AIMS Mathematics, 11(7): 20267–20290.
DOI: 10.3934/math.2026823
Received: 03 March 2026
Revised: 13 June 2026
Accepted: 24 June 2026
Published: 09 July 2026

https://www.aimspress.com/journal/Math

Review

A brief view on the linear and 2-adic complexities of pseudorandom binary sequences

Hezheng Lin[1], **Lingmei Xiao**[1,*] **and Zhixiong Chen**[1,2]

[1] Fujian Key Laboratory of Financial Information Processing, Putian University, Putian, Fujian 351100, China

[2] Key Laboratory of Applied Mathematics of Fujian Province University, Putian University, Putian, Fujian 351100, China

* **Correspondence:** Email: xiaolm1996@163.com.

Abstract: In this survey, we review pseudorandom binary sequences generated by linear feedback shift registers (LFSRs) and feedback with carry shift registers (FCSRs), respectively. A natural question is how to determine the size of a register (LFSR or FCSR) that generates a given sequence. It can be transferred mathematically in terms of the theory of formal power series for LFSRs and of 2-adic integers for FCSRs, respectively. Hence, the linear complexity (resp. 2-adic complexity) of an eventually periodic sequence is determined by its rational formal power series (resp. rational 2-adic integer). The Nth linear complexity (resp. Nth 2-adic complexity) of a sequence of length N is the minimal linear complexity (resp. 2-adic complexity) of all eventually periodic sequences which start with the N-length sequence. We present results on the average and asymptotic behavior of finite length and periodic sequences. We also present bounds on the Nth linear complexity (resp. Nth 2-adic complexity) for algebraic sequences which are non-eventually periodic. Our primary goal is to assist cryptographic novices in gaining a better understanding and mastery of the design and analysis of shift register sequences.

Keywords: stream cipher; binary sequence; linear complexity; 2-adic complexity
Mathematics Subject Classification: 94A60

1. Introduction

Pseudorandom sequences are extensively applied in cryptography and communications. A main way to design their generation mechanisms is to utilize shift registers, including linear feedback shift registers (LFSRs), feedback shift registers with carry (FCSRs), and finite automata; see [1–3] and references therein.

Complexity measures are introduced to measure how easy it is to produce pseudorandom sequences using shift registers; see the recent survey [4] for detailed introductions. In this work, we continue the discussion and focus on linear and 2-adic complexities. We explain them from a mathematical viewpoint and help beginning learners better understand the design and analysis of shift register sequences. Specifically, in Section 2, we elaborate on the basic concepts of linear complexity and Nth linear complexity for LFSR sequences and their statistical behaviors. In Section 3, we parallel these discussions (on linear complexity) by examining the corresponding features of 2-adic complexity and Nth 2-adic complexity. We mention a relation between linear/2-adic complexity and maximum-order complexity in Section 4. We summarize the work and introduce some further research issues in Section 5.

Throughout the work, we identify the sequence $\mathcal{S}^\infty = (s_n)_{n=0}^\infty$ for an infinite sequence and $\mathcal{S}^N = (s_n)_{n=0}^{N-1}$ for a finite sequence of length N. An $\mathcal{S}^\infty$ is eventually periodic if there exist t and T such that

$$s_{n+T+t} = s_{n+t}$$

for all $n \geq 0$, where t is the pre-period, and T is the period. In particular, $\mathcal{S}^\infty$ is strictly periodic (or briefly, periodic) if $t = 0$.

2. LFSR and linear complexity

A binary LFSR of length r is a common hardware circuit used to generate binary sequences over the binary field $\mathbb{F}_2 = \{0, 1\}$. As shown in Figure 1, it consists of a series of cells and a predefined feedback network.

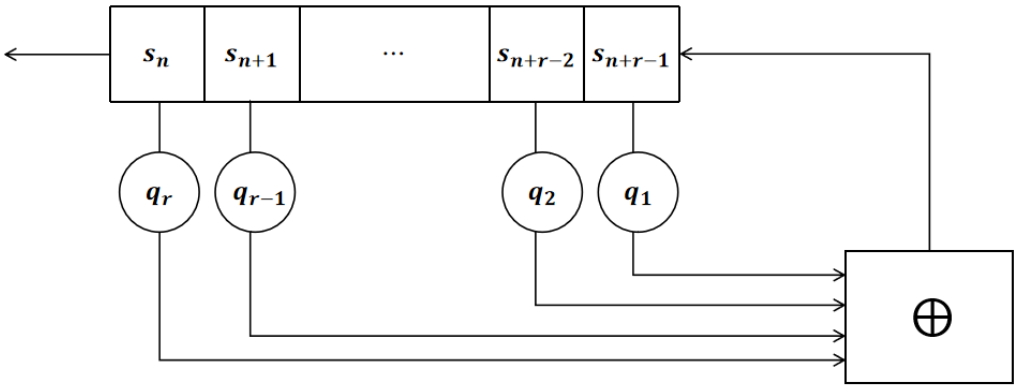

Figure 1. A binary LFSR of length r.

The state change operation is described as follows: The leftmost bit is output, and the new rightmost bit s_{n+r} is computed as a linear combination of the current r bits:

$$s_{n+r} = \sum_{j=1}^{r} q_j s_{n+r-j} \pmod 2, \quad n \geq 0, \tag{2.1}$$

where $q_1, q_2, \ldots, q_r \in \mathbb{F}_2$ are the feedback coefficients. The entire sequence is uniquely determined by the initial state $s_0, s_1, \ldots, s_{r-1}$ and the recurrence. Sequences generated by LFSRs have good statistical properties, and they are hence are widely used in the design of keystream generators for stream ciphers.

Sequences generated by LFSRs are always eventually periodic. To analyze their periodicity, it is convenient to use the tool of generating functions. For a sequence $\mathcal{S}^\infty = (s_n)_{n=0}^\infty$, its generating function is defined as the formal power series

$$G_{\mathcal{S}}(x) = \sum_{n=0}^{\infty} s_n x^n \in \mathbb{F}_2[[x]],$$

where $\mathbb{F}_2[[x]]$ denotes the ring of all formal power series over $\mathbb{F}_2$. The coefficients $q_1, q_2, \ldots, q_r$ in Eq (2.1) define a connection polynomial

$$q(x) = -1 + \sum_{i=1}^{r} q_i x^i \in \mathbb{F}_2[x],$$

where $\mathbb{F}_2[x]$ is the ring of polynomials over $\mathbb{F}_2$. It is known that $\mathcal{S}^\infty$ is eventually periodic if and only if $G_{\mathcal{S}}(x)$ can be expressed as a rational function

$$G_{\mathcal{S}}(x) = \frac{f(x)}{q(x)},$$

where $q(x)$ is exactly the connection polynomial, and $f(x) \in \mathbb{F}_2[x]$ with $\gcd(f(x), q(x)) = 1$. Moreover, $\mathcal{S}^\infty$ is strictly periodic if and only if $\deg(f(x)) < \deg(q(x))$.

Consequently, $\mathcal{S}^\infty$ is aperiodic (i.e., non-eventually periodic) if and only if (iff) $G_{\mathcal{S}}(x)$ is not rational, which is also equivalent to declare that $\mathcal{S}^\infty$ cannot be generated by any LFSRs.

2.1. Linear complexity of eventually periodic sequences

In this subsection, we introduce the linear complexity of infinite binary sequences. It is a fundamental measure of pseudorandomness, indicating how hard a sequence is to generate or reproduce.

Definition 2.1. *The smallest length r of an LFSR that generates $\mathcal{S}^\infty$ is called the linear span, denoted by $LS(\mathcal{S}^\infty)$. If no such LFSR exists, we set $LS(\mathcal{S}^\infty) = \infty$.*

Specifically, a cryptographically strong sequence should have high linear span, whereas one with low linear span can be easily reconstructed and exhibits poor randomness.

The linear span is an engineering notion. It can also be defined mathematically via the formal power series, leading to the concept of "linear complexity".

Definition 2.2. *The linear complexity of $\mathcal{S}^\infty$, denoted by $LC(\mathcal{S}^\infty)$, is defined to be*

$$LC(\mathcal{S}^\infty) = \max\{1 + \deg(f(x)), \deg(q(x))\}$$

if the formal power series $G_{\mathcal{S}}(x) = f(x)/q(x)$ is rational in lowest terms with $f(x), q(x) \in \mathbb{F}_2[x]$, and otherwise, we set $LC(\mathcal{S}^\infty) = \infty$.

We summarize:

Proposition 2.1. *Let $\mathcal{S}^\infty$ be an eventually periodic sequence with the generating function $G_{\mathcal{S}}(x) = f(x)/q(x)$ in lowest terms. If its least pre-period is t, then we have*

$$LC(\mathcal{S}^\infty) = t + \deg(q(x)).$$

Proof. If $t = 0$, then $\mathcal{S}^\infty$ is strictly periodic, and hence, $\deg(f(x)) < \deg(q(x))$. By Definition 2.2, we get $LC(\mathcal{S}^\infty) = \deg(q(x))$.

If $t > 0$, let T be the least period, and it is easy to check that $s_{t-1} \neq s_{t+T-1}$ because t is the least pre-period. We rewrite $G_{\mathcal{S}}(x)$ as the following:

$$\frac{f(x)}{q(x)} = G_{\mathcal{S}}(x) = R(x) + x^t \cdot \frac{S^T(x)}{1 - x^T} = R(x) + x^t \cdot \frac{u(x)}{q(x)} = \frac{R(x)q(x) + x^t \cdot u(x)}{q(x)},$$

where $R(x) = s_0 + \ldots + s_{t-1}x^{t-1}$. We now proceed to discuss the following two cases:

Case 1. If $s_{t-1} = 1$, and $s_{t+T-1} = 0$, then we see that $\deg(R(x)) = t-1$, and $\deg(u(x)) \leq \deg(q(x))-2$, as $\deg(S^T(x)) \leq T - 2$. We therefore have

$$\begin{aligned} \deg(f(x)) &= \deg\left(R(x)q(x) + x^t \cdot u(x)\right) \\ &= \max\left\{\deg(R(x)) + \deg(q(x)), t + \deg(u(x))\right\} \\ &= t - 1 + \deg(q(x)), \end{aligned}$$

which implies the desired result by Definition 2.2.

