sciendo

uniform distribution theory

DOI: 10.2478/udt-2019–0012
Unif. Distrib. Theory **14** (2019), no.2, 33–42

ON THE MAXIMUM ORDER COMPLEXITY OF THE THUE-MORSE AND RUDIN-SHAPIRO SEQUENCE

Zhimin Sun[1] — Arne Winterhof[2]

[1]Hubei University, Wuhan, CHINA

[2]RICAM, Linz, AUSTRIA

ABSTRACT. Expansion complexity and maximum order complexity are both finer measures of pseudorandomness than the linear complexity which is the most prominent quality measure for cryptographic sequences. The expected value of the Nth maximum order complexity is of order of magnitude $\log N$ whereas it is easy to find families of sequences with Nth expansion complexity exponential in $\log N$. This might lead to the conjecture that the maximum order complexity is a finer measure than the expansion complexity. However, in this paper we provide two examples, the Thue-Morse sequence and the Rudin-Shapiro sequence with very small expansion complexity but very large maximum order complexity. More precisely, we prove explicit formulas for their Nth maximum order complexity which are both of the largest possible order of magnitude N. We present the result on the Rudin-Shapiro sequence in a more general form as a formula for the maximum order complexity of certain pattern sequences.

Communicated by Christian Mauduit

1. Introduction

1.1. Motivation

For a sequence $\mathcal{S} = (s_i)_{i=0}^{\infty}$ over the finite field $\mathbb{F}_2$ of two elements and a positive integer N, the *Nth linear complexity* $L(\mathcal{S}, N)$ is the length L of the shortest

2010 Mathematics Subject Classification: 11B85, 11K45.

Keywords: Thue-Morse sequence, Rudin-Shapiro sequence, automatic sequences, maximum order complexity, measures of pseudorandomness.

linear recurrence

$$s_{i+L} = \sum_{\ell=0}^{L-1} c_\ell s_{i+\ell}, \quad 0 \le i \le N-L-1,$$

with coefficients $c_\ell \in \mathbb{F}_2$, which is satisfied by the first N terms of the sequence.

The (Nth) linear complexity is a measure for the unpredictability of a sequence and thus its suitability in cryptography. A sequence $\mathcal{S}$ with small $L(\mathcal{S}, N)$ for a sufficiently large N is disastrous for cryptographic applications. However, the converse is not true. There are highly predictable sequences $\mathcal{S}$ with large $L(\mathcal{S}, N)$, including the example

$$s_0 = \cdots = s_{N-2} = 0 \ne s_{N-1}. \tag{1}$$

Hence, for testing the suitability of a sequence in cryptography we also have to study finer figures of merit. A recent survey on linear complexity and related measures is given in [14].

The *Nth maximum order complexity* $M(\mathcal{S}, N)$ (or the *Nth nonlinear complexity*) of a binary sequence $\mathcal{S} = (s_i)_{i=0}^{\infty}$ with $(s_0, \ldots, s_{N-2}) \ne (a, \ldots, a)$ and $a \in \{0, 1\}$ is the smallest positive integer M such that there is a polynomial $f(x_1, \ldots, x_M) \in \mathbb{F}_2[x_1, \ldots, x_M]$ with

$$s_{i+M} = f(s_i, s_{i+1}, \ldots, s_{i+M-1}), \quad 0 \le i \le N-M-1,$$

see [7, 8, 18]. If $s_i = a$ for $i = 0, \ldots, N-2$, we define

$$M(\mathcal{S}, N) = 0 \quad \text{if } s_{N-1} = a \quad \text{and} \quad M(\mathcal{S}, N) = N-1 \quad \text{if } s_{N-1} \ne a.$$

Obviously, we have

$$M(\mathcal{S}, N) \le L(\mathcal{S}, N).$$

We have $M(\mathcal{S}, N) = L(\mathcal{S}, N) - 1$ for the example (1). However, the expected value of $M(\mathcal{S}, N)$ is of order of magnitude $\log N$, see [7] and also [4, 9, 18], and the expected value of $L(N)$ is $N/2 + O(1)$ by [5]. Hence, the maximum order complexity is a finer measure of pseudorandomness than the linear complexity.

