Chaotic Nature of Integer Sequences From Primitive Linear Feedback Shift Registers

Hyojeong Choi, *Graduate Student Member, IEEE*, Gangsan Kim, *Member, IEEE*, Hong-Yeop Song, *Senior Member, IEEE*, and Hongjun Noh

***Abstract*—In this brief, we investigate the chaotic characteristics of the integer sequences generated by primitive linear feedback shift registers (LFSRs) by interpreting the internal states as integers. We prove that the discrete Lyapunov exponent (dLE) of the permutations induced by these sequences from an L-stage primitive LFSR approches to the range between $\ln(\sqrt{3})$ and $\ln(2)$ as L increases indefinitely and hence the dynamic systems satisfy the definition of discrete chaos. Furthermore, the 0-1 test of the sequences yields statistics close to 1, supporting the conclusion that these sequences exhibit chaotic dynamics under both theoretical and empirical evaluations.**

***Index Terms*—Discrete chaos, chaotic behaviors, discrete Lyapunov exponent, 0-1 test, linear feedback shift registers.**

I. Introduction

CHAOS, characterized by its aperiodic and unpredictable dynamics, has been widely adopted as a powerful tool for modeling nonlinear and complex systems. In particular, chaotic systems have found extensive applications in cryptography [1], [2], [3], digital watermarking [4], spread-spectrum communication [5], and random number generation [2], [3].

Traditional chaotic maps such as the Logistic, Tent, Sine, and Hénon maps are typically defined over the real field. However, when these continuous chaotic systems are implemented in digital environments, finite-precision arithmetic inevitably introduces rounding and quantization errors [6], [7], [8]. Such errors accumulate systematically depending on the system state. As a result, key chaotic properties–such as aperiodicity, unpredictability, and complexity–are significantly degraded. Moreover, the internal structure of chaotic maps realized in digital hardware often remains unclear, and rare but important behaviors may be overlooked due to the limited scope of empirical testing [7]. Accordingly, two main research directions have emerged: the first is analyzing the dynamic behaviors of traditional chaotic maps under finite-precision arithmetic and the second is exploring the need for chaotic systems defined directly over discrete spaces [1], [7], [9], [10], [11], [12].

The first direction highlights that digital implementations of continuous chaotic systems inevitably exhibit periodic trajectories due to limited state space, leading to a collapse of their original chaotic properties–a phenomenon referred to as dynamical degradation. In particular, [1], [7], [10] analyzed the dynamic behaviors that arise when well-known chaotic maps such as the Logistic, Tent, and Hénon maps are implemented with fixed or floating-point precision.

Meanwhile, a parallel line of research has sought to rigorously define chaos over discrete spaces as mentioned in the second direction above [9], [11], [12]. For example, [9] showed that semi-digital chaotic systems – continuous maps subjected to quantization – can still satisfy Devaney's definition of chaos under certain conditions. As a fundamental approach, [11], [12] proposed the discrete Lyapunov exponent (dLE) as a discrete analog of the traditional Lyapunov exponent, suitable for characterizing the average divergence of neighboring points in discrete dynamical systems. Here, neighboring points refer to the elements that are adjacent to a given element in the discrete domain, based on the natural ordering of the discrete space defined by the system [11], [12]. They defined discrete chaos as the regime in which dLE remains positive as the size of the discrete space tends to infinity. Moreover, they emphasized that some bijective maps, by eliminating stable periodic orbits, facilitate the emergence of chaotic behavior in discrete systems.

Building on these foundations, numerous studies have focused on proposing new chaotic maps defined over discrete spaces and analyzing their dynamical behavior. These studies primarily evaluate whether the proposed maps exhibit chaotic properties using the dLE [8], [13], [14], [15], [16]. For example, [8] proposed a discrete Arnold's cat map over the integer ring to generate integer pseudo-random number generator (PRNG), and [13] presented a PRNG based on a modified logistic map. Other discrete chaotic maps have been proposed based on finite fields [14], based on reversible modular operations [15] and based on