

On the pseudorandomness of automatic sequences

László Mériai and Arne Winterhof

Johann Radon Institute for Computational and Applied Mathematics
 Austrian Academy of Sciences
 Altenbergerstr. 69, 4040 Linz, Austria
`{laszlo.merai, arne.winterhof}@oeaw.ac.at`

Abstract

We study the pseudorandomness of automatic sequences in terms of well-distribution and correlation measure of order 2. We detect non-random behavior which can be derived either from the functional equations satisfied by their generating functions or from their generating finite automata, respectively.

2000 Mathematics Subject Classification: 11K45, 03D05, 68Q25, 68Q70

Keywords and phrases: finite automaton, automatic sequences, correlation measure, pseudorandom sequences, Thue-Morse sequence, state complexity

1 Introduction

Let $k \geq 2$ be an integer. A k -automatic sequence (s_n) over an alphabet Σ is the output sequence of a finite automaton, where the input is the k -ary digital expansion of n . Automatic sequences have gained much attention during the last decades. For monographs and surveys about automatic sequences we refer to [1, 2, 7, 8].

The authors are partially supported by the Austrian Science Fund FWF Project 5511-N26 which is part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications".

"This is a pre-print of an article published in *Cryptography and Communications*. The final authenticated version is available online at: <https://doi.org/10.1007/s12095-017-0260-7>".

For a prime $k = p$, p -automatic sequences (s_n) over the finite field \mathbb{F}_p of p elements can be characterized by a result of Christol [4], see also [5]: Let

$$G(x) = \sum_{n=0}^{\infty} s_n x^n$$

be the *generating function* of the sequence (s_n) over \mathbb{F}_p . Then (s_n) is p -automatic over \mathbb{F}_p if and only if $G(x)$ is algebraic over $\mathbb{F}_p[x]$, that is, there is a characteristic polynomial $0 \neq h(x, y) \in \mathbb{F}_p[x, y]$ such that $h(x, G(x)) = 0$.

For example, the *Thue-Morse sequence* over \mathbb{F}_2 is defined by

$$t_n = \begin{cases} t_{n/2} & \text{if } n \text{ is even,} \\ t_{(n-1)/2} + 1 & \text{if } n \text{ is odd,} \end{cases} \quad n = 1, 2, \dots$$

with initial value $t_0 = 0$. Taking

$$h(x, y) = (x + 1)^3 y^2 + (x + 1)^2 y + x,$$

its generating function $G(x)$ satisfies $h(x, G(x)) = 0$.

Any p -automatic sequence over \mathbb{F}_p which is not ultimately periodic, that is, its generating function $G(x)$ is not rational, passes some unpredictability tests. In particular, it has large linear complexity profile. This can be expressed in terms of the local degrees of $h(x, y)$.

We recall that the N th linear complexity $L(s_n, N)$ of a sequence (s_n) over \mathbb{F}_p is the length L of a shortest linear recurrence relation satisfied by the first N elements of (s_n) :

$$s_{n+L} = c_{L-1} s_{n+L-1} + \dots + c_1 s_{n+1} + c_0 s_n, \quad 0 \leq n \leq N - L - 1,$$

for some $c_0, \dots, c_{L-1} \in \mathbb{F}_q$. We use the convention that $L(s_n, N) = 0$ if the first N elements of (s_n) are all zero and $L(s_n, N) = N$ if $s_0 = \dots = s_{N-2} = 0 \neq s_{N-1}$.

For a random sequence (s_n) we have

$$L(s_n, N) = \frac{N}{2} + O(\log N) \quad \text{for all } N \geq 2, \quad (1)$$

see [14].

The authors proved in [13] that any p -automatic sequence over \mathbb{F}_p which is not ultimately periodic has N th linear complexity of (best possible) order of magnitude N , that is constant times N , where the implied constant depends on the degree of a characteristic polynomial $h(x, y)$ of $G(x)$.