Diem [3] introduced the expansion complexity of the sequence $\mathcal{S}$ as follows. We define the *generating function* $G(x)$ of $\mathcal{S}$ by

$$G(x) = \sum_{i=0}^{\infty} s_i x^i,$$

viewed as a formal power series over $\mathbb{F}_2$. (Note the change by the factor x compared to the definition in [3].) For a positive integer N, the *Nth expansion complexity* $E_N = E_N(\mathcal{S})$ is $E_N = 0$ if $s_0 = \cdots = s_{N-1} = 0$ and, otherwise, the least total degree of a nonzero polynomial $h(x, y) \in \mathbb{F}_2[x, y]$ with

$$h\big(x, G(x)\big) \equiv 0 \bmod x^N.$$

By [15, Theorem 3] we have

$$E(\mathcal{S}, N) \le L(\mathcal{S}, N) + 1$$

and also in [15] examples of sequences $\mathcal{S}$ are given with $E(\mathcal{S}, N)$ substantially smaller than $L(\mathcal{S}, N)$. Hence, the expansion complexity is also a finer measure of pseudorandomness than the linear complexity. In particular, for (ultimately) non-periodic automatic sequences we have seen in [17] that they have bounded expansion complexity but linear complexity of order of magnitude N.

Now, it is a natural question to compare the two finer measures of pseudorandomness, expansion complexity and maximum order complexity. On the one hand, by [15, Theorem 1] for any T-periodic sequence $\mathcal{S}$ and $N > T(T-1)$ we have $E(\mathcal{S}, N) = L(\mathcal{S}, N) + 1$ which has an expected value of order of magnitude T, see for example [14]. On the other hand, the expected value of $M(\mathcal{S}, N)$ is of order of magnitude $\log N$. This might lead to the conjecture that $M(\mathcal{S}, N)$ is a finer measure of pseudorandomness than $E(\mathcal{S}, N)$. However, in this paper we will disprove this conjecture by showing that certain pattern sequences which include the Thue-Morse and the Rudin-Shapiro sequence have bounded expansion complexity but maximum order complexity of the largest possible order of magnitude N. We explain this more precisely in the next subsection.

1.2. Results of this paper

The *Thue-Morse sequence* $\mathcal{T} = (t_i)_{i=0}^{\infty}$ over $\mathbb{F}_2$ is defined by

$$t_i = \begin{cases} t_{i/2} & \text{if } \ i \text{ is even,} \\ t_{(i-1)/2} + 1 & \text{if } \ i \text{ is odd,} \end{cases} \qquad i = 1, 2, \ldots \tag{2}$$

with initial value $t_0 = 0$. In other words t_i is the parity of the sum of digits of i. Taking

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

its generating function $G(x)$ satisfies $h\big(x, G(x)\big) = 0$ and thus

$$E(\mathcal{T}, N) \le 5, \quad N = 1, 2, \ldots$$

Theorem 1 below gives an explicit formula for $M(\mathcal{T}, N)$ of order of magnitude N.

More generally, for a positive integer k we study the *pattern sequence* $\mathcal{P}_k = (p_i)_{i=0}^{\infty}$ over $\mathbb{F}_2$ defined by

$$p_i = \begin{cases} p_{\lfloor i/2 \rfloor} + 1 & \text{if } \ i \equiv -1 \mod 2^k, \\ p_{\lfloor i/2 \rfloor}, & \text{otherwise,} \end{cases} \qquad i = 1, 2, \ldots \tag{3}$$

with the initial value $p_0 = 0$.

In other words, p_i is the parity of the number of occurences of the all one pattern of length k in the binary expansion of i. For $k = 1$ we get the Thue-Morse sequence and for $k = 2$ the *Rudin-Shapiro sequence*.

Taking

$$h(x, y) = (x + 1)^{2^k+1}y^2 + (x + 1)^{2^k}y + x^{2^k-1}$$

its generating function $G(x)$ satisfies $h\big(x, G(x)\big) = 0$ and thus

$$E(\mathcal{P}_k, N) \le 2^k + 3, \quad N = 1, 2, \dots$$

Theorem 2 below provides an explicit formula for $M(\mathcal{P}_k, N)$ for $k \ge 2$ of order of magnitude N. Note that the case $k = 1$ is slightly different than the case $k \ge 2$.