Case 2. If $s_{t-1} = 0$, and $s_{t+T-1} = 1$, then we see that $\deg(R(x)) \leq t-2$, and $\deg(u(x)) = \deg(q(x))-1$, as $\deg(S^T(x)) = T - 1$. We then have

$$\deg(f(x)) = \max\left\{\deg(R(x)) + \deg(q(x)), t + \deg(u(x))\right\} = t + \deg(q(x)) - 1,$$

which also leads to the desired result. □

From the proof of Proposition 2.1, we see that $q(x)$ is a divisor of $x^T - 1$ if T is the period of $\mathcal{S}^\infty$. We therefore have the following corollary:

Corollary 2.1. *Let $\mathcal{S}^\infty$ be an eventually periodic sequence with least pre-period t and least period T. Then $LS(\mathcal{S}^\infty) = LC(\mathcal{S}^\infty)$, and*

$$LC(\mathcal{S}^\infty) \leq t + T.$$

Proof. By Definition 2.1, we see that $LS(\mathcal{S}^\infty)$ is the shortest length of the LFSR, and it exactly equals $t + \deg(q(x))$, which is $LC(\mathcal{S}^\infty)$. □

Under the same conditions, if we set $S^T(x) = s_t + s_{t+1}x + \ldots + s_{t+T-1}x^{T-1}$, then the linear complexity can also be computed via Proposition 2.1 as

$$LC(\mathcal{S}^\infty) = t + T - \deg\left(\gcd\left(x^T - 1, S^T(x)\right)\right).$$

The discrete Fourier transform can also be used to compute the value of linear complexity; see, for example, [5, 6].

Example 2.1. *Consider the eventually periodic sequence $\mathcal{S}^\infty = 0010(01)^\infty$ with pre-period $t = 4$ and period $T = 2$. Its generating function is*

$$G_{\mathcal{S}}(x) = x^2 + x^4 \cdot \frac{x}{x^2 - 1} = \frac{x^5 + x^4 - x^2}{x^2 - 1}.$$

Then $\deg(f(x)) = 5$, $\deg(q(x)) = 2$, *and*

$$LC(\mathcal{S}^\infty) = 6 = 1 + \deg(f(x)) = 4 + \deg(q(x)).$$

2.2. Nth linear complexity of sequences of length N

In practical applications, such as stream cipher systems, we often deal with finite keystream sequences. A (finite) sequence that is highly predictable and easy to reconstruct poses serious security risks. This motivates us to consider the Nth linear span/complexity of a length-N sequence.

Definition 2.3. *The smallest length of an LFSR that generates a finite sequence $\mathcal{S}^N$ is called the Nth linear span, denoted by $LS(\mathcal{S}^N, N)$.*

For $\mathcal{S}^\infty$, we set $LS(\mathcal{S}^\infty, N) = LS(\mathcal{S}^N, N)$, where $\mathcal{S}^N$ is the first N terms of $\mathcal{S}^\infty$. The sequence $LS(\mathcal{S}^\infty, 1), LS(\mathcal{S}^\infty, 2), \ldots$ is the linear span profile of $\mathcal{S}^\infty$.

For $\mathcal{S}^\infty$ with $LS(\mathcal{S}^\infty) = \infty$, considering $LS(\mathcal{S}^\infty, N)$ is particularly necessary.

The quantity $LS(\mathcal{S}^N, N)$ also admits an equivalent mathematical formulation, in which case, it is called the Nth linear complexity, denoted by $LC(\mathcal{S}^N, N)$. By Definition 2.3, any LFSR that generates the first N terms can produce an eventually periodic sequence. Therefore, the Nth linear complexity is naturally formalized as follows

Definition 2.4. *The Nth linear complexity $LC(\mathcal{S}^N, N)$ of $\mathcal{S}^N$ is the minimal value of*

$$\left\{ LC(\mathcal{R}^\infty) : \mathcal{R}^\infty = (r_n)_{n=0}^\infty \text{ with } G_{\mathcal{R}}(x) = \frac{f(x)}{q(x)} \text{ and } r_n = s_n, \text{ for } 0 \le n < N \right\},$$

where $f(x), q(x) \in \mathbb{F}_2[x]$, and $\gcd(f(x), q(x)) = 1$.

Clearly, for any $\mathcal{S}^N$,

$$LC(\mathcal{S}^N, N) = \min_{\mathcal{R}^\infty \in \Delta} LC(\mathcal{R}^\infty) = LS(\mathcal{S}^N, N),$$

where Δ denotes the set of eventually periodic sequences whose first N terms coincide with $\mathcal{S}^N$. We emphasize that the Nth linear complexity measures the pseudorandomness of a length-N binary sequence by comparing it with eventually periodic sequences.

To compute the Nth linear complexity, we need to find a pair $(f(x), q(x))$ satisfying

$$q(x) \cdot \sum_{j=0}^{N-1} s_j x^j \equiv f(x) \pmod{x^N}, \tag{2.2}$$

where $q(x) \equiv 1 \pmod{x}$. By taking $q(x) = 1$ and $f(x) = \sum_{j=0}^{N-1} s_j x^j$ in Eq (2.2), we obtain $0 \le LC(\mathcal{S}^N, N) \le N$. Moreover, $LC(\mathcal{S}^\infty, N) \le LC(\mathcal{S}^\infty, N+1)$ holds because any LFSR that generates the first $N+1$ terms of $\mathcal{S}^\infty$ also generates the first N terms. In particular:

For $\mathcal{S}^\infty$, the linear complexity is related to its Nth linear complexity by

$$LC(\mathcal{S}^\infty) = \sup_{N \ge 1} LC(\mathcal{S}^\infty, N).$$

This implies that $LC(\mathcal{S}^\infty)$ is finite if $\mathcal{S}^\infty$ is eventually periodic, and $LC(\mathcal{S}^\infty) = \infty$ otherwise. For the former, we have the following:

Proposition 2.2. *Let $\mathcal{S}^\infty$ be an eventually periodic sequence with linear complexity L. Then for every $N \ge 2L - 1$,*

$$LC(\mathcal{S}^\infty) = LC(\mathcal{S}^\infty, N).$$

Proof. We suppose that $LC(\mathcal{S}^\infty, 2L-1) < L$. By a result of Massey (see [7, Theorem 2]) with

$$LC(\mathcal{S}^\infty, N+1) \in \{LC(\mathcal{S}^\infty, N), N+1-LC(\mathcal{S}^\infty, N)\}, \tag{2.3}$$

we always have $LC(\mathcal{S}^\infty, 2L) < L$ because $2L - LC(\mathcal{S}^\infty, 2L-1) > L$. Then, using Eq (2.3) repeatedly, we have

$$LC(\mathcal{S}^\infty, N) < L \text{ for } N \geq 2L,$$

a contradiction to $LC(\mathcal{S}^\infty) = L$. □

We remark that the proof of Proposition 2.2 is mentioned by one of the reviewers by Eq (2.3) so as to shorten the proof.

Example 2.2. *Consider the eventually periodic sequence* $\mathcal{S}^\infty = 1100(01)^\infty$ *with pre-period* $t = 4$ *and period* $T = 2$. *The* N*th linear complexity of* $\mathcal{S}^\infty$ *is*

$$\begin{aligned}
&LC(\mathcal{S}^\infty, 1) = LC(\mathcal{S}^\infty, 2) = 1;\\
&LC(\mathcal{S}^\infty, 3) = LC(\mathcal{S}^\infty, 4) = LC(\mathcal{S}^\infty, 5) = 2;\\
&LC(\mathcal{S}^\infty, 6) = LC(\mathcal{S}^\infty, 7) = LC(\mathcal{S}^\infty, 8) = 4;\\
&LC(\mathcal{S}^\infty, 9) = LC(\mathcal{S}^\infty, 10) = 5;\\
&LC(\mathcal{S}^\infty, N) = 6,\ N \geq 11.
\end{aligned}$$

That is, $LC(\mathcal{S}^\infty) = LC(\mathcal{S}^\infty, N) = 6$ *for all* $N \geq 11$ (*note that* $11 = 2L - 1$).

Example 2.3. *Consider the eventually periodic sequence* $\mathcal{S}^\infty = 0010(1)^\infty$ *with pre-period* $t = 4$ *and period* $T = 1$. *The* N*th linear complexity of* $\mathcal{S}^\infty$ *is*

$$\begin{aligned}
&LC(\mathcal{S}^\infty, 1) = LC(\mathcal{S}^\infty, 2) = 0;\\
&LC(\mathcal{S}^\infty, 3) = LC(\mathcal{S}^\infty, 4) = LC(\mathcal{S}^\infty, 5) = LC(\mathcal{S}^\infty, 6) = LC(\mathcal{S}^\infty, 7) = 3;\\
&LC(\mathcal{S}^\infty, N) = 5,\ N \geq 8.
\end{aligned}$$

That is, $LC(\mathcal{S}^\infty) = LC(\mathcal{S}^\infty, N) = 5$ *for all* $N \geq 8$ (*note that* $8 < 2L - 1$).

The (Nth) linear complexity L can be computed efficiently using the Berlekamp–Massey (BM) algorithm [7]. Only $2L$ consecutive bits are needed to fully reconstruct the whole sequence. Therefore, for a cryptographically strong sequence, L should be as large as possible. In particular, it should be at least half of the sequence's length (or half of its period).

2.3. Average and asymptotic behavior of linear complexity

We review the expected Nth linear complexity for binary sequences of length N and the expected linear complexity for binary sequences of period T, respectively, as well as the asymptotic behavior of the Nth linear complexity for aperiodic sequences as N grows.

For finite sequences of length N, Rueppel [8] proved that the expected value of the Nth linear complexity is given by

$$E_N^{\text{linear}} := \frac{1}{2^N} \sum_{\mathcal{S}^N \in \mathbb{F}_2^N} LC(\mathcal{S}^N, N) = \frac{N}{2} + O(1),$$

or exactly

$$E_N^{\text{linear}} = \frac{N}{2} + c_N \text{ with } 0 \le c_N \le \frac{5}{18}.$$

The variance of the Nth linear complexity, defined as

$$V_N^{\text{linear}} := \frac{1}{2^N} \sum_{\mathcal{S}^N \in \mathbb{F}_2^N} \left(LC(\mathcal{S}^N, N)\right)^2 - \left(E_N^{\text{linear}}\right)^2$$

is proved to be

$$\lim_{N\to\infty} V_N^{\text{linear}} = \frac{86}{81}.$$

Details can be found in [8, Propositions 4.2 and 4.3]; see also a recent survey [4].

