$ by

$$e_n = \begin{cases} \left(\dfrac{f_{\mathcal{A}(n)}}{p}\right) & \text{for } n \notin \mathcal{A} \\ (-1)^i & \text{for } n \in \mathcal{A} \text{ and } |\{1,\dots,n\}\cap\mathcal{A}| = i. \end{cases}$$

For $d \in \mathbb{N}$, $d \le p$, $m \in \mathbb{N}$, $l+m \le p$ write

$$\mathcal{F} = \mathcal{F}\,(p,l,m,d) = \big\{E_{p,l}\,(f_{\mathcal{A}}) : |\mathcal{A}| = d, \mathcal{A} \subset \{1,\dots,m\}\big\}.$$

Then for $E_{p,l}\,(f_{\mathcal{A}}) \in \mathcal{F}$ we have

$$W\big(E_{p,l}\,(f_{\mathcal{A}})\big) < 10\,dp^{1/2}\log p\,,$$

and if one of the following three conditions holds:

a) $k = 2$,

b) $k < p$ *and* 2 *is a primitive root modulo* p,

c) $(4d)^k < p$,

then we also have

$$C_k\big(E_{p,l}\,(f_{\mathcal{A}})\big) < 10\,kdp^{1/2}\log p\,.$$

For a given specification S let $\mathcal{F}(S)$ denote the set of those sequences in $\mathcal{F}$ which satisfy the specification S. Then for

$$\min\,(l,m) > 20\,dp^{1/2}\log p\,,$$

$d < p^{^{1/2}}$, $t \in \mathbb{N}$ and $t \le l$, for any specification S of length t from $\{1,2,\dots,l\}$ we have

$$\left|\big|\mathcal{F}(S)\big| - \frac{|\mathcal{F}|}{2^t}\right| \le \frac{12\,tp^{^{1/2}}\,\log p}{m}\,|\mathcal{F}|\,.$$

Recall that by a slight modification of the Legendre symbol construction in Theorems 3 and 4 a PRBG can be obtained. This PRBG can be considered *cryptographically secure*in the computational complexity sense as well, under the hypothesis that the reconstruction of the polynomial $f(x)$ from the values

$\left(\frac{f(n)}{p}\right)$ is difficult if the degree of $f(x)$ is "large" (but $< p^{1/2}$). This hypothesis can be supported by the fact that best estimate in this direction is a recent result of Russel and Shparlinski [49], and even this gives only a very weak upper bound for the number of bit operations needed for determining $f(x)$.

4. Further good constructions

There are further constructions which are nearly as good as the ones in Theorems 1, 3 and 4 (based on the Legendre symbol).

Denote the least non-negative residue of n modulo m by $r_m(n)$, and the multiplicative inverse of a modulo p (for fixed p) by a^{-1}.

1. Mauduit and I [43] studied the following construction: let p be a prime, $f(x) \in F_p[x]$, and define $E_p = (e_1, e_2, \dots, e_p)$ by

$$e_n = \begin{cases} +1 & \text{if } \big(f(n), p\big) = 1 \text{ and } r_p\left(f(n)^{-1}\right) < p/2, \\ -1 & \text{otherwise.} \end{cases}$$

This is, perhaps, the second best construction.

2. Mauduit, Rivat and I [38] studied the following construction: let p be a prime, $f(x) \in F_p[x]$, and define $E_p = (e_1, e_2, \dots, e_p)$ by

$$e_n = \begin{cases} +1 & \text{if } r_p\big(f(n)\big) < p/2, \\ -1 & \text{if } r_p\big(f(n)\big) > p/2\,. \end{cases}$$

This is the fastest construction but it has the weakness that the correlations of high order can be large.

3. In [51] I gave the following construction: let p be a prime, $N = p-1$, and define $E_N = (e_1, e_2, \dots, e_N)$ by

$$e_n = \begin{cases} +1 & \text{if } 1 \le \operatorname{ind} n \le \frac{p-1}{2}, \\ -1 & \text{if } \frac{p+1}{2} \le \operatorname{ind} n \le p-1\,, \end{cases}$$

where $\operatorname{ind} n$ denotes the base g index (discrete logarithm) of n for a fixed primitive root g modulo p.

Gyarmati [24] extended this construction: she replaced n by $f(n)$ where $f(x) \in F_p[x]$ satisfies conditions. If p is "not very large" then this construction is as good as the best ones, but for "large" p it is slow; thus later she developed a faster version of the construction [25].

4. In a recent paper Gyarmati, Pethő and I [27] studied the following construction (which has just been implemented): let $a_1, a_2, \dots$ be a sequence

defined by a linear recursion over F_p such that the characteristic polynomial of it satisfies certain conditions, and let

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

(= Legendre symbol). (More exactly, we studied a slightly modified form of this construction.)