Especially, the N th linear complexity of sequences with $h(x, G(x)) = 0$ and local degree 2 in y of $h(x, y)$ satisfy (1). For example, [13, Theorem 1] applied to the Thue-Morse sequence gives

$$\left\lceil \frac{N-1}{2} \right\rceil \leq L(t_n, N) \leq \left\lfloor \frac{N-1}{2} \right\rfloor + 1.$$

(The exact value $L(t_n, N) = 2 \lfloor \frac{N+2}{4} \rfloor$ can be obtained using a different method, see also [13].)

Although automatic sequences have large linear complexity profile, they are statistically distinguishable from random sequences if N is sufficiently large and certain pseudorandom measures are of (worst possible) order of magnitude N .

For a given finite sequence (s_n) over \mathbb{F}_2 write

$$U(s_n, t, a, b) = \sum_{j=0}^{t-1} (-1)^{s_{a+jb}},$$

and for $D = (d_1, \dots, d_k)$ with non-negative integers $0 \leq d_1 < \dots < d_k$ write

$$V(s_n, M, D) = \sum_{n=0}^{M-1} (-1)^{s_{n+d_1} + s_{n+d_2} + \dots + s_{n+d_k}}.$$

Then the N th well-distribution measure of (s_n) is

$$W(s_n, N) = \max_{a,b,t} |U(s_n, t, a, b)| = \max_{a,b,t} \left| \sum_{j=0}^{t-1} (-1)^{s_{a+jb}} \right|,$$

where the maximum is taken over all $a, b, t \in \mathbb{N}$ such that $0 \leq a \leq a + (t-1)b < N$, and the N th correlation measure of order k of (s_n) is

$$C_k(s_n, N) = \max_{M,D} |V(s_n, M, D)| = \max_{M,D} \left| \sum_{n=0}^M (-1)^{s_{n+d_1} + s_{n+d_2} + \dots + s_{n+d_k}} \right|,$$

where the maximum is taken over all D and M such that $d_k + M < N$. For more background on pseudorandom measures see [9, 16, 17].

The sequence (s_n) possesses good properties of pseudorandomness if both these measures $W(s_n, N)$ and $C_k(s_n, N)$ (at least for small k) are ‘small’ in terms of N (in particular, both are $o(N)$ as $N \rightarrow \infty$). This terminology is justified since for a truly random sequence $(s_n)_{n=0}^{N-1}$ each of these measures

is $N^{1/2}(\log N)^{O(1)}$. (For a more precise version of this result see [3].) The Legendre sequence is an example of such a pseudorandom sequence with both small well-distribution and correlation measures, see [11].

In Section 2 we show that a certain family of 2-automatic sequences classified by its functional equation for its generating function $h(x, G(x)) = 0$ suffers a large well-distribution measure. This family includes the Baum-Sweet sequence and the characteristic sequence of the set of sums of three integer squares. In Section 3 we show that another family, again characterized by $h(x, G(x)) = 0$ for a certain class of polynomials $h(x, y)$, is of large correlation measure of order 2. This family includes pattern sequences such as the Thue-Morse sequence as well as the Rudin-Shapiro sequence and the regular paperfolding sequence.

Note that it is known that both the Thue-Morse sequence and the Rudin-Shapiro sequence have a large correlation measure of order 2, see [12].

In Section 4 we prove another bound on the correlation measure of order 2 of any 2-automatic sequence in terms of the number of states of its generating finite automaton. Roughly speaking, if the number of states of the finite automaton is small, the correlation measure of order 2 of the corresponding sequence is large. However, the results of Section 3 are slightly stronger but apply only to some special automatic sequences.

On the other hand, our last result implies that for any automatic sequence with small correlation measure of order 2, its state complexity has to be large. In particular, we apply this result to the Legendre sequence.

2 Sequences with large well-distribution measure

First we mention two sequences with large well-distribution measure, the Baum-Sweet sequence and the characteristic sequence of the set of sums of three squares. Then we show that these sequences belong to a larger family of sequences with a certain type of polynomials $h(x, y)$ with $h(x, G(x)) = 0$ which all have a large well-distribution measure.