Niederreiter [9, 10] proved that for varying N with probability 1,

$$LC(\mathcal{S}^\infty, N) = \frac{N}{2} + O\left(\log(N)\right) \quad \text{for } N \ge 2$$

for a random $\mathcal{S}^\infty$.

These results provide a fine theoretical basis for the assessment of sequence randomness and give rise to the notion of a sequence with a perfect linear complexity profile (PLCP). An $\mathcal{S}^\infty$ is said to have a PLCP if $LC(\mathcal{S}^\infty, N) = \lceil N/2 \rceil$ for $N \ge 1$, which is called a perfect sequence.

It was proved by Wang and Massey [11] that $\mathcal{S}^\infty = (s_n)_{n=0}^\infty$ has a PLCP if and only if

$$s_0 = 1 \text{ and } s_{2n+2} = s_{2n+1} + s_n, \text{ for } n = 0, 1, \ldots, \tag{2.4}$$

which is also called apwenian; see [12, Example 8], and for further discussions, see [13, 14] and the recent master's thesis [15]. This is a sequence whose linear complexity profile follows the expected behavior of random sequences as closely as possible. More generally, a sequence has a d-perfect linear complexity profile (d-PLCP) if

$$\left| LC(\mathcal{S}^\infty, N) - \frac{N}{2} \right| \le \frac{d}{2} \text{ for all } N \ge 1,$$

where d is a positive integer. A perfect sequence corresponds to the case $d = 1$. Generally, any sequence with a d-PLCP is called a sequence with an almost PLCP. With the help of continued fractions, Niederreiter (partly with other co-authors) proved that the generating function $G_{\mathcal{S}}(x)$ of a d-perfect sequence $\mathcal{S}^\infty$ is irrational and that the partial quotients A_j in the continued fraction expansion of $G_{\mathcal{S}}(x)$ satisfy $\deg(A_j) \le d$ for all $j \ge 1$; see [14, 16, 17]. Sequences with d-PLCP were constructed using curves over finite fields [18].

The expected linear complexity of binary periodic sequences $\mathcal{S}^\infty$ with period T, denoted by

$$E_T^{\text{linear}} := \frac{1}{2^T} \sum_{T-\text{periodic}\mathcal{S}^\infty \in \mathbb{F}_2^\infty} LC(\mathcal{S}^\infty),$$

is categorized based on the form of T:

- If $T = 2^k$ for some positive integer k, Rueppel [8, Proposition 4.6] proved that

$$E_T^{\text{linear}} = T - 1 + 2^{-T}.$$

- If $T = 2^k w$ for some positive integer k and odd w, the expected linear complexity is formulated in [19] and has a lower bound

$$E_T^{\text{linear}} \geq \begin{cases} T - \frac{w+2}{3}, & \text{if } k > 0, \\ \frac{3T-1}{4}, & \text{if } k = 0, \end{cases}$$

  which is derived from the study on q-ary sequences; see more details in [16, 19] or a recent survey [4].

2.4. Linear complexity of automatic sequences

Let $\mathbb{F}_2(x)$ be the fractional field (or field of rational functions) of the ring of polynomials $\mathbb{F}_2[x]$. Any element in $\mathbb{F}_2(x)$ is of the form $f(x)/q(x)$ for $f(x), q(x) \in \mathbb{F}_2[x]$ with $q(x) \neq 0$.

For an $\mathcal{S}^\infty$, its generating function $G_{\mathcal{S}}(x)$ is algebraic over $\mathbb{F}_2(x)$ (or $\mathbb{F}_2[x]$) if there exists a nonzero polynomial $h(y) \in \mathbb{F}_2[x][y]$ such that $h(G_{\mathcal{S}}(x)) = 0$, where $h(y)$ is of the form

$$h(y) = \sum_{i=0}^{d} a_i(x) y^i, \quad a_i(x) \in \mathbb{F}_2[x].$$

Otherwise, $G_{\mathcal{S}}(x)$ is transcendental over $\mathbb{F}_2(x)$. Clearly, $G_{\mathcal{S}}(x) = f(x)/q(x)$ is algebraic for any eventually periodic sequences, as $h(y) = q(x)y - f(x)$, and $h(G_{\mathcal{S}}(x)) = 0$.

Automatic sequences, such as the Thue–Morse and Rudin–Shapiro sequences, are a family of important sequences generated by finite automata; see [1] or the recent survey [12]. They can be characterized by the algebraicity of their generating functions. More precisely, an $\mathcal{S}^\infty$ is automatic over $\mathbb{F}_2$ iff its $G_{\mathcal{S}}(x)$ is algebraic. To measure how difficult it is to produce a sequence via a finite automaton, the notions of automatic complexity [20–22] and state complexity [12, 23] have been introduced.

Question 2.1. *Consider the state complexity of sequences and the relation between the state complexity and the linear complexity.*

Merai and Winterhof [24] proved the following:

Proposition 2.3. *Let $\mathcal{S}^\infty$ be an aperiodic. Let $h(y) = h_0(x) + h_1(x)y + \ldots + h_d(x)y^d \in \mathbb{F}_2[x][y]$ be a non-zero polynomial of degree d in y with no rational zero and $h(G_{\mathcal{S}}(x)) = 0$. Put*

$$M = \max_{0 \leq i \leq d} \{\deg(h_i(x)) - i\}.$$

Then for $N \geq 1$, we have

$$\frac{N - M}{d} \leq LC(\mathcal{S}^\infty, N) \leq \frac{(d-1)N + M + 1}{d}.$$

Consequently, for any $\mathcal{S}^\infty$ whose generating function is a root of an irreducible polynomial $h(y) \in \mathbb{F}_2[x][y]$ of degree $d = 2$ in y, the Nth linear complexity grows roughly as $N/2$, which is typical for random sequences. This includes several well-known automatic sequences:

- Thue–Morse sequence: $h(y) = (x+1)^3 y^2 + (x+1)^2 y + x$;

- Rudin–Shapiro sequence: $h(y) = (x+1)^5y^2 + (x+1)^4y + x^3$;
- paper-folding sequence: $h(y) = (x+1)^4(y^2+y) + x$;
- apwenian sequence in Eq (2.4) with $s_{2n} = 1$ for $n \geq 0$: $h(y) = (x+1)(xy^2+y) + 1$.

See details in [12, Example 9].

The algebraicity of $G_{\mathcal{S}}(x)$ leads to a new notion of the expansion complexity of $\mathcal{S}^\infty$ [25]. Precisely speaking, the expansion complexity of a non-all-zero $\mathcal{S}^\infty$, denoted by $E(\mathcal{S}^\infty)$, is defined to be the least total degree of $h(y)$ with $h(G_{\mathcal{S}}(x)) = 0$,

$$E(\mathcal{S}^\infty) = \max\{i + \deg(a_i(x)) : 0 \leq i \leq d\}.$$

We restrict $E(0^\infty) = 0$ and $E(\mathcal{S}^\infty) = \infty$ if $G_{\mathcal{S}}(x)$ is transcendental. Many automatic sequences such as the Thue–Morse and Rudin–Shapiro sequences mentioned above have low expansion complexity and hence have a strong nonrandomness property; see [12].

Although $E(\mathcal{S}^\infty)$ characterizes the global property of $\mathcal{S}^\infty$, it is necessary to consider the growth of its finite analog at length N. Accordingly, the Nth expansion complexity, denoted by $E(\mathcal{S}^\infty, N)$ or $E(\mathcal{S}^N, N)$, is introduced. For $\mathcal{S}^\infty$ whose first N terms are not all zero, $E(\mathcal{S}^\infty, N)$ is defined as the least total degree of a nonzero $h(y) \in \mathbb{F}_2[x][y]$ satisfying

$$h(G_{\mathcal{S}}(x)) \equiv 0 \pmod{x^N}. \tag{2.5}$$

By [26, Proposition 2], when $E(\mathcal{S}^\infty, N) \geq 1$,

$$E(\mathcal{S}^\infty, N) \leq E(\mathcal{S}^\infty, N+1) \leq 1 + E(\mathcal{S}^\infty, N).$$

If the polynomial $h(y)$ satisfying Eq (2.5) is restricted to be irreducible, this constraint leads to the Nth i-expansion complexity, denoted by $E^*(\mathcal{S}^\infty, N)$. We then have

$$E^*(\mathcal{S}^\infty, N) \leq N - 1 \quad \text{and} \quad E(\mathcal{S}^\infty, N) \leq E^*(\mathcal{S}^\infty, N) \leq E^*(\mathcal{S}^\infty, N+1).$$

For detailed study of the expansion complexity, we refer the reader to [25, 27–29].

Question 2.2. *It is interesting to consider the Nth expansion complexity of sequences and the average behavior as the Nth linear complexity.*

3. FCSR and 2-adic complexity

In order to strengthen the feedback mechanism in LFSRs, Goresky and Klapper created another structure by introducing integer addition with carry and proposed a new register called feedback with carry shift register (FCSR) in 1990s [3, 30]. The structure of an FCSR is illustrated in Figure 2.

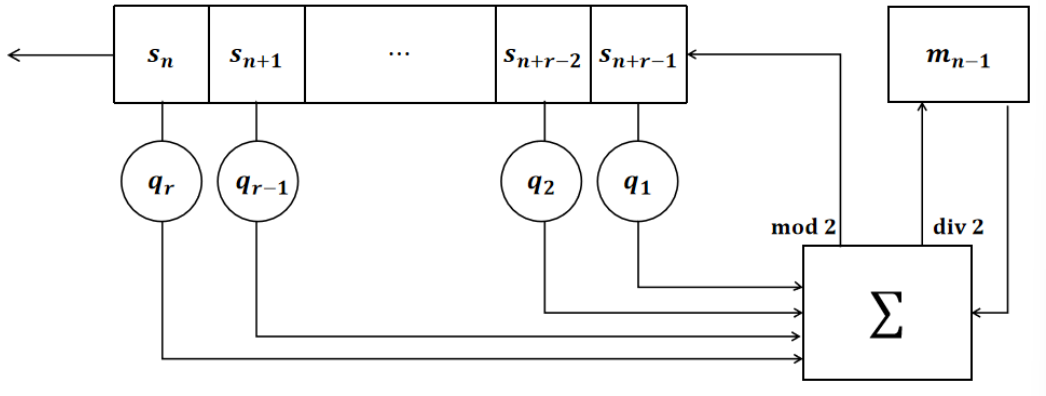

Figure 2. A binary FCSR of length r.