5. Oon [45] studied

$$e_n = \mathcal{R}e\chi\left(f(n)\right),$$

where χ is a (multiplicative) character modulo p, $f(x) \in F_p[x]$.

6. Louboutin, Rivat and I [36] studied the following construction: let

$$e_n = \begin{cases} +1 & \text{if } r_p\left(f(n)^{-1}\right) \equiv r_p\left(f(n)\right) \pmod 2, \\ -1 & \text{if } r_p\left(f(n)^{-1}\right) \not\equiv r_p\left(f(n)\right) \pmod 2 \end{cases}$$

(where $r_p(0^{-1}) = 0$ by definition).

Note that all the construction above are modular constructions with prime moduli. Rivat and I [48] extended some of these constructions to the case of "RSA moduli" m, i.e., to $m = pq$ with m=pq with $p \asymp q$. It turned aut that *the correlation is large* in these cases.

5. The measures of pseudorandomness, connection with other properties

In [39] Mauduit and I also introduced and studied the so called *normality measure* which reflects the "local" PR properties.

Cassaigne, Mauduit and I [12] studied the PR measures for truly random binary sequences and also studied their extreme values. Some of these results have been improved upon by Alon, Kohayakawa, Mauduit, Moreira and Rödl [6], [7]. In [12] we also studied *the connection between C_k and C_l* for $k \neq l$.

Mauduit and I [42] studied the connection between W and C_2. Later Gyarmati [26] extended this result.

Gyarmati [23] studied the connection between the *extreme values of C_2 and C_3*.

Fehér [17] studied the *linear complexity* of some of the sequences constructed above.

Gyarmati [22] introduced and studied the so called *"symmetry measure"*.

Ahlswede, Cassaigne and I [1] estimated the number of sequences with large correlation.

6. Extensions, generalizations, further problems

Mauduit and I [41] studied the case when instead of binary sequences we take *sequences of k symbols.* Later Ahlswede, Mauduit and I [3], [4] extended the notion of f-complexity to this case.

Hubert and I [31] studied the case of *p- pseudorandom binary sequences,* i.e., the case when the binary sequence simulates the binomial distribution of parameter p.

Hubert, Mauduit and I [30] studied the *several dimensional extension* of this theory of pseudorandomness.

In the last several decades Niederreiter and others have studied PR $[0, 1)$ sequences (used in numerical integration) intensively. In a very recent paper Mauduit, Niederreiter and I [37] are studying the connection between PR binary sequences and PR $[0, 1)$ sequences.

Kodila [34] studied the *numerical aspects* of the best constructions described above, and she also analyzed their running time.

7. Applications in number theory

Numerous applications of this theory of pseudorandomness have been given in number theory by Cassaigne, Ferenczi, Mauduit, Rivat, Daboussi, Philip, Tichy, Fouvry, Michel, Oon and me.

In particular, Fouvry, Michael, Rivat and I [18] studied the PR measures of binary sequences formed by the signs of Kloosterman sums. The significance of these result is that later Shparlinski showed that it follows from our estimates for C_2 that the *nonlinearity* of the sequence is large; his proof shows that small C_2 always implies large nonlinearity.

REFERENCES

[1] AHLSWEDE, R.—CASSAIGNE, J.—SÁRKÖZY, A.: *On the correlation of binary sequences.* In: Proceedings of General theory of information transfer and combinatorics (R. Ahlswede et al., eds.). Electron. Notes Discrete Math., Vol. 21, Elsevier, Amsterdam, 2005, pp. 169–171.

[2] AHLSWEDE, R.—KHACHATRIAN, L.—MAUDUIT, C.—SÁRKÖZY, A.: *A complexity measure for families of binary sequences*, Periodica Math. Hungar. **46** (2003), 107–118.

[3] AHLSWEDE, R.—MAUDUIT, C.—SÁRKÖZY, A.: *Large families of pseudorandom sequences of k symbols and their complexity, I.* In: Proceedings of General Theory of Information Transfer and Combinatorics (R. Ahlswede et al., eds.), Electron. Notes Discrete Math., Vol. 21, Elsevier, Amsterdam, 2005, pp. 203–204.

[4] AHLSWEDE, R.—MAUDUIT, C.—SÁRKÖZY, A.: *Large families of pseudorandom sequences of k symbols and their complexity, II.* In: Proceedings of General Theory of Information Transfer and Combinatorics (R. Ahlswede et al., eds.), Electron. Notes Discrete Math., Vol. 21, Elsevier, Amsterdam, 2005, pp. 199–201.

[5] ALEXI, W.—CHOR, B.—GOLDREICH, O.—SCHNORR, C. P.: *RSA and Rabin functions: Certain parts are as hard as the whole*, SIAM J. Comput. **17** (1988), 194–209.