Baum-Sweet sequence

The Baum-Sweet sequence (b_n) is a 2-automatic sequence defined by the rule $b_0 = 1$ and for $n \geq 1$

$$b_n = \begin{cases} 1 & \text{if the binary representation of } n \text{ contains no block of} \\ & \text{consecutive 0's of odd length,} \\ 0 & \text{otherwise.} \end{cases}$$

Equivalently, we have for $n \geq 1$ of the form $n = 4^k m$ with m not divisible by 4

$$b_n = \begin{cases} 0 & \text{if } m \text{ is even,} \\ b_{(m-1)/2} & \text{if } m \text{ is odd.} \end{cases}$$

The Baum-Sweet sequence satisfies

$$W(b_n, N) \geq \left| \sum_{n=0}^{\lfloor (N-3)/4 \rfloor} (-1)^{b_{4n+2}} \right| = \left\lfloor \frac{N+1}{4} \right\rfloor \quad \text{for } N \geq 1. \quad (2)$$

The generating function $G(x)$ of (b_n) satisfies

$$h(x, G(x)) = 0 \quad \text{with} \quad h(x, y) = y^4 + xy^2 + y.$$

The characteristic sequence of the set of sums of three squares

Let (u_n) be the characteristic sequence of non-negative integers that can be written as a sum of three squares

$$u_n = \begin{cases} 1 & \text{if } n = u^2 + v^2 + w^2 \text{ for some integers } u, v, w, \\ 0 & \text{otherwise.} \end{cases}$$

By the Three-Square Theorem this is equivalent to

$$u_n = \begin{cases} 0 & \text{if there exist non-negative integers } a, k \text{ with } n = 4^a(8k+7), \\ 1 & \text{otherwise.} \end{cases}$$

We have

$$W(u_n, N) \geq \left| \sum_{n=0}^{\lfloor N/8 \rfloor - 1} (-1)^{u_{8n+7}} \right| = \left\lfloor \frac{N}{8} \right\rfloor \quad \text{for } N \geq 1. \quad (3)$$

The generating function $G(x)$ of (u_n) satisfies $h(x, G(x)) = 0$ with

$$h(x, y) = (x^8 + 1)y^4 + (x^8 + 1)y + x^6 + x^5 + x^3 + x^2 + x,$$

see [10].

We present some generalizations of (2) and (3).

Theorem 1. *Let (s_n) be a sequence over \mathbb{F}_2 with generating function $G(X)$ satisfying $h(x, G(x)) = 0$ for some polynomial $h(x, y)$ over \mathbb{F}_2 of the form*

$$h(x, y) = f_2(y^{2^\ell}) + x f_1(y^2) + y + f_0(x) \quad (4)$$

with polynomials f_0, f_1, f_2 over \mathbb{F}_2 , $\deg f_0 \leq 2^\ell - 3$, and $\ell \geq 2$. Then we have

$$W(s_n, N) \geq \left\lfloor \frac{N+1}{2^\ell} \right\rfloor.$$

If $h(x, y)$ is of the form

$$h(x, y) = f_1(x^2, y^2) + (x^{2^\ell} + 1)y + f_0(x) \quad (5)$$

with polynomials f_1 and f_0 over \mathbb{F}_2 with $\deg f_0 \leq 2^\ell - 2$ and $\ell \geq 1$, then we have

$$W(s_n, N) \geq \left\lfloor \frac{N}{2^\ell} \right\rfloor.$$

Proof. First let $h(x, y)$ be of the form (4). Comparing the coefficients of $h(x, G(x)) = 0$ at $x^{2^\ell n + 2^\ell - 2}$ we see that $s_{2^\ell n + 2^\ell - 2} = 0$. Hence,

$$\sum_{n=0}^{M-1} (-1)^{s_{2^\ell n + 2^\ell - 2}} = M.$$

Taking

$$M = \left\lfloor \frac{N+1}{2^\ell} \right\rfloor$$

gives the first result.

If $h(x, y)$ is of the form (5), we compare the coefficients at $x^{2^\ell n + 2^\ell - 1}$ and get $s_{2^\ell - 1} = 0$ and $s_{2^\ell(n+1) + 2^\ell - 1} = s_{2^\ell n + 2^\ell - 1}$ for $n \geq 0$ and the result follows analogously. \square

3 Large correlation measure of order 2 obtained from a characteristic polynomial

Now we prove a lower bound on the correlation measure of order 2 for a large class of automatic sequences.