In Section 2, we study the maximum order complexity of the Thue-Morse sequence, that is, $\mathcal{P}_1$ and in Section 3, of $\mathcal{P}_k$ for $k \ge 2$.

2. Thue-Morse sequence

Theorem 1. *For $N \ge 4$, the Nth maximum order complexity of the Thue-Morse sequence $\mathcal{T}$ satisfies*

$$M(\mathcal{T}, N) = 2^\ell + 1,$$

where

$$\ell = \left\lceil \frac{\log(N/5)}{\log 2} \right\rceil.$$

P r o o f. For $N = 4, 5, 6$ the result is easy to verify.

By the monotony of the maximum order complexity it is enough to show

$$M(\mathcal{T}, 5 \cdot 2^{\ell-1} + 1) \ge 2^\ell + 1 \ge M(\mathcal{T}, 5 \cdot 2^\ell) \quad \text{for } \ell = 1, 2, \dots$$

From Proposition 3.1 in [7], if t be the length of the longest subsequence of $\mathcal{T}$ that occurs at least twice with different successors, then $\mathcal{T}$ has the maximum order complexity $t + 1$. Hence the first inequality follows from

$$t_i = t_{i+3\cdot 2^{\ell-1}} \quad \text{for } i = 0, 1, \dots, 2^\ell - 1 \quad \text{and} \quad t_{2^\ell} \ne t_{5\cdot 2^{\ell-1}}, \quad \ell = 1, 2, \dots \tag{4}$$

which we show by induction over ℓ below. More precisely, if there was a recurrence of length 2^ℓ for the first $5 \cdot 2^{\ell-1} + 1$ sequence elements,

$$t_{i+2^\ell} = f(t_i, \dots, t_{i+2^{\ell-1}}), \quad 0 \le i \le 3 \cdot 2^{\ell-1},$$

then from $(t_0, \dots, t_{2^\ell-1}) = (t_{3\cdot 2^{\ell-1}}, \dots, t_{5\cdot 2^{\ell-1}-1})$ we would get $t_{2^\ell} = t_{5\cdot 2^{\ell-1}}$, a contradiction to (4).

For $\ell = 1$ the assertion (4) is obviously true and we may assume $\ell \geq 2$. For even i we get by (2) and induction

$$t_i = t_{i/2} = t_{i/2+3\cdot 2^{\ell-2}} = t_{i+3\cdot 2^{\ell-1}}, \quad i = 0, 2, \ldots, 2^\ell - 2.$$

For odd i we get

$$t_i = t_{(i-1)/2} + 1 = t_{(i-1)/2+3\cdot 2^{\ell-2}} + 1 = t_{i+3\cdot 2^{\ell-1}}, \quad i = 1, 3, \ldots, 2^\ell - 1.$$

Moreover,

$$t_{2^\ell} = t_{2^{\ell-1}} \neq t_{5\cdot 2^{\ell-2}} = t_{5\cdot 2^{\ell-1}}.$$

Now, we prove $M(\mathcal{T}, 5 \cdot 2^\ell) \leq 2^\ell + 1$ for $\ell = 1, 2, \ldots$ In other words, we have to show that for any $\ell = 1, 2, \ldots$, if for some $0 \leq j < k \leq 2^{\ell+2} - 2$ we have

$$t_{i+j} = t_{i+k} \quad \text{for } i = 0, 1, \ldots, 2^\ell, \tag{5}$$

then we also have

$$t_{2^\ell+1+j} = t_{2^\ell+1+k}.$$

This can be easily verified for $\ell = 1$ and we may assume $\ell \geq 2$.

First, we note that $(t_j, t_{j+1}, t_{j+2}, t_{j+3})$ is of the form $(x, x+1, y, y+1)$ if j is even since $t_{2m+1} = t_m + 1 = t_{2m} + 1$ and either of the form $(x, x, x+1, y)$ for $j \equiv 1 \mod 4$ or $(x, y, y+1, y+1)$ for $j \equiv 3 \mod 4$ since $t_{4m+1} = t_m + 1 = t_{4m+2}$ and $t_{4m+3} = t_m = t_{4m}$. Hence, $(t_j, t_{j+1}, t_{j+2}, t_{j+3}) = (t_k, t_{k+1}, t_{k+2}, t_{k+3})$ implies $j \equiv k \bmod 2$.