[6] ALON, N.—KOHAYAKAWA, Y.—MAUDUIT, C.—MOREIRA, C. G—RÖDL, V.: *Measures of pseudorandomness for finite sequences: minimal values*, Comb. Probab. Comput. 15, No. 1-2, **15** (2006), 1–29.

[7] ALON, N.—KOHAYAKAWA, Y.—MAUDUIT, C.—MOREIRA, C. G—RÖDL, V.: *Measures of pseudorandomness for finite sequences: typical values*, Proc. Lond. Math. Soc. (3), **95** (2007) 778–812.

[8] BACH, E.: *Realistic analysis of some randomized algorithms*, J. Comput. Syst. Sci. **42** (1991), 30–53.

[9] BLUM, L.—BLUM, M.—SHUB,M.: *A simple unpredictable pseudorandom number generator*, SIAM J. Comput. **15** (1986), 364–383.

[10] BLUM, M.—MICHELI, S.: *How to generate cryptographically strong sequences of pseudorandom bits*, SIAM J. Comput. **13** (1984), 850–864.

[11] BOREL, E.: *Leqons sur la Théorie des Fonctions*, (2nd ed.), Gauthier-Villars, Paris, 1914.

[12] CASSAIGNE, J.—MAUDUIT, C.—SÁRKÖZY, A.: *On finite pseudorandom binary sequences VII: The measures of pseudorandomness*, Acta Arith. **103** (2002), 97–118.

[13] CHAITIN, G. J.: *On the length of programs for computing finite binary sequences*, J. Assoc. Comput. Mach. **13** (1966), 547–569.

[14] DAMGÅRD, I. B.: *On the randomness of Legendre and Jacobi sequences.* In: Advances in Cryptology – CRYPTO '88 (S. Goldwasser, ed.), Lect. Notes Comput. Sci., Vol. 403, Springer-Verlag, Berlin, 1990, pp. 163–172.

[15] DAVENPORT, H.: *On the distribution of quadratic residues (*mod *p)*, J. London Math. Soc. **6** (1931), 49–54.

[16] DAVENPORT, H.: *On the distributions of quadratic residues (*mod *p)*, J. London Math. Soc. **8** (1933), 46–52.

[17] FEHÉR, Á.: *Complexity and pseudorandomness*, in preparation.

[18] FOUVRY, E.—MICHEL, P.—RIVAT, J.—SÁRKÖZY, A.: *On the pseudorandomness of the signs of Kloosterman sums*, J. Aust. Math. Soc. **77** (2004), 425–436.

[19] GOLDWASSER, S.: *Mathematical Foundations of Modern Cryptography: Computational Complexity Perspective*, In: Proceedings of the international congress of mathematicians––ICM 2002 (T. T. Li et al., eds.), Vol., I, Higher Education Press, Beijing, 2002, pp. 245–272.

[20] GOLOMB, S. W.: *Shift Register Sequences*. With portions co-authored by L. R. Welch, R. M. Goldstein and A. W. Hales. Series in Information Systems, San Francisco etc.: Holden-Day, Inc. XIV, 1967.

[21] GOUBIN, L.—MAUDUIT, C.—SÁRKÖZY, A.: *Construction of large families of pseudorandom binary sequences*, J. Number Theory **106** (2004), 56–69.

[22] GYARMATI, K.: *On a pseudorandom property of binary sequences*, Ramanujan J. **8**(2004), 289–302.

[23] GYARMATI, K.: *On the correlation of binary sequences*, Studia Sci. Math. Hungar. **42** (2005), 79–93.

[24] GYARMATI, K.: *On a family of pseudorandom binary sequences*, Periodica Math. Hungar. **49** (2004), 45–63.

[25] GYARMATI, K.: *On a fast version of a pseudorandom generator*. In: Proceedings on General Theory of Information Transfer and Combinatorics (R. Ahlswede et al., eds.), Electron. Notes Discrete Math. 21, **291** (2005).

[26] GYARMATI, K.: *An inequality between the measures of pseudorandomness*, Annales Univ. Sci. Budapest. Eötvös Sect. Math. **46** (2003), 157–166.

[27] GYARMATI, K.—PETHŐ, A.—SÁRKÖZY, A.: *On linear recursions and pseudorandomness*, Acta Arith. **118** (2005), 359–374.

[28] HOFFSTEIN, J.—LIEMAN, D.: *The distribution of the quadratic symbol in function fields and a faster mathematical stream cipher*. In: Proceedings of the workshop–CCNT '99 (K.-Y. Lam et al., eds.) Progr. Comput. Sci. and Appl. Logic, Vol. 20, Birkhauser Verlag, Basel, 2001, pp. 59–68.