Theorem 2. *Let (s_n) be a sequence over \mathbb{F}_2 with generating function $G(x)$ satisfying*

$$h(x, G(x)) = 0$$

for some polynomial $h(x, y)$ of the form

$$h(x, y) = (x+1)^{2^\ell} ((a_1 x + a_0)y^2 + y) + f(x)$$

with $\ell \geq 0$, $\deg f \leq 2^\ell - 1$, and $(a_1, a_0) \neq (0, 0)$. Then we have

$$C_2(s_n, N) > \frac{N}{2^\ell + 2} - 2 \quad \text{for } N \geq 2^{\ell+1} + 4.$$

Proof. For any $k \geq 0$ comparing coefficients in $(x+1)^{2^{k+\ell}-2^\ell} h(x, G(x)) = 0$ at $x^{2n+2^{k+\ell}}$ and $x^{2n+2^{k+\ell}+1}$ provides

$$s_{2n} + s_{2n+2^{k+\ell}} = a_0(s_n + s_{n+2^{k+\ell}-1}), \quad n \geq 0, \quad (6)$$

and

$$s_{2n+1} + s_{2n+2^{k+\ell}+1} = a_1(s_n + s_{n+2^{k+\ell}-1}), \quad n \geq 0, \quad (7)$$

respectively.

We define the integer M by $2^M \leq \frac{N}{2^{\ell+1}} < 2^{M+1}$ and put for $k = 0, 1, \dots, M$

$$\gamma_k = \sum_{n=0}^{2^k-1} (-1)^{s_n+s_{n+2^{k+\ell}}}.$$

By (6) and (7) we get for $1 \leq k \leq M$

$$\begin{aligned} \gamma_k &= \sum_{n=0}^{2^{k-1}-1} (-1)^{s_{2n}+s_{2n+2^{k+\ell}}} + \sum_{n=0}^{2^{k-1}-1} (-1)^{s_{2n+1}+s_{2n+2^{k+\ell}+1}} \\ &= \sum_{n=0}^{2^{k-1}-1} (-1)^{a_0(s_n+s_{n+2^{k+\ell}-1})} + \sum_{n=0}^{2^{k-1}-1} (-1)^{a_1(s_{2n+1}+s_{n+2^{k+\ell}-1})} \\ &= (a_0 + a_1)\gamma_{k-1} + (2 - a_0 - a_1)2^{k-1}, \end{aligned}$$

$\gamma_0 = \pm 1$, and thus by induction

$$\gamma_k = (a_0 + a_1)^k \gamma_0 + (2 - a_0 - a_1)(2^k - 1) \quad \text{for } k = 1, \dots, M.$$

Hence, $C_2(s_n, N) \geq |\gamma_M| = 2^M > \frac{N}{2^{\ell+2}}$ if $a_0 = a_1 = 1$ and $C_2(s_n, N) \geq |\gamma_M| \geq 2^M - 2 > \frac{N}{2^{\ell+2}} - 2$ otherwise. \square

Remark 3. The method can be extended to larger families of polynomials $h(x, y)$. However, for the readability we chose a simple family which covers all of the following examples.

Examples

Pattern sequence

For a pattern $P \neq (0, \dots, 0)$ of length ℓ define the sequence (r_n) by

$$r_n \equiv e_P(n) \pmod{2}, \quad r_n \in \mathbb{F}_2, \quad n = 0, 1, \dots$$

where $e_P(n)$ is the number of occurrences of P in the binary expansion of n . The sequence (r_n) over \mathbb{F}_2 satisfies the following recurrence relation

$$r_n = \begin{cases} r_{\lfloor n/2 \rfloor} + 1 & \text{if } n \equiv a \pmod{2^\ell}, \\ r_{\lfloor n/2 \rfloor} & \text{otherwise,} \end{cases} \quad n = 1, 2, \dots \quad (8)$$

with initial value $r_0 = 0$, where a is the integer $0 < a < 2^\ell$ such that its binary expansion corresponds to the pattern P .

Classical examples for binary pattern sequences are the *Thue-Morse sequence* ($\ell = 1$ and $P = 1$ ($a = 1$)) and the *Rudin-Shapiro sequence* ($\ell = 2$ and $P = 11$ ($a = 3$)).