In fact, an additional memory (for carry) is embedded into the LFSR architecture. For binary FCSRs, the state recurrence follows the relation

$$s_{n+r} + 2m_n = \sum_{j=1}^{r} q_j s_{n+r-j} + m_{n-1}, \quad n \geq 0, \tag{3.1}$$

where $q_1, q_2, \ldots, q_r \in \{0, 1\}$ are the feedback coefficients, and m_{-1} is an initial value. The coefficients in Eq (3.1) define an integer

$$q = -1 + q_1 2 + q_2 2^2 + \ldots + q_r 2^r \in \mathbb{Z},$$

which is called a connection integer of the FCSR. It is clear that any sequences generated by FCSRs are eventually periodic.

For any $\mathcal{S}^\infty = (s_n)_{n=0}^\infty$, its 2-adic integer is given by

$$G_{\mathcal{S}}(2) = \sum_{n=0}^{\infty} s_n 2^n \in \mathbb{Z}_2,$$

where $\mathbb{Z}_2$ is the ring of 2-adic integers of the form $\sum_{n=0}^\infty a_n 2^n$ with $a_n \in \{0, 1\}$ for $n \geq 0$.

For a positive integer T, the equation

$$\sum_{n=0}^{\infty} 2^{nT} - 2^T \sum_{n=0}^{\infty} 2^{nT} = 1$$

implies that

$$\sum_{n=0}^{\infty} 2^{nT} = \frac{1}{1 - 2^T}.$$

Hence, it is easy to check that an $\mathcal{S}^\infty$ is eventually periodic if and only if $G_{\mathcal{S}}(2)$ is a rational number. Moreover, $\mathcal{S}^\infty$ is strictly periodic if and only if $G_{\mathcal{S}}(2) \in \mathbb{Q} \cap [-1, 0]$. In particular, if we suppose that $\mathcal{S}^\infty$ is eventually periodic with pre-period t and period T, and $G_{\mathcal{S}}(2) = f/q$ with $f, q \in \mathbb{Z}$ and $\gcd(f, q) = 1$; we see that q is the connection integer of $\mathcal{S}^\infty$ and $q|(2^T - 1)$.

The discussions above also imply that an $\mathcal{S}^\infty$ is aperiodic iff $G_{\mathcal{S}}(2)$ is irrational iff $\mathcal{S}^\infty$ cannot be generated by any FCSRs.

3.1. 2-Adic complexity of eventually periodic sequences

In this subsection, we recall the concept of 2-adic complexity for infinite binary sequences. This metric measures a sequence's resistance to rational approximation attacks and serves as an important algebraic complement to linear complexity.

An FCSR, as illustrated in Figure 2, consists of a linear register of r cells and a memory for carry. The capacity of this memory depends on the initial value and the maximum possible carry value during the operation.

Definition 3.1. *The number of the least memory plus the smallest length of FCSRs that generate $\mathcal{S}^\infty$ is called the 2-adic span of $\mathcal{S}^\infty$, denoted by $\phi(\mathcal{S}^\infty)$. If $\mathcal{S}^\infty$ cannot be generated by any FCSRs, we set $\phi(\mathcal{S}^\infty) = \infty$.*

The 2-adic span of $\mathcal{S}^\infty$ is an engineering notion that is difficult to determine. A mathematical notion called 2-adic complexity arises via 2-adic integers.

Definition 3.2. *The 2-adic complexity of $\mathcal{S}^\infty$, denoted by $\lambda_2(\mathcal{S}^\infty)$, is defined to be*

$$\lambda_2(\mathcal{S}^\infty) := \log_2 (\max\{|f|, q\}) \in \mathbb{R}$$

if its 2-adic integer $G_S(2) = f/q$ is a rational number in lowest terms, and otherwise, we set $\lambda_2(\mathcal{S}^\infty) = \infty$.

We find that the 2-adic span is an integer, whereas the 2-adic complexity may not be an integer; consequently, $\phi(\mathcal{S}^\infty) = \lambda_2(\mathcal{S}^\infty)$ may not hold. Goresky and Klapper [30] proved the following relation:

Proposition 3.1. *Let $\mathcal{S}^\infty$ be an eventually periodic sequence. We have*

$$|(\lambda_2(\mathcal{S}^\infty) - 2) - \phi(\mathcal{S}^\infty)| \leq \log_2(\phi(\mathcal{S}^\infty)),$$

or

$$|(\lambda_2(\mathcal{S}^\infty) - 2) - \phi(\mathcal{S}^\infty)| \leq \log_2(\lambda_2(\mathcal{S}^\infty) - 2) + 1.$$

Proposition 3.1 indicates that the 2-adic complexity is close to the 2-adic span. Large 2-adic complexity implies large 2-adic span, and vice versa. Therefore, the 2-adic complexity $\lambda_2(\mathcal{S}^\infty)$ is enough to characterize the length of the shortest FCSR that generates $\mathcal{S}^\infty$. Clearly, sequences with low 2-adic complexity can be easily reconstructed and exhibit poor randomness.

Proposition 3.2. *Let $\mathcal{S}^\infty$ be an eventually periodic sequence with least pre-period $t > 0$ and least period T. Then the 2-adic complexity satisfies*

$$\lambda_2(\mathcal{S}^\infty) < t + T.$$

Proof. For $\mathcal{S}^\infty = (s_n)_{n=0}^\infty$, we compute the 2-adic integer

$$G_S(2) = \sum_{i=0}^{t-1} s_i 2^i + 2^t \cdot \frac{S^T(2)}{1 - 2^T} := \frac{A}{2^T - 1},$$

where $S^T(2) = s_t + s_{t+1}2 + \ldots + s_{t+T-1}2^{T-1}$ ($\leq 2^T - 1$). The absolute numerator $|A|$ satisfies

$$\begin{aligned} |A| &= \left|(2^T - 1)\sum_{i=0}^{t-1} s_i 2^i - 2^t \cdot S^T(2)\right| \\ &\leq \max\left\{(2^T - 1)\sum_{i=0}^{t-1} s_i 2^i,\ 2^t \cdot S^T(2)\right\} \\ &\leq 2^t(2^T - 1). \end{aligned}$$

Thus, by Definition 3.2, we derive

$$\lambda_2(\mathcal{S}^\infty) \leq \log_2(2^t(2^T - 1)) < \log_2(2^t \cdot 2^T) = t + T.$$

This completes the proof. □

Finally, for a strictly periodic sequence $\mathcal{S}^\infty$, let $\overleftarrow{\mathcal{S}^\infty}$ denote the sequence written in the reverse order of $\mathcal{S}^\infty$. A sequence $\mathcal{S}^\infty$ with large $\lambda_2(\mathcal{S}^\infty)$ might have low $\lambda_2(\overleftarrow{\mathcal{S}^\infty})$, and vice versa. Therefore, the symmetric 2-adic complexity of $\mathcal{S}^\infty$, denoted by $\overline{\lambda}_2(\mathcal{S}^\infty)$, is defined as

$$\overline{\lambda}_2(\mathcal{S}^\infty) = \min\left\{\lambda_2(\mathcal{S}^\infty), \lambda_2(\overleftarrow{\mathcal{S}^\infty})\right\}.$$

This symmetric 2-adic complexity is a finer measure than the 2-adic complexity.

3.2. Nth 2-Adic complexity of sequences of length N

For $\mathcal{S}^N$, one might similarly consider its Nth 2-adic span and complexity. However, unlike linear complexity, defining the Nth 2-adic span is not straightforward because the memory of the corresponding FCSR may grow during its operation [3, p.328]. Hence, we focus on the Nth 2-adic complexity of finite sequences.

Definition 3.3. *The Nth 2-adic complexity $\lambda_2(\mathcal{S}^N, N)$ of $\mathcal{S}^N$ is the minimal value of*

$$\left\{\lambda_2(\mathcal{R}^\infty) : \mathcal{R}^\infty = (r_n)_{n=0}^\infty \text{ with } G_{\mathcal{R}}(2) = \frac{f}{q} \text{ and } r_n = s_n, \text{ for } 0 \leq n < N\right\},$$

where $f, q \in \mathbb{Z}$, and $\gcd(f, q) = 1$.

We have $\lambda_2(\mathcal{S}^\infty, N) = \lambda_2(\mathcal{S}^N, N)$, where $\mathcal{S}^N$ is the first N elements of $\mathcal{S}^\infty$. The sequence $\lambda_2(\mathcal{S}^\infty, 1), \lambda_2(\mathcal{S}^\infty, 2), \ldots$ is the 2-adic complexity profile of $\mathcal{S}^\infty$.

From Definition 3.3, the Nth 2-adic complexity is a measure for binary sequences of length N by comparison with eventually periodic sequences.

For $\mathcal{S}^\infty$ with $\lambda_2(\mathcal{S}^\infty) = \infty$, similar to the Nth linear span and complexity, it is necessary to consider the Nth 2-adic span and complexity of the first N terms of $\mathcal{S}^\infty$ for $N \geq 1$.

According to Definition 3.3, to compute the Nth 2-adic complexity, we only need to determine the pair (f, q) satisfying

$$q \cdot \sum_{n=0}^{N-1} s_n 2^n \equiv f \pmod{2^N}, \tag{3.2}$$

where q is an odd number. The pair (f, q) coinciding with the Nth 2-adic complexity $\lambda_2(\mathcal{S}^N, N)$ is called a minimal pair of $\mathcal{S}^N$.

It is clear that

$$\lambda_2(\mathcal{S}^N, N) = \min_{\mathcal{R}^\infty \in \Delta} \lambda_2(\mathcal{R}^\infty),$$

where Δ is the set of eventually periodic sequences whose first N terms begin with $\mathcal{S}^N$. It is straightforward to verify that $0 \le \lambda_2(\mathcal{S}^N, N) \le N - 1$. Indeed, by Eq (3.2), we take the pair (f, q) with $q = 1$ and

$$f = \begin{cases} \sum_{n=0}^{N-1} s_n 2^n, & \text{if } \sum_{n=0}^{N-1} s_n 2^n \le 2^{N-1}, \\ \sum_{n=0}^{N-1} s_n 2^n - 2^N, & \text{otherwise,} \end{cases}$$

where $0 \le |f| \le 2^{N-1}$. Like the Nth linear complexity, the Nth 2-adic complexity is also a nondecreasing function, that is, $\lambda_2(\mathcal{S}^\infty, N) \le \lambda_2(\mathcal{S}^\infty, N + 1)$.