If j and k are both even, then from (2) and (5) with $i = 2^\ell$ we get

$$t_{2^\ell+1+j} = t_{2^{\ell-1}+j/2} + 1 = t_{2^\ell+j} + 1 = t_{2^\ell+k} + 1 = t_{2^\ell+k+1}.$$

If j and k are both odd, then (5) implies for any even i

$$t_{i/2+(j-1)/2} = t_{i+j} + 1 = t_{i+k} + 1 = t_{i/2+(k-1)/2} \quad \text{for } i = 0, 2, \ldots, 2^\ell$$

and by induction

$$t_{2^\ell+1+j} = t_{2^{\ell-1}+(j+1)/2} = t_{2^{\ell-1}+(k+1)/2} = t_{2^\ell+1+k},$$

which completes the proof. □

Remark 1. It is easy to see that

$$\frac{N}{5} + 1 \leq M(\mathcal{T}, N) \leq 2\frac{N-1}{5} + 1 \quad \text{for } N \geq 4$$

and

$$M(\mathcal{T}, 1) = 0, \quad M(\mathcal{T}, 2) = M(\mathcal{T}, 3) = 1.$$

3. Pattern sequences

Theorem 2. *For $k \geq 2$ and $N \geq 2^{k+3}-7$, the Nth maximum order complexity of the pattern sequence $\mathcal{P}_k$ satisfies*

$$M(\mathcal{P}_k, N) = (2^{k-1}-1)2^{\ell}+1,$$

where

$$\ell = \left\lceil \frac{\log(N/(2^k-1))}{\log 2} \right\rceil - 1.$$

P r o o f. By the monotony of the maximum order complexity it is enough to show

$$M\big(\mathcal{P}_k, (2^k-1)2^{\ell}+1\big) \geq (2^{k-1}-1)2^{\ell}+1 \geq M\big(\mathcal{P}_k, (2^k-1)2^{\ell+1}\big) \quad \text{for} \quad \ell \geq 3.$$

From Proposition 3.1 in [7], the first inequality follows from

$$p_i = p_{i+2^{\ell+k-1}} \quad \text{for} \quad i = 0, 1, \ldots, (2^{k-1}-1)2^{\ell}-1 \tag{6}$$

and

$$p_{(2^{k-1}-1)2^{\ell}} \neq p_{(2^k-1)2^{\ell}}$$

for $\ell \geq 0$, which we show by induction over ℓ. For $\ell = 0$ the assertion is obviously true since $p_i = 0$ for $i = 0, 1, \ldots, 2^k-2$ and $p_{2^k-1} = 1$ by (3). We may assume $\ell \geq 1$. For even i we get from (3) and induction

$$p_i = p_{i/2} = p_{i/2+2^{\ell+k-2}} = p_{i+2^{\ell+k-1}}, \quad i = 0, 2, \ldots, (2^{k-1}-1)2^{\ell}-2. \tag{7}$$

For odd i we get from (3)

$$p_i = \begin{cases} p_{i-1} & \text{if } i \not\equiv -1 \bmod 2^k, \\ p_{i-1}+1 & \text{if } i \equiv -1 \bmod 2^k, \end{cases} \qquad i = 1, 3, \ldots \tag{8}$$

Now fix any odd $i = 1, 3, \ldots, (2^{k-1}-1)2^{\ell}-1$. If $i \not\equiv -1 \bmod 2^k$, then we get from (7) and (8)

$$p_i = p_{i-1} = p_{i-1+2^{\ell+k-1}} = p_{i+2^{\ell+k-1}}.$$

If $i \equiv -1 \bmod 2^k$, then

$$p_i = p_{i-1}+1 = p_{i-1+2^{\ell+k-1}}+1 = p_{i+2^{\ell+k-1}}.$$

Moreover,

$$p_{(2^{k-1}-1)2^{\ell}} = p_{(2^{k-1}-1)2^{\ell-1}} \neq p_{(2^k-1)2^{\ell-1}} = p_{(2^k-1)2^{\ell}} \quad \text{by induction.}$$

Now, we prove $M\big(\mathcal{P}_k, (2^k-1)2^{\ell+1}\big) \leq (2^{k-1}-1)2^{\ell}+1$ for $\ell \geq 3$.