Corollary 4. *Let a, ℓ be integers with $1 \leq a < 2^\ell$. If (r_n) is the pattern sequence defined by (8), then*

$$C_2(r_n, N) > \frac{N}{2^\ell + 2} - 2 \quad \text{for } N \geq 2^{\ell+1} + 4.$$

Proof. The result follows from Theorem 2 with $h(x, y) = (x + 1)^{2^\ell+1}y^2 + (x + 1)^{2^\ell}y + x^a$. \square

Regular paperfolding sequence

The value of any given term $v_n \in \mathbb{F}_2$ in the regular paperfolding sequence can be defined as follows. If $n = m \cdot 2^k$ where m is odd, then

$$v_n = \begin{cases} 1 & \text{if } m \equiv 1 \pmod{4}, \\ 0 & \text{if } m \equiv 3 \pmod{4}, \end{cases} \quad n = 1, 2, \dots$$

and any $v_0 \in \mathbb{F}_2$.

Corollary 5. *Let (v_n) be the regular paperfolding sequence. Then*

$$C_2(v_n, N) > \frac{N}{6} - 2 \quad \text{for } N \geq 12.$$

Proof. The result follows from Theorem 2 with $h(x, y) = (x + 1)^4(y^2 + y) + 1$. \square

A sequence with perfect lattice profile and perfect linear complexity profile

The generating function $G(x)$ of the sequence (w_n) over \mathbb{F}_2 defined by

$$w_{2n} = 1 \quad \text{and} \quad w_{2n+1} = w_n + 1, \quad n = 0, 1, \dots \quad (9)$$

satisfies the functional equation $h(x, G(x)) = 0$ with $h(x, y) = (x+1)(xy^2 + y) + 1 \in \mathbb{F}_2[x, y]$. This is the only sequence with both a perfect linear complexity profile and a perfect 'lattice profile', see [6] for more details. Sequences with the first are characterized by $w_0 = 1$ and $w_{2n+2} = w_{2n+1} + w_n$ but the choice of w_{2n+1} is free for $n \geq 1$, see [15]. Sequences with the latter are characterized by $w_{2n+1} = w_n + 1$ but the choice of any w_{2n} is free, see [6].

Corollary 6. *Let (w_n) be the sequence defined by (9). Then*

$$C_2(w_n, N) > \frac{N}{3} - 2 \quad \text{for } N \geq 6.$$

4 Large correlation measures of order 2 obtained from the generating automaton

In this section we prove lower bounds on the correlation measure of order 2 of automatic sequences in terms of the number of states of the automaton which generates the sequence.

We recall that a *finite automaton* is defined to be a 6-tuple $M = (Q, \Sigma, \delta, q_0, \Delta, \tau)$, where Q is a finite set of states, Σ is the finite input alphabet, $\delta : Q \times \Sigma \rightarrow Q$ is the transition function, $q_0 \in Q$ is the initial state, Δ is the output alphabet and $\tau : Q \rightarrow \Delta$ is the output function. As usual, we define $\delta(q, xa) = \delta(\delta(q, x), a)$ for all $q \in Q$, $x \in \Sigma^*$ and $a \in \Sigma$. For $k \geq 2$ put $\Sigma_k = \{0, 1, \dots, k-1\}$. Then we say that the sequence (s_n) over a finite alphabet Δ is *k-automatic* if there exists an automaton $(Q, \Sigma_k, \delta, q_0, \Delta, \tau)$ such that $s_n = \tau(\delta(q_0, (n)_k))$ for all $n \geq 0$ where $(n)_k \in \Sigma_k^*$ is the word consisting of the k -ary digits of n .

In the following theorem we prove that an automatic sequence which is generated by an automaton with only a few states cannot have good pseudorandomness properties in terms of the correlation measure of order 2.