For $\mathcal{S}^\infty$, the 2-adic complexity is related to its Nth 2-adic complexity by

$$\lambda_2(\mathcal{S}^\infty) = \sup_{N \ge 1} \lambda_2(\mathcal{S}^\infty, N).$$

This implies that $\lambda_2(\mathcal{S}^\infty)$ is finite if $\mathcal{S}^\infty$ is eventually periodic, and $\lambda_2(\mathcal{S}^\infty) = \infty$ otherwise. For the former, we have the following:

Proposition 3.3. *Let $\mathcal{S}^\infty$ be an eventually periodic sequence with the 2-adic complexity λ. Then for every $N \ge 2\lceil\lambda\rceil - 1$,*

$$\lceil\lambda_2(\mathcal{S}^\infty)\rceil = \lceil\lambda_2(\mathcal{S}^\infty, N)\rceil.$$

Proof. We suppose that the 2-adic integer $G(2) = f/q$ with $|f| \le 2^{\lceil\lambda\rceil}$ and that $q \le 2^{\lceil\lambda\rceil} - 1$ by Proposition 3.2. We want to prove $\lceil\lambda_2(\mathcal{S}^\infty, 2\lceil\lambda\rceil - 1)\rceil = \lceil\lambda\rceil$.

Let (f_1, q_1) be the minimal pair of the first $2\lceil\lambda\rceil - 1$ terms of $\mathcal{S}^\infty$. If $\lceil\lambda_2(\mathcal{S}^\infty, 2\lceil\lambda\rceil - 1)\rceil = \lceil\log_2[\max\{|f_1|, q_1\}]\rceil < \lceil\lambda\rceil$, that is, $\lceil\lambda_2(\mathcal{S}^\infty, 2\lceil\lambda\rceil - 1)\rceil \le \lceil\lambda\rceil - 1$, by Definition 3.2, we have

$$|f_1| \le 2^{\lceil\lambda\rceil - 1} \text{ and } q_1 \le 2^{\lceil\lambda\rceil - 1} - 1.$$

Now, from the congruence

$$\frac{f}{q} \equiv \frac{f_1}{q_1} \pmod{2^{2\lceil\lambda\rceil - 1}},$$

or

$$fq_1 \equiv f_1 q \pmod{2^{2\lceil\lambda\rceil - 1}},$$

we get

$$|fq_1| \le 2^{\lceil\lambda\rceil}(2^{\lceil\lambda\rceil - 1} - 1) < 2^{2\lceil\lambda\rceil - 1} \text{ and } |f_1 q| \le 2^{\lceil\lambda\rceil - 1}(2^{\lceil\lambda\rceil} - 1) < 2^{2\lceil\lambda\rceil - 1},$$

which implies $fq_1 = f_1 q$; hence, $\lceil\lambda_2(\mathcal{S}^\infty)\rceil = \lceil\lambda_2(\mathcal{S}^\infty, 2\lceil\lambda\rceil - 1)\rceil$, a contradiction. We complete the proof. □

Example 3.1. *Consider the strictly periodic sequence $\mathcal{S}^\infty = (01001)^\infty$ with the 2-adic complexity $\lambda = 5$. The Nth 2-adic complexity of $\mathcal{S}^\infty$ is*

$$\begin{aligned} &\lceil\lambda_2(\mathcal{S}^\infty, 1)\rceil = 0; \\ &\lceil\lambda_2(\mathcal{S}^\infty, 2)\rceil = \lceil\lambda_2(\mathcal{S}^\infty, 3)\rceil = \lceil\lambda_2(\mathcal{S}^\infty, 4)\rceil = 1; \\ &\lceil\lambda_2(\mathcal{S}^\infty, 5)\rceil = \lceil\lambda_2(\mathcal{S}^\infty, 6)\rceil = 3; \\ &\lceil\lambda_2(\mathcal{S}^\infty, 7)\rceil = \lceil\lambda_2(\mathcal{S}^\infty, 8)\rceil = 4; \\ &\lceil\lambda_2(\mathcal{S}^\infty, N)\rceil = 5,\ N \ge 9. \end{aligned}$$

That is, $\lceil \lambda_2(\mathcal{S}^\infty) \rceil = \lceil \lambda_2(\mathcal{S}^\infty, N) \rceil = 5$ *for* $N \geq 9$ (*note that* $9 = 2\lceil \lambda \rceil - 1$).

Because $\lambda_2(\mathcal{S}^\infty)$ may be not an integer, we have the following general statement.

Proposition 3.4. *Let* $\mathcal{S}^\infty$ *be an eventually periodic sequence with least pre-period* t *and least period* T. *Then the* 2*-adic complexity satisfies*

$$\lambda_2(\mathcal{S}^\infty) = \lambda_2(\mathcal{S}^\infty, N) \text{ for } N \geq 2T + 1$$

if $t = 0$, *and otherwise,*

$$\lambda_2(\mathcal{S}^\infty) = \lambda_2(\mathcal{S}^\infty, N) \text{ for } N \geq 2(t + T).$$

Proof. See Lemma 1 and examples in [31] for $t = 0$.

For $t > 0$, we suppose that the 2-adic integer $G_{\mathcal{S}}(2) = f/q$ with $\max\{|f|, q\} < 2^{t+T}$ by Proposition 3.2. Let (f_1, q_1) be the minimal pair of $\mathcal{S}^{2(t+T)}$, the first $2(t + T)$ terms of $\mathcal{S}^\infty$. It is clear that

$$\max\{|f_1|, q_1\} = 2^{\lambda_2(\mathcal{S}^\infty, 2(t+T))} \leq 2^{\lambda_2(\mathcal{S}^\infty)} < 2^{t+T}.$$

Now, from the congruence

$$\frac{f}{q} \equiv \frac{f_1}{q_1} \pmod{2^{2(t+T)}},$$

or

$$fq_1 \equiv f_1 q \pmod{2^{2(t+T)}},$$

we get

$$|fq_1| < 2^{2(t+T)} \text{ and } |f_1 q| < 2^{2(t+T)},$$

which implies $fq_1 = f_1 q$, and hence, $\lambda_2(\mathcal{S}^\infty) = \lambda_2(\mathcal{S}^\infty, 2(t + T))$. □

We remark that it seems that no similar proof as Proposition 2.2 exists for Proposition 3.3, as Eq (2.3) is not true for Nth 2-adic complexity. By [32, Lemma 3.1.4] the Nth 2-adic complexity holds:

$$N - 1 - \lambda_2(\mathcal{S}^\infty, N) \leq \lambda_2(\mathcal{S}^\infty, N + 1) \leq \max\left(\lambda_2(\mathcal{S}^\infty, N), N - \lambda_2(\mathcal{S}^\infty, N)\right) + 1.$$

Example 3.2. *Consider the eventually periodic sequence* $\mathcal{S}^\infty = 111(1000)^\infty$ *with pre-period* $t = 3$ *and period* $T = 4$. *The* N*th* 2*-adic complexity of* $\mathcal{S}^\infty$ *is*

$$\begin{aligned}
&\lambda_2(\mathcal{S}^\infty, 1) = \lambda_2(\mathcal{S}^\infty, 2) = \lambda_2(\mathcal{S}^\infty, 3) = \lambda_2(\mathcal{S}^\infty, 4) = \log_2(1);\\
&\lambda_2(\mathcal{S}^\infty, 5) = \lambda_2(\mathcal{S}^\infty, 6) = \lambda_2(\mathcal{S}^\infty, 7) = \lambda_2(\mathcal{S}^\infty, 8) = \log_2(3);\\
&\lambda_2(\mathcal{S}^\infty, 9) = \lambda_2(\mathcal{S}^\infty, 10) = \log_2(23);\\
&\lambda_2(\mathcal{S}^\infty, 11) = \lambda_2(\mathcal{S}^\infty, 12) = \log_2(43);\\
&\lambda_2(\mathcal{S}^\infty, 13) = \log_2(87);\\
&\lambda_2(\mathcal{S}^\infty, N) = \log_2(97),\ N \geq 14.
\end{aligned}$$

That is, $\lambda_2(\mathcal{S}^\infty) = \lambda_2(\mathcal{S}^\infty, N) = \log_2(97)$ *for* $N \geq 14$ (*note that* $14 = 2(t + T)$).

Example 3.3. *Consider the eventually periodic sequence* $\mathcal{S}^\infty = 11(1000)^\infty$ *with pre-period* $t = 2$ *and period* $T = 4$*. The* N*th* 2*-adic complexity of* $\mathcal{S}^\infty$ *is*

$$\begin{aligned}
&\lambda_2(\mathcal{S}^\infty, 1) = \lambda_2(\mathcal{S}^\infty, 2) = \lambda_2(\mathcal{S}^\infty, 3) = \log_2(1);\\
&\lambda_2(\mathcal{S}^\infty, 4) = \lambda_2(\mathcal{S}^\infty, 5) = \log_2(5);\\
&\lambda_2(\mathcal{S}^\infty, 6) = \log_2(7); \lambda_2(\mathcal{S}^\infty, 7) = \log_2(9); \lambda_2(\mathcal{S}^\infty, 8) = \log_2(13);\\
&\lambda_2(\mathcal{S}^\infty, 9) = \log_2(15); \lambda_2(\mathcal{S}^\infty, 10) = \log_2(29);\\
&\lambda_2(\mathcal{S}^\infty, N) = \log_2(41),\ N \geq 11.
\end{aligned}$$

That is, $\lambda_2(\mathcal{S}^\infty) = \lambda_2(\mathcal{S}^\infty, N) = \log_2(41)$ *for* $N \geq 11$ (*note that* $11 < 2(t + T)$).

The (Nth) 2-adic complexity can be computed efficiently using the rational approximation algorithm (RAA) [33, Section 3], and thus, it can be used to estimate the minimal size of FCSRs that generate the sequence. A number of consecutive bits equal to twice the 2-adic complexity suffices to reconstruct the whole sequence. Hence, the 2-adic complexity should be as large as possible, ideally at least half of its period or its length.