That is, we have to show for any $\ell \geq 3$ that, if for some $0 \leq j < n \leq (3 \cdot 2^{k-1}-1)2^{\ell}-2$ we have

$$p_{i+j} = p_{i+n} \quad \text{for } i = 0, 1, \ldots, (2^{k-1}-1)2^{\ell}, \tag{9}$$

then we also have

$$p_{(2^{k-1}-1)2^{\ell}+1+j} = p_{(2^{k-1}-1)2^{\ell}+1+n}. \tag{10}$$

First, we observe that (9) implies $j \equiv n \bmod 2^k$: We choose any m_1, m_2 with

$$n + m_1 \equiv 2^k - 1 \bmod 2^{k+1} \quad \text{and} \quad n + m_2 \equiv -1 \bmod 2^{k+1}$$

and see that

$$n + m_1 \equiv n + m_2 \equiv -1 \bmod 2^k, \quad (n + m_1 - 1)/2 \equiv 2^{k-1} - 1 \bmod 2^k$$

and

$$(n + m_2 - 1)/2 \equiv -1 \bmod 2^k.$$

If $j \equiv n \bmod 2$, then $j + m_1 \equiv 1 \bmod 2$. Moreover, we assume $1 \le m_1 \le 2^{k+1}$ in this case. Now (9) with $i \in \{m_1, m_1 - 1\}$ and (8) imply $p_{j+m_1} = p_{n+m_1} = p_{n+m_1-1} + 1 = p_{j+m_1-1} + 1$ and from (8) again we get $j + m_1 \equiv -1 \bmod 2^k$ and thus $j \equiv n \bmod 2^k$ in this case.

If $j \not\equiv n \bmod 2$, we assume $2 \le m_1, m_2 \le 2^{k+1} + 1$. Then from (9) with $i \in \{m_1 - 1, m_1 - 2\}$, (3) and (8) we get $p_{j+m_1-1} = p_{n+m_1-1} = p_{(n+m_1-1)/2} = p_{(n+m_1-3)/2} = p_{n+m_1-3} = p_{n+m_1-2} = p_{j+m_1-2}$ implies $j + m_1 - 1 \not\equiv -1 \bmod 2^k$. However, $p_{j+m_2-1} = p_{n+m_2-1} = p_{n+m_2-2} + 1 = p_{j+m_2-2} + 1$ and (8) imply $j + m_2 - 1 \equiv -1 \bmod 2^k$ in contradiction to $m_1 \equiv m_2 \bmod 2^k$.

It remains to show that (9) implies (10) for any $j \equiv n \bmod 2^k$.

- For $j \equiv n \equiv 0 \bmod 2$, (8) and (9) with $i = (2^{k-1}-1)2^\ell$ immediately imply (10).
- For $j \equiv n \equiv 1 \bmod 2$ we prove the assertion by induction.

Note that from (6) we get the last $(2^{k-1} - 1)2^{\ell+1}$ elements from the first ones

$$p_{i+2^{\ell+k}} = p_i \quad \text{for } i = 0, 1, \ldots, (2^{k-1} - 1)2^{\ell+1} - 1.$$

Then for verifying our assertion for $\ell = 3$ we need only the first $3 \cdot 2^{k+2} - 7$ elements of P_k. We use the abbreviation

$$a^t = \underbrace{aa \ldots a}_{t}$$

for the word of t consecutive a and get using (3)

$$\mathcal{P}_2 = \big(0^3 10^2 10^4 1^3 010^3 10^2 101^3 0^3 10^4 10^2 100 \ldots\big),$$

$$\mathcal{P}_3 = \big(0^7 10^6 10^8 10^4 1^2 010^7 10^6 10^8 1^5 0^2 10^8 10^6 10^8 10 \ldots\big),$$

and for $k \ge 4$

$$\mathcal{P}_k = \big(0^{2^k-1} 10^{2^k-2} 10^{2^k} 10^{2^k-4} 1^2 010^{2^k-1} 10^{2^k-2} 10^{2^k} 10^{2^k-8} 1^4 0^2 1$$

$$0^{2^k} 10^{2^k-2} 10^{2^k} 10^{2^k-7} \ldots\big).$$

Note that we have to compare only the patterns of length $(2^{k-1} - 1)2^\ell + 2$ starting with p_j and p_n with $j \equiv n \bmod 2^k$, $j \equiv n \equiv 1 \bmod 2$ and $0 \le j < n \le 2^{k+3}-1$.