[29] HONKALA, I.—TIETÄVÄINEN, A.: *Codes and Number Theory*. In: Handbook of Coding Theory (V. S. Pless et al., eds.), Elsevier, Amsterdam, 1998, pp. 1141–1194.

[30] HUBERT, P.—MAUDUIT, C.—SÁRKÖZY, A.: *On pseudorandom binary lattices*, Acta Arith. **125** (2006), 51–68.

[31] HUBERT, P.—SÁRKÖZY, A.: *On p-pseudorandom binary sequences*, Periodica Math. Hungar. **49** (2004) 73–91.

[32] JACOBSTAHL,E.: *Anwendungen einer Formel aus der Theorie der quadratischen Reste*, Dissertation, Berlin, 1906, 26–32.

[33] KNUTH, D. E.: The Art of Computer Programming, vol. 2, (2nd ed.), Addison-Wesley, Reading, Mass., 1981.

[34] KODILA, D.: *Running time analysis of constructions of pseudorandom binary sequences*, Annales Univ. Sci. Budapest, Eötvös Sect. Math., to appear.

[35] KOLMOGOROV, A.: *Three approaches to the definition of the concept "quantity of information"*, Problemy Peredachi Informatsii **1** (1965), 3–11.

[36] LOUBOUTIN, S.—RIVAT, J.—SÁRKÖZY, A.: *On a problem of D. H. Lehmer*, Compositio Math., to appear.

[37] MAUDUIT, C.—NIEDERREITER, H.—SÁRKÖZY, A.: *Pseudorandom binary and [0.1) sequences*, in preparation.

[38] MAUDUIT, C.—RIVAT,J.—SÁRKÖZY, A.: *Construction of pseudorandom binary sequences using additive characters*, Monatshefte Math. **141** (2004), 197–208.

[39] MAUDUIT, C.—SÁRKÖZY, A.: *On finite pseudorandom binary sequences, I.* Measure of pseudorandomness, the Legendre symbol, Acta Arith. **82** (1997), 365–377.

[40] MAUDUIT, C.—SÁRKÖZY, A.: *On finite pseudorandom binary sequences, II. (The Champernowne, Rudin-Shapiro and Thue-Morse sequences. A further construction.)* J. Number Theory **73** (1998), 256–276.

[41] MAUDUIT, C.—SÁRKÖZY, A.: *On finite pseudorandom sequences of k symbols*, Indag. Math. **13** (2002), 89–101.

[42] MAUDUIT, C.—SÁRKÖZY, A.: *On the measures of pseudorandomness of binary sequences*, Discrete Math. **271**(2003), 195–207.

[43] MAUDUIT,C.—SÁRKÖZY, A.: *Construction of pseudorandom binary sequences by using the multiplicative inverse*, Acta Math. Hungar. **108** (2005), 239–252.

[44] MENEZES, A.—van OORSHOT, P.—VANSTONE, S. A.: *Handbook of Applied Cryptography*, CRS Press, Boca Raton, 1997.

[45] OON, S. M.: *Construction des Suites Binaires Pseudo-aléatories*, PhD Thesis, Nancy, 2005.

[46] PERALTA, R.: *On the distribution of quadratic residues and nonresidues modulo a prime number*, Math. Comp. **58** (1992), 433–440.

[47] RIVAT, J.—SÁRKÖZY, A.: *On pseudo-random binary sequences and their applications*, Proceedings on General Theory of Information Transfer and Combinatorics, to appear.

[48] RIVAT, J.—SÁRKÖZY, A.: *Modular constructions of pseudorandom binary sequences with composite moduli*, Periodica Math. Hungar. **51** (2005), 75–107.

[49] RUSSEL, A.—SHPARLINSKI, I.: *Classical and quantum function reconstruction via character evaluation*, to appear.

[50] SÁRKÖZY, A.: *Number Theory and Its Applications*, Műszaki Könyvkiadó, Budapest, 1978 (in Hungarian).

[51] SÁRKÖZY, A.: *A finite pseudorandom binary sequence*, Studia Sci. Math. Hungar. **38** (2001), 377–384.

[52] SÁRKÖZY, A.—STEWART, C. L.: *On pseudorandomness in families of sequences derived from the Legendre symbol*, Designs, Codes and Cryptography. Period Math. Hungar. **54** (2007), 163–173.

[53] VINOGRADOV, I. M.: *Elements of Number Theory*. Transl. from the 5th rev. ed. by S. Kravetz, Dover Publ. VIII, New York, 1954.

[54] WEIL, A.: *Sur les courbes algébriques et les variétés qui s'en déduisent*, Acta Sci. Ind. Vol. 1041, Hermann, Paris, 1948.

Received November 10, 2005

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