3.3. Average and asymptotic behavior of 2*-adic complexity*

In this subsection, we review the expected Nth 2-adic complexity for binary sequences of length N and the expected 2-adic complexity for binary sequences of period T, respectively, as well as the asymptotic behavior of the Nth 2-adic complexity for infinite binary sequences as N grows.

For finite sequences of length N, the expected value of the Nth 2-adic complexity is defined to be

$$E_N^{2-\text{adic}} = \frac{1}{2^N} \sum_{\mathcal{S}^N \in \mathbb{F}_2^N} \lambda_2(\mathcal{S}^N, N).$$

The theoretical analysis about $E_N^{2-\text{adic}}$ goes back to the date when FCSRs were introduced in 1990s [3, 30, 34, 35]. The numerical experiments claimed that the average behavior $E_N^{2-\text{adic}}$ behaves like that of the Nth linear complexity [32, 36]. In 2024, Chen and Winterhof [37] theoretically proved that

$$E_N^{2-\text{adic}} = \frac{N}{2} + O(\log(N)),$$

where the implied constant is absolute. More exactly, they got the bounds

$$E_N^{2-\text{adic}} \geq \frac{N}{2} - 1 \quad \text{and} \quad E_N^{2-\text{adic}} \leq \frac{N}{2} + \delta(\log_2(N)) + O(N^{2-2\delta}),$$

where the implied constant in O depends only on $\delta > 1/2$. From Figure 3, it seems that $E_N^{2-\text{adic}} \leq N/2$ (we leave it open). They also proved the asymptotic behavior of Nth 2-adic complexity for varying N with probability 1,

$$\lambda_2(\mathcal{S}^\infty, N) = \frac{N}{2} + O(\log(N)) \quad \text{for } N \geq 1,$$

for a random $\mathcal{S}^\infty$.

The numerical analysis on the variance of the Nth 2-adic complexity, denoted by $V_N^{2-\text{adic}}$, seems to imply that

$$\lim_{N\to\infty} V_N^{2-\text{adic}} \approx 0.9.$$

See Figure 3.

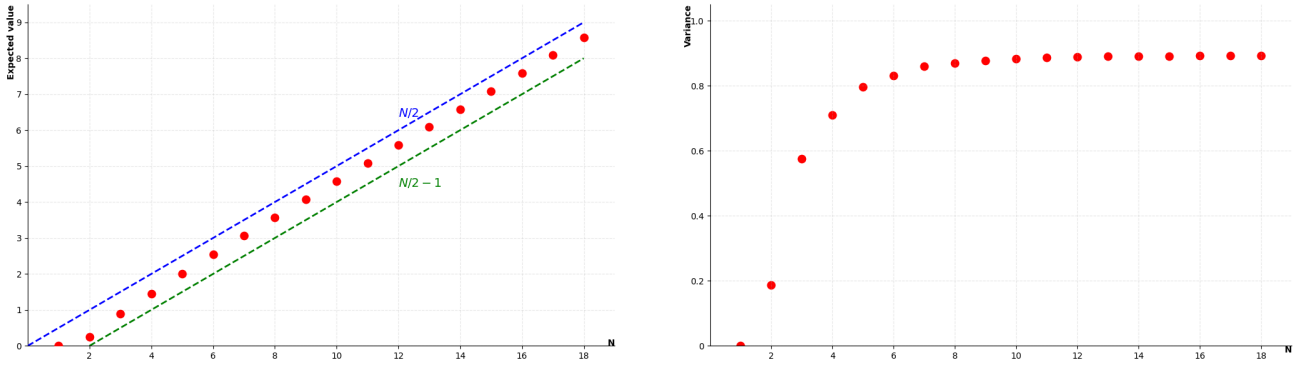

Figure 3. Expected value (left) and variance (right) of Nth 2-adic complexity.

Question 3.1. *Prove* $E_N^{2-\text{adic}} \leq N/2$, *and compute the variance of the* N*th 2-adic complexity of sequences.*

We remark that the way in [37] can be used to prove a lower bound on the expected value of Nth k-adic complexity of k-ary sequences of length $N \geq 1$ for $k \geq 3$. Exactly speaking, for k-ary sequence $\mathcal{S}^N$, by using [3, Lemma 18.5.1], we have

$$\lambda_k(\mathcal{S}^N, N) \geq N - 1 - \frac{1}{\log_2(k)} - \lambda_k(\mathcal{S}^{N-1}, N-1)$$

if $\mathcal{S}^{N-1}$ and $\mathcal{S}^N$ have no common minimal pair. Then, using $E_{N-1}^{\text{k-adic}} < E_N^{\text{k-adic}}$, we compute

$$\begin{aligned} k^N \cdot E_N^{\text{k-adic}} &= \sum_{\mathcal{S}^N} \lambda_k(\mathcal{S}^N, N) \\ &\geq \sum_{\mathcal{S}^{N-1}} \left(\lambda_k(\mathcal{S}^{N-1}, N-1) + (k-1)(N - 1 - \frac{1}{\log_2(k)} - \lambda_k(\mathcal{S}^{N-1}, N-1)) \right) \\ &= k^{N-1}(k-1)\left(N - 1 - \frac{1}{\log_2(k)}\right) - (k-2)k^{N-1}E_{N-1}^{\text{k-adic}} \\ &> k^{N-1}(k-1)\left(N - 1 - \frac{1}{\log_2(k)}\right) - (k-2)k^{N-1}E_N^{\text{k-adic}}, \end{aligned}$$

from which we derive

$$E_N^{\text{k-adic}} \geq \frac{N}{2} - \frac{1 + 1/\log_2(k)}{2}.$$

Question 3.2. *Estimate an upper bound on* $E_N^{\text{k-adic}}$.

The expected 2-adic complexity of binary periodic sequences $\mathcal{S}^\infty$ with period T, denoted by

$$E_T^{2-\text{adic}} := \frac{1}{2^T} \sum_{\mathcal{S}^\infty \in \mathbb{F}_2^\infty} \lambda_2(\mathcal{S}^\infty), \quad \mathcal{S}^\infty \text{ is } T-\text{periodic}.$$

Hu and Feng derived explicit formulas for the expectation $E_T^{2-\text{adic}}$ and the variance $V_T^{2-\text{adic}}$ according to the factorization of $2^T - 1$. In particular, when $2^T - 1$ is prime, we have the simple form

$$E_T^{2-\text{adic}} = \left(1 - \frac{1}{2^T - 1}\right)\log_2(2^T - 1), \quad V_T^{2-\text{adic}} = \frac{2^{T-1} - 1}{2^{2T-2}}\left(\log_2(2^T - 1)\right)^2;$$

see [38, Theorem 1 and Corollary 2]. In [3, Section 18.2] Goresky and Klapper studied the expectation of k-adic complexity of periodic k-ary sequences with connection integer dividing q.

3.4. 2-adic complexity of algebraic sequences

$G_{\mathcal{S}}(2) = \sum_{n=0}^{\infty} s_n 2^n$ is algebraic over $\mathbb{Z}$ if there is a nonzero polynomial $h(y) \in \mathbb{Z}[y]$ such that $h(G_{\mathcal{S}}(2)) = 0$, and otherwise, it is transcendental.

If $G_{\mathcal{S}}(2)$ is algebraic, we also call $\mathcal{S}^{\infty}$ a 2-adic algebraic sequence. It is clear that $G_{\mathcal{S}}(2) = f/q$ (which is a rational number) of any eventually periodic sequences are algebraic, as $h(y) = qy - f$.

Chen and Winterhof [39] proved the following:

Proposition 3.5. *Let $\mathcal{S}^{\infty}$ be a binary sequence which is not eventually periodic. Let $h(y) = h_0 + h_1 y + \ldots + h_d y^d \in \mathbb{Z}[y]$ be a nonzero polynomial of degree d with no rational zero and $h(G_{\mathcal{S}}(2)) = 0$. Put*

$$H = \sum_{i=0}^{d} |h_i|.$$

Then, for $N \geq 1$, we have

$$\frac{N}{d} - \frac{\log_2(H)}{d} \leq \lambda_2(\mathcal{S}^{\infty}, N) \leq \frac{d-1}{d}N + \frac{\log_2(H)}{d} + 1.3.$$

Hence, with respect to the Nth 2-adic complexity, any $\mathcal{S}^{\infty}$ for which $G_{\mathcal{S}}(2)$ is a root of an irreducible polynomial $h(y) \in \mathbb{Z}[y]$ of degree $d = 2$ behaves like a random sequence due to the average and asymptotic behavior of binary sequences stated in Subsection 3.3. See some examples in [39].

Similarly to PLCP (in Subsection 2.3), one can define a sequence with a d-perfect 2-adic complexity profile (d-PACP): A binary $\mathcal{S}^{\infty}$ is said to have a d-PACP if

$$\left|\lambda_2(\mathcal{S}^{\infty}, N) - \frac{N}{2}\right| \leq \frac{d}{2}$$

for any $N \geq 1$. In particular, $\mathcal{S}^{\infty}$ is said to have a PACP if $d = 1$. Generally, any sequence with a d-PACP is called a sequence with an almost PACP.

Question 3.3. *Construct a sequence with a PACP.*

Question 3.4. *Analogously to expansion complexity, one may introduce a similar notion of complexity in terms of the polynomial $h(y)$ with $h(G_{\mathcal{S}}(2)) = 0$.*

4. Relations between complexity measures

The linear complexity and the 2-adic complexity complement each other. For example, for the m-sequence with period $2^n - 1$, its linear complexity equals n, but its 2-adic complexity equals $\log_2(2^{2^n-1} -$

1); see [40]. For the ℓ-sequence with prime connection integer q, its linear complexity is less than or equal to $(q+1)/2$, but its 2-adic complexity equals $\log_2(q)$; see [41].