Now, we consider $\ell \geq 4$. For even i with $0 \leq i \leq (2^{k-1}-1)2^{\ell}$ we get from (3) and (9)

$$p_{i/2+(j-1)/2} = p_{i/2+(n-1)/2}\,.$$

From the observations above we know that this is only possible if $(j-1)/2 \equiv (n-1)/2 \bmod 2^k$. Either by induction if $(j-1)/2 \equiv (n-1)/2 \equiv 1 \bmod 2$ or using the already above verified result if $(j-1)/2 \equiv (n-1)/2 \equiv 0 \bmod 2$, we get

$$\begin{aligned} p_{(2^{k-1}-1)2^{\ell}+1+j} &= p_{(2^{k-1}-1)2^{\ell-1}+(j+1)/2} \\ &= p_{(2^{k-1}-1)2^{\ell-1}+(n+1)/2} \\ &= p_{(2^{k-1}-1)2^{\ell}+1+n}, \end{aligned}$$

which completes the proof. □

Remark 2. The restriction on N in Theorem 2 is needed. For example, for the Rudin-Shapiro sequence we have

$$M(\mathcal{P}_2, N) = \begin{cases} 0, & 1 \leq N \leq 3, \\ 3, & 4 \leq N \leq 9, \\ 6, & 10 \leq N \leq 24. \end{cases}$$

Remark 3. For $k \geq 2$ and $N \geq 2^{k+3} - 7$ Theorem 2 implies

$$\frac{N}{6} + 1 \leq \frac{2^{k-1}-1}{2^k-1}\frac{N}{2} + 1 \leq M(\mathcal{P}_k, N) \leq \frac{2^{k-1}-1}{2^k-1}(N-1) + 1 < \frac{N+1}{2}.$$

4. Final remarks

The subsequence of the Thue-Morse sequence along $(t_{i^2})_{i=0}^{\infty}$ is not automatic. Hence, its expansion complexity is unbounded. It is shown by the authors in [19] that its Nth maximum order complexity is at least of order of magnitude $N^{1/2}$ and this sequence may be an attractive candidate for cryptographic applications. Pattern sequences along squares are also analyzed in [19].

The correlation measure of order k introduced by Mauduit and Sárközy [12] is another figure of merit which is finer than the linear complexity, see [1]. A cryptographic sequence must have small correlation measure of all orders k up to a sufficiently large k. In [6], the maximum order complexity of a binary sequence was estimated in terms of its correlation measures. Roughly speaking, it was shown that any sequence with small correlation measure up to a sufficiently large order k cannot have very small maximum order complexity. Moreover, the correlation measure of order 2 of both the Thue-Morse sequence and the Rudin-Shapiro sequence of length N is of order of magnitude N, see [13].

The same is true for any pattern sequence, see [16]. Hence, together with the results of this paper we see that the correlation measure of order k is a finer quality measure for cryptographic sequences than the maximum order complexity.

Combining a bound of [2] on the state complexity in terms of the expansion complexity and a bound of [16] on the state complexity in terms of the correlation measure of order 2, we can also estimate the expansion complexity in terms of the correlation measure of order 2.

Furthermore, the maximum order complexity and its connections with the Lempel-Ziv complexity was studied in [10].

In [20], the (periodic) sequences of the largest possible maximum order complexity were classified. However, these sequences are highly predictable and not suitable in cryptography. In [11] and [18], several sequence constructions are given which have very large maximum order complexity but no obvious flaw.

Finally, we mention that although the linear complexity is a weaker quality measure for cryptographic sequences than maximum order complexity as well as correlation measure and expansion complexity, it is still of high practical importance since it is much easier to calculate than all of the finer measures.

Acknowledgements 1. The first author is supported by China Scholarship Council and the National Natural Science Foundation of China Grant 61472120. The second author is partially supported by the Austrian Science Fund FWF, Project P 30405-N32.