Theorem 7. *Let (s_n) be a k -automatic binary sequence generated by the finite automaton $(Q, \Sigma_k, \delta, q_0, \Sigma_2, \tau)$. Then*

$$C_2(s_n, N) \geq \frac{N}{k(|Q| + 1)} \quad \text{for } N \geq k(|Q| + 1).$$

Proof. We can assume that $\delta(q_0, 0) = 0$, see [2, Theorem 5.2.1]. Let $\varphi : Q^* \rightarrow Q^*$ be defined by $\varphi(q) = \delta(q, 0)\delta(q, 1) \dots \delta(q, k-1)$ for $q \in Q$ and $\varphi(xy) = \varphi(x)\varphi(y)$. Let $\mathbf{w} = w_0w_1w_2 \dots$ be an infinite word over Q which

is a fixed point of φ . Then $\delta(q_0, (n)_k) = w_n$ and $\tau(w_n) = s_n$ for all $n \geq 0$, see [2, Proof of Theorem 6.3.2].

Put

$$M = \left\lfloor \frac{\log(N/(|Q| + 1))}{\log k} \right\rfloor \geq 1.$$

By the pigeon hole principle, among the first $|Q| + 1$ elements of (w_n) there are two elements having the same value, say $w_i = w_j$, $0 \leq i < j \leq |Q|$. Then for the M th iteration of φ , $\varphi^M : Q \rightarrow Q^{k^M}$ we have $\varphi^M(w_i) = \varphi^M(w_j)$, thus $w_{i \cdot k^{M+l}} = w_{j \cdot k^{M+l}}$ for $l = 0, \dots, k^M - 1$ so $s_{i \cdot k^{M+l}} = s_{j \cdot k^{M+l}}$ for $l = 0, \dots, k^M - 1$. Then

$$C_2(s_n, N) \geq V(s_n, N, k^M, D) = \sum_{l=0}^{k^M-1} (-1)^{u_{i \cdot k^{M+l}} + u_{j \cdot k^{M+l}}} = k^M \geq \frac{N}{k(|Q| + 1)}$$

with lags $D = (i \cdot k^M, j \cdot k^M)$. □

Examples

The Thue-Morse sequence $(t_n)_{n \geq 0}$ can be defined by a finite automaton with two states, see Figure 1. Hence, Theorem 7 yields

$$C_2(t_n, N) \geq \frac{N}{6} \quad \text{for } N \geq 6.$$

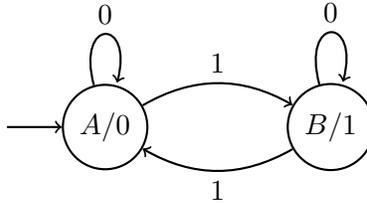


Figure 1: Automaton generating the Thue-Morse sequence.

The Rudin-Shapiro sequence $(r_n)_{n \geq 0}$ can be defined by a finite automaton with four states, see Figure 2. Hence, Theorem 7 yields

$$C_2(t_n, N) \geq \frac{N}{10} \quad \text{for } N \geq 10.$$

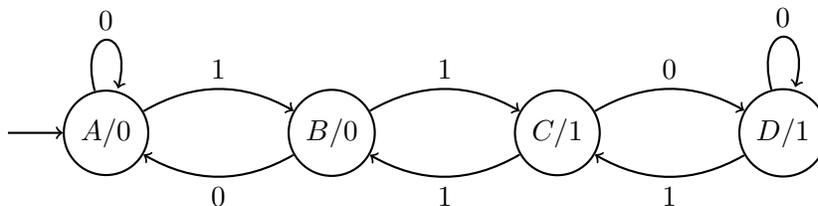


Figure 2: Automaton generating the Rudin-Shapiro sequence.

State complexity of binary sequences

Theorem 7 allows to give lower bounds on the state complexity of binary sequences in terms of the correlation measure of order 2.

Let $k \geq 2$. Then the N th state complexity $SC_k(s_n, N)$ of a sequence (s_n) over \mathbb{F}_2 is the minimum of the number of states of finite k -automatons which generate the first N elements. For example, the state complexity of the Thue-Morse sequence (t_n) is $SC_2(t_n, N) = 2$ for $N \geq 2$. By Theorem 7 we get lower bound on the N th state complexity of binary sequences.