A finer complexity measure is the maximum order complexity, which is the length of a shortest feedback shift register that generates the sequence. That is, the Nth maximum order complexity $M(\mathcal{S}^N, N)$ of $\mathcal{S}^N$ is the smallest positive integer M such that there is a polynomial $F(x_1, \ldots, x_M) \in \mathbb{F}_2[x_1, \ldots, x_M]$ satisfying

$$s_{i+M} = F(s_i, s_{i+1}, \ldots, s_{i+M-1}) \text{ for } 0 \le i \le N - M - 1.$$

The maximum order complexity $M(\mathcal{S}^\infty)$ of $\mathcal{S}^\infty$ is characterized by

$$M(\mathcal{S}^\infty) = \sup_{N \ge 1} M(\mathcal{S}^\infty, N).$$

If $\mathcal{S}^\infty$ is T-periodic, we have $M(\mathcal{S}^\infty) = M(\mathcal{S}^\infty, N)$ for $N \ge 2T - 1$. For more details on the maximum order complexity, we refer the reader to [42–48].

From the definitions, it is straightforward to see that $M(\mathcal{S}^\infty) \le LC(\mathcal{S}^\infty)$, and $M(\mathcal{S}^\infty, N) \le LC(\mathcal{S}^\infty, N)$.

Recently, Chen et al. [31] established the first explicit inequality between the maximum order complexity and the 2-adic complexity, which gave a negative answer of a question in [3, p. 329]. They proved that

$$M(\mathcal{S}^\infty, N) \le \lceil \lambda_2(\mathcal{S}^\infty, N) \rceil + 1, \text{ for } N \ge 1,$$

and for strictly periodic sequence $\mathcal{S}^\infty$,

$$M(\mathcal{S}^\infty) \le \lceil \lambda_2(\mathcal{S}^\infty) \rceil.$$

These results build a solid theoretical bridge between the maximum order complexity and the 2-adic complexity. It offers a convenient criterion for assessing resistance to FCSR attacks: A sufficiently large maximum order complexity automatically ensures a large 2-adic complexity.

A short summary was stated in [31, Section V] about relationships among them.

5. Conclusions and final remarks

In this work, we have reviewed two complexity measures: the linear and 2-adic complexities of eventually periodic binary sequences. They are defined by formal power series and 2-adic integers of the corresponding sequences, respectively. They can therefore be dealt with in a mathematical way.

For the linear complexity of $\mathcal{S}^\infty$ with rational function $G_S(x) = \sum_{n=0}^{\infty} s_n x^n = f(x)/q(x)$ in the lowest term, it is just the value $\max\{1 + \deg(f(x)), \deg(q(x)\}$. The notion of the Nth linear complexity of $\mathcal{S}^N$ (of length N) is the minimal linear complexity of all eventually periodic sequences which start with the $\mathcal{S}^N$. This measure characterizes the local complexity of a finite segment of $\mathcal{S}^\infty$, reflecting the smallest length of LFSRs that generate that exactly prefix. The average and asymptotic behavior arise the study of sequences with a perfect linear complexity profile, that is, sequences whose linear complexity profile follows the asymptotic behavior of random sequences as closely as possible. The algebraicity of $G_S(x)$ can be used to estimate the Nth linear complexity of an aperiodic sequence.

We have similar statements for the 2-adic complexity of $\mathcal{S}^\infty$ with the 2-adic integer $G_S(2) = \sum_{n=0}^{\infty} s_n 2^n = f/q$ in the lowest term. The 2-adic complexity is defined as the value

$\log_2(\max\{|f|, q\})$. The notion of the Nth 2-adic complexity of $\mathcal{S}^N$ (of length N) is the minimal 2-adic complexity of all eventually periodic sequences which start with $\mathcal{S}^N$. This measure characterizes the local complexity of a finite segment of $\mathcal{S}^\infty$, reflecting the smallest size of FCSRs that generate that exactly prefix. The average and asymptotic behavior motivate the study of sequences with perfect 2-adic complexity profile. The algebraicity of $G_S(2)$ can be used to estimate the Nth 2-adic complexity of aperiodic sequence.

As mentioned in [39, Section 4.1], any aperiodic sequences are not 2-adic algebraic (resp. automatic) if they are automatic (resp. 2-adic algebraic), so we have the following question.

Question 5.1. *Consider the Nth linear complexity for 2-adic algebraic sequences which are not eventually periodic as well as the Nth 2-adic complexity for automatic sequences which are not eventually periodic.*

We remark that 2-adic algebraic sequences with an almost PACP corresponding to $\sqrt{17}$ and $\sqrt{-7}$ in [37, Figures 1 and 2] have an almost PLCP (without proof). Numerical experiments on the Nth 2-adic complexity of $\mathcal{S}^\infty$ with a PLCP defined in Eq (2.4), which is apwenian [13] or [12, Example 8], indicate that it has an almost PACP (without proof); see Figure 4. Furthermore, in the master thesis [32, Section 5], experimental results indicate that the Nth 2-adic complexity of the Thue–Morse sequence (with an almost PLCP [24]) is very close to $N/2$, which means that it has an almost PACP (without proof). It is therefore interesting to consider sequences with both a PLCP and a PACP.

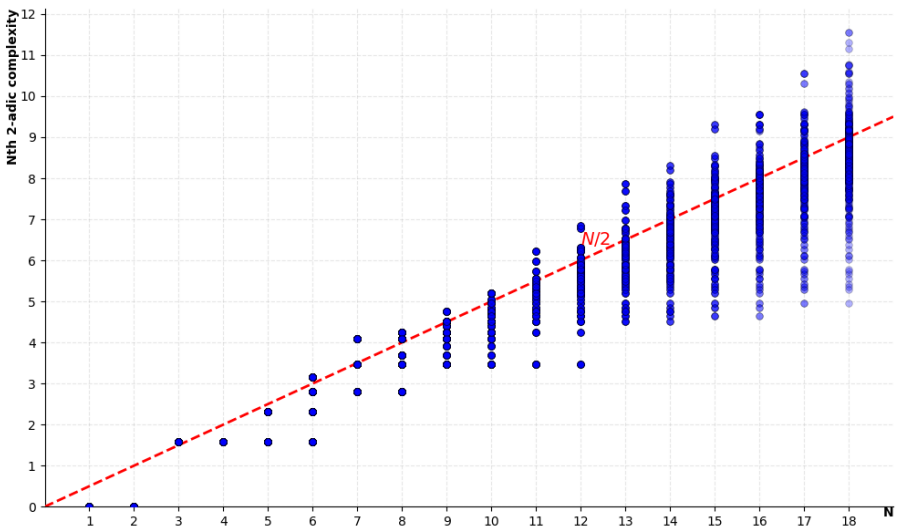

Figure 4. Nth 2-adic complexity of apwenian sequences in Eq (2.4).

Goresky and Klapper [3] extended the concepts of LFSRs and FCSRs and introduced a class of more general registers called algebraic feedback shift registers (AFSRs) with respect to some particular algebraic ring R and parameter π; see Figure 5.

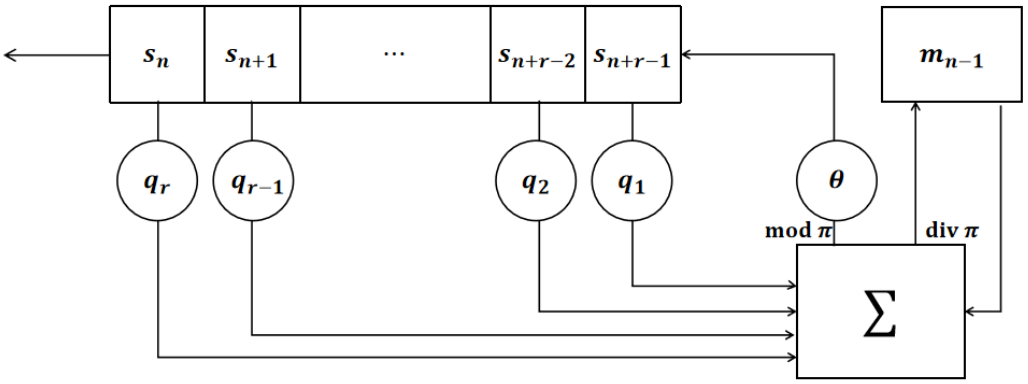

Figure 5. An AFSR of length r.

The state change satisfies a linear recurrence with carry

$$-q_0 s_{n+r} + \pi m_n = q_1 s_{n+r-1} + \cdots + q_r s_n + m_{n-1} \quad \text{for} \quad n \geq 0,$$

where $q_0 = -\theta^{-1} \pmod{\pi}$, and the coefficients q_i's are in R. The notions of π-adic span and π-adic complexity are introduced to measure the minimal size of AFSRs that generated the sequences [3, 49].

Question 5.2. *Consider the average behavior of Nth π-adic complexity.*

Finally, we conclude this survey by mentioning a new measure called rational complexity, which was introduced in [50]. It is interesting to study its behavior.

Author contributions

Hezheng Lin: Investigation; writing—original draft. Lingmei Xiao: Investigation; visualization; writing—review & editing. Zhixiong Chen: Project administration; supervision; writing—review & editing. All authors have read and approved the final version of the manuscript for publication.

Use of Generative-AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

We'd like to thank the editor, the reviewers, and Arne Winterhof for their constructive comments.

The work was supported in part by the National Science Foundation of China (No. 62372256), the Co-innovation Platform Project of Fuzhou-Xiamen-Quanzhou National Independent Innovation Demonstration Zone (No. 2025E3006), and the Science and Technology Project of Putian City of China (No. 2024SZ3001PTXY02, No. 2025GZ2001PTXY22).

Conflict of interest

The authors declare that they have no conflicts of interest.

References

1. J. P. Allouche, J. Shallit, *Automatic sequences: Theory, applications, generalizations*, Cambridge University Press, 2003. https://doi.org/10.1017/CBO9780511546563
2. S. W. Golomb, G. Gong, *Signal design for good correlation - for wireless communication, cryptography and radar*, Cambridge University Press, 2005. https://doi.org/10.1017/CBO9780511546907
3. M. Goresky, A. Klapper, *Algebraic shift register sequences*, Cambridge University Press, 2012. https://doi.org/10.1017/CBO9781139057448
4. C. L. Li, A survey on complexity measures for pseudo-random sequences, *Cryptography*, **8** (2024), 25. http://dx.doi.org/10.3390/cryptography8020025
5. Z. X. Chen, Trace representation and linear complexity of binary sequences derived from Fermat quotients, *Sci. China Inf. Sci.*, **57** (2014), 1–10. http://dx.doi.org/10.1007/s11432-014-5092-x
6. Z. X. Chen, X. N. Du, R. Marzouk, Trace representation of pseudorandom binary sequences derived from Euler quotients, *Appl. Algebra Eng. Commun. Comput.*, **26** (2015), 555–570. http://dx.doi.org/10.1007/s00200-015-0265-4
7. J. L. Massey, Shift-register synthesis and BCH decoding, *IEEE Trans. Inf. Theory*, **15** (1969), 122–127. http://dx.doi.org/10.1109/tit.1969.1054260
8. R. A. Rueppel, *Analysis and design of stream ciphers*, Berlin, Heidelberg: Springer, 2012. https://doi.org/10.1007/978-3-642-82865-2
9. H. Niederreiter, The probabilistic theory of linear complexity, In: *Advances in cryptology - EUROCRYPT' 88*, **330** (1988), 191–209. https://doi.org/10.1007/3-540-45961-8_17
10. H. Niederreiter, A combinatorial approach to probabilistic results on the linear complexity profile of random sequences, *J. Cryptol.*, **2** (1990), 105–112. http://dx.doi.org/10.1007/bf00204450
11. M. Z. Wang, J. L. Massey, The characterization of all binary sequences with perfect linear complexity profiles, In: *Workshop on the theory and application of cryptographic techniques - EUROCRYPT' 86*, 1986, 35–36.
12. L. Mérai, A. Winterhof, Pseudorandom sequences derived from automatic sequences, *Cryptogr. Commun.*, **14** (2022), 783–815. http://dx.doi.org/10.1007/s12095-022-00556-9
13. J. P. Allouche, G. N. Han, H. Niederreiter, Perfect linear complexity profile and apwenian sequences, *Finite Fields Appl.*, **68** (2020), 101761. http://dx.doi.org/10.1016/j.ffa.2020.101761
14. H. Niederreiter, Sequences with almost perfect linear complexity profile, In: *Advances in cryptology — EUROCRYPT' 87*, **304** (1987), 37–51. https://doi.org/10.1007/3-540-39118-5_5
15. J. Grünberger, *Linear complexity and continued fractions of families of binary sequences*, Master Thesis, Johannes Kepler University Linz, 2024.
16. H. Niederreiter, Linear complexity and related complexity measures for sequences, In: *Progress in cryptology - INDOCRYPT 2003*, **2904** (2003), 1–17. http://dx.doi.org/10.1007/978-3-540-24582-7_1

17. H. Niederreiter, C. P. Xing, *Rational points on curves over finite fields: Theory and applications*, Cambridge University Press, 2001. http://dx.doi.org/10.1017/CBO9781107325951.003

18. C. P. Xing, K. Y. Lam, Sequences with almost perfect linear complexity profiles and curves over finite fields, *IEEE Trans. Inf. Theory*, **45** (1999), 1267–1270. http://dx.doi.org/10.1109/18.761282

19. W. Meidl, H. Niederreiter, On the expected value of the linear complexity and the k-error linear complexity of periodic sequences, *IEEE Trans. Inf. Theory*, **48** (2002), 2817–2825. http://dx.doi.org/10.1109/tit.2002.804050

20. B. Kjos-Hanssen, On the complexity of automatic complexity, *Theory Comput. Syst.*, **61** (2017), 1427–1439. http://dx.doi.org/10.1007/s00224-017-9795-4

21. B. Kjos-Hanssen, Automatic complexity of shift register sequences, *Discrete Math.*, **341** (2018), 2409–2417. http://dx.doi.org/10.1016/j.disc.2018.05.015

22. H. Zantema, W. Bosma, Complexity of automatic sequences, *Inf. Comput.*, **288** (2022), 104710. http://dx.doi.org/10.1016/j.ic.2021.104710

23. L. Mérai, A. Winterhof, On the pseudorandomness of automatic sequences, *Cryptogr. Commun.*, **10** (2018), 1013–1022. http://dx.doi.org/10.1007/s12095-017-0260-7

24. L. Mérai, A. Winterhof, On the Nth linear complexity of automatic sequences, *J. Number Theory*, **187** (2018), 415–429. http://dx.doi.org/10.1016/j.jnt.2017.11.008

25. C. Diem, On the use of expansion series for stream ciphers, *LMS J. Comput. Math.*, **15** (2012), 326–340. http://dx.doi.org/10.1112/s146115701200109x

26. L. Mérai, H. Niederreiter, A. Winterhof, Expansion complexity and linear complexity of sequences over finite fields, *Cryptogr. Commun.*, **9** (2017), 501–509. http://dx.doi.org/10.1007/s12095-016-0189-2

27. D. Gómez-Pérez, L. Mérai, Algebraic dependence in generating functions and expansion complexity, *Adv. Math. Commun.*, **14** (2020), 307–318. http://dx.doi.org/10.3934/amc.2020022

28. D. Gómez-Pérez, L. Mérai, H. Niederreiter, On the expansion complexity of sequences over finite fields, *IEEE Trans. Inf. Theory*, **64** (2018), 4228–4232. http://dx.doi.org/10.1109/TIT.2018.2792490

29. Z. M. Sun, X. Y. Zeng, C. L. Li, Y. Zhang, L. Yi, The expansion complexity of ultimately periodic sequences over finite fields, *IEEE Trans. Inf. Theory*, **67** (2021), 7550–7560. http://dx.doi.org/10.1109/TIT.2021.3112824

30. A. Klapper, M. Goresky, Feedback shift registers, 2-adic span, and combiners with memory, *J. Cryptol.*, **10** (1997), 111–147. http://dx.doi.org/10.1007/s001459900024

31. Z. R. Chen, Z. X. Chen, J. Obrovsky, A. Winterhof, Maximum-order complexity and 2-adic complexity, *IEEE Trans. Inf. Theory*, **70** (2024), 6060–6067. http://dx.doi.org/10.1109/TIT.2024.3405946

32. J. Obrovsky, 2-*Adic complexity and related measures of pseudorandomness*, Master Thesis, Johannes Kepler University Linz, 2023.

33. A. Klapper, M. Goresky, Cryptanalysis based on 2-adic rational approximation, In: *Advances in cryptology - CRYPTO' 95*, **963** (1995), 262–273. http://dx.doi.org/10.1007/3-540-44750-4_21

34. A. Klapper, Open problems on with-carry sequence generators, In: *Open problems in mathematics and computational science*, 2014, 181–201. http://dx.doi.org/10.1007/978-3-319-10683-0_9

35. T. Tian, W. F. Qi, Expected values for the rational complexity of finite binary sequences, *Des. Codes Cryptogr.*, **55** (2010), 65–79. http://dx.doi.org/10.1007/s10623-009-9331-x

36. A. Winterhof, Pseudorandom binary sequences: Quality measures and number theoretic constructions, *IEICE Trans. Fundam.*, **106** (2023), 1452–1460. https://doi.org/10.1587/transfun.2023SDI0001

37. Z. X. Chen, A. Winterhof, Probabilistic results on the 2-adic complexity, *Des. Codes Cryptogr.*, **93** (2025), 2191–2203. http://dx.doi.org/10.1007/s10623-025-01592-1

38. H. G. Hu, D. G. Feng, On the 2-adic complexity and the k-error 2-adic complexity of periodic binary sequences, *IEEE Trans. Inf. Theory*, **54** (2008), 874–883. http://dx.doi.org/10.1109/TIT.2007.913238

39. Z. X. Chen, A. Winterhof, On the Nth 2-adic complexity of binary sequences identified with algebraic 2-adic integers, *Discrete Appl. Math.*, **373** (2025), 279–289. http://dx.doi.org/10.1016/j.dam.2025.05.024

40. T. Tian, W. F. Qi, 2-Adic complexity of binary m-sequences, *IEEE Trans. Inf. Theory*, **56** (2009), 450–454. http://dx.doi.org/10.1109/TIT.2009.2034904

41. C. Seo, S. Lee, Y. Sung, K. Han, S. Kim, A lower bound on the linear span of an FCSR, *IEEE Trans. Inf. Theory*, **46** (2000), 691–693. http://dx.doi.org/10.1109/18.825844

42. Z. X. Chen, A. I. Gómez, D. Gómez-Pérez, A. Tirkel, Correlation measure, linear complexity and maximum order complexity for families of binary sequences, *Finite Fields Appl.*, **78** (2022), 101977. http://dx.doi.org/10.1016/j.ffa.2021.101977

43. C. J. A. Jansen, *Investigations on nonlinear stream cipher systems: Construction and evaluation methods*, Ph.D. dissertation, Technical University of Delft, 1989.

44. C. J. A. Jansen, The maximum order complexity of sequence ensembles, In: *Advances in cryptology - EUROCRYPT'91*, **547** (1991), 153–159. http://dx.doi.org/10.1007/3-540-46416-6_13

45. C. J. A. Jansen, D. E. Boekee, The shortest feedback shift register that can generate a given sequence, In: *Advances in cryptology - CRYPTO'89*, **435** (1990), 90–99. http://dx.doi.org/10.1007/0-387-34805-0_10

46. S. C. Liang, X. Y. Zeng, Z. B. Xiao, Z. M. Sun, Binary sequences with length n and nonlinear complexity not less than $n/2$, *IEEE Trans. Inf. Theory*, **69** (2023), 8116–8125. http://dx.doi.org/10.1109/TIT.2023.3316252

47. P. Rizomiliotis, N. Kalouptsidis, Results on the nonlinear span of binary sequences, *IEEE Trans. Inf. Theory*, **51** (2005), 1555–1563. http://dx.doi.org/10.1109/isit.2004.1365157

48. Z. M. Sun, X. Y. Zeng, C. L. Li, T. Helleseth, Investigations on periodic sequences with maximum nonlinear complexity, *IEEE Trans. Inf. Theory*, **63** (2017), 6188–6198. http://dx.doi.org/10.1109/TIT.2017.2714681

49. A. Klapper, Expected π-adic security measures of sequences, *IEEE Trans. Inf. Theory*, **56** (2010), 2486–2501. http://dx.doi.org/10.1109/TIT.2010.2044059

50. M. Vielhaber, M. P. Canales Chacón, S. Jara Ceballos, Rational complexity of binary sequences, F$\mathbb{Q}$SRs and pseudo-ultrametric continued fractions in $\mathbb{R}$, *Cryptogr. Commun.*, **14** (2022), 433–457. http://dx.doi.org/10.1007/s12095-021-00539-2

AIMS Press