REFERENCES

[1] BRANDSTÄTTER, N.—WINTERHOF, A.: *Linear complexity profile of binary sequences with small correlation measure*, Period. Math. Hungar. **52** (2006), 1–8.

[2] BRIDY, A.: *Automatic sequences and curves over finite fields*, Algebra Number Theory **11** (2017), 685–712.

[3] DIEM, C.: *On the use of expansion series for stream ciphers*, LMS J. Comput. Math. **15** (2012), 326–340.

[4] ERDMANN, D.—MURPHY, S.: *An approximate distribution for the maximum order complexity*, Des. Codes Cryptogr. **10** (1997), 325–339.

[5] GUSTAVSON, F. G.: *Analysis of the Berlekamp-Massey linear feedback shift-register synthesis algorithm*, IBM J. Res. Develop. **20** (1976), 204–212.

[6] IŞIK, L.—WINTERHOF, A.: *Maximum-order complexity and correlation measures*, Cryptography **1** (2017), no. 7, 1–5.

[7] JANSEN, C. J. A.: *Investigations on Nonlinear Streamcipher Systems: Construction and Evaluation Methods*, Ph.D. Dissertation, Technical University of Delft, Delft, 1989.

[8] JANSEN, C. J. A.: *The maximum order complexity of sequence ensembles*, In: *Advances in Cryptology—EUROCRYPT '91* (D. W. Davies, ed.), *Lecture Notes in Comput. Sci.* Vol. 547, Springer-Verlag, Berlin, 1991, pp. 153–159.

[9] JANSEN, C. J. A.—BOEKEE; D. E.: *The shortest feedback shift register that can generate a given sequence*, In: *Advances in Cryptology—CRYPTO* (G. Brassard, ed.), *Lecture Notes in Comput. Sci.* Vol. 435, Springer-Verlag, Berlin Heidelberg, 1990, pp. 90–99,

[10] LIMNIOTIS, K.—KOLOKOTRONIS, N.—KALOUPTSIDIS, N.: *On the nonlinear complexity and Lempel-Ziv complexity of finite length sequences*, IEEE Trans. Inform. Theory **53** (2007), 4293–4302.

[11] LUO, Y .—XING, C.—YOU, L.: *Construction of sequences with high nonlinear complexity from function fields*, IEEE Trans. Inform. Theory **63** (2017), 7646–7650..

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

[13] 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.

[14] MEIDL, W .—WINTERHOF, A.: *Linear complexity of sequences and multisequences*. In: *Handbook of finite fields* (G. L. Mullen, D. Panario, eds.), CRC Press, Boca Raton, FL, 2013, 324–336.

[15] MÉRAI, L.—NIEDERREITER, H.—WINTERHOF, A.: *Expansion complexity and linear complexity of sequences over finite fields*, Cryptogr. Commun. **9** (2107), 501–509.

[16] MÉRAI, L.—WINTERHOF, A.: *On the pseudorandomness of automatic sequences*, Cryptogr. Commun. **10** (2018), 1013–1022.

[17] MÉRAI, L.—WINTERHOF, A.: *On the Nth linear complexity of automatic sequences*, J. Number Theory **187** (2018), 415–429.

[18] NIEDERREITER, H.—XING, C.: *Sequences with high nonlinear complexity*, IEEE Trans. Inform. Theory **60** (2014), 6696–6701.

[19] SUN, Z.—WINTERHOF, A.: *On the maximum order complexity of subsequences of the Thue-Morse and Rudin-Shapiro sequence along squares*, Int. J. Comput. Math. Comput. Syst. Theory **4** (2019), 30–36.

[20] SUN, Z.—ZENG, Z.—LI, C.—HELLESETH, T.: *Investigations on periodic sequences with maximum nonlinear complexity*, IEEE Trans. Inform. Theory **63** (2017), 6188–6198.

Received May 30, 2018
Accepted May 17, 2019

Zhimin Sun
Faculty of Mathematics and Statistics
Hubei Key Laboratory of Applied Mathematics
Hubei University
Wuhan, 430062
CHINA
E-mail: zmsun@hubu.edu.cn

Arne Winterhof
Johann Radon Institute for Computational and Applied Mathematics
Altenberger Straße 69
A-4040 Linz
AUSTRIA
E-mail: arne.winterhof@oeaww.ac.at