Corollary 8. *Let (s_n) be a binary sequence. Then for all $k \geq 2$ we have*

$$SC_k(s_n, N) \geq \frac{N}{k \cdot C_2(s_n, N)} - 1 \quad \text{for } N \geq 3.$$

As an example we can give a lower bound on the state complexity of the Legendre sequence (l_n) defined by

$$l_n = \begin{cases} 0 & \text{if } \left(\frac{n}{p}\right) = 1, \\ 1 & \text{otherwise,} \end{cases}$$

where $p > 2$ is a prime number and $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol modulo p . Mauduit and Sárközy [11] proved that $C_2(l_n, N) \ll p^{1/2} \log p$ for $N \leq p$ thus Corollary 8 gives

$$SC_k(l_n, N) \gg \frac{N}{k \cdot p^{1/2} \log p} - 1 \quad \text{for } 3 \leq N \leq p.$$

Acknowledgment

The authors would like to thank Christian Mauduit for helpful discussions.

References

- [1] J.-P. Allouche. Finite automata and arithmetic. *Séminaire Lotharingien de Combinatoire* (Gerolfingen, 1993), 1–18, Prépubl. Inst. Rech. Math. Av., 1993/34, Univ. Louis Pasteur, Strasbourg, 1993.
- [2] J. P. Allouche and J. Shallit. Automatic sequences. Theory, applications, generalizations. Cambridge University Press, Cambridge, 2003.
- [3] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl. Measures of pseudorandomness for finite sequences: typical values. *Proc. Lond. Math. Soc.* 95(3): 778–812, 2007.
- [4] G. Christol. Ensembles presque périodiques k -reconnaissables. *Theoret. Comput. Sci.* 9:141–145, 1979.
- [5] G. Christol, T. Kamae, M. Mendés France, and G. Rauzy. Suites algébriques, automates et substitutions. *Bull. Soc. Math. France* 108(4):401–419, 1980.
- [6] G. Dorfer, W. Meidl, and A. Winterhof. Counting functions and expected values for the lattice profile at n . *Finite Fields Appl.* 10(4):636–652, 2004.
- [7] M. Drmota. Subsequences of automatic sequences and uniform distribution. In P. Kritzer et al. (eds.), Uniform distribution and quasi-Monte Carlo methods, 87–104, *Radon Ser. Comput. Appl. Math.*, 15, De Gruyter, Berlin, 2014.
- [8] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward. Recurrence sequences. *Mathematical Surveys and Monographs*, 104. American Mathematical Society, Providence, RI, 2003
- [9] K. Gyarmati. Measures of pseudorandomness. In P. Charpin, A. Pott, A. Winterhof (eds.), Finite fields and their applications *Radon Series in Computational and Applied Mathematics*, de Gruyter 2013, 43-64.
- [10] R. Hofer and A. Winterhof, Linear complexity and expansion complexity of some number theoretic sequences. In *Arithmetics in Finite Fields (WAIFI 2016)*. Lecture Notes in Computer Science, vol. 10064 (Springer, Cham, 2017), pp. 67–74.
- [11] C. Mauduit and A. Sárközy. On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol. *Acta Arith.* 82(4): 365–377, 1997.

- [12] 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):256–276, 1998.
- [13] L. Mérai and A. Winterhof. On the N th linear complexity of p -automatic sequences over \mathbb{F}_p . Preprint 2016.
- [14] H. Niederreiter. The probabilistic theory of linear complexity. Advances in cryptology-EUROCRYPT '88 (Davos, 1988), 191–209, Lecture Notes in Comput. Sci. 330, Springer, Berlin, 1988.
- [15] H. Niederreiter. Sequences with almost perfect linear complexity profile. Advances in cryptology-EUROCRYPT '87 (D. Chaum and W. L. Price, Eds.), Lecture Notes in Computer Science, Vol. 304, pp. 37–51, Springer-Verlag, Berlin/Heidelberg/New York, 1988.
- [16] A. Sárközy. On finite pseudorandom binary sequences and their applications in cryptography. *Tatra Mt. Math. Publ.* 37:123–136, 2007.
- [17] A. Topuzoğlu and A. Winterhof. Pseudorandom sequences. Topics in geometry, coding theory and cryptography, 135–166, *Algebr. Appl.*, 6, Springer, Dordrecht, 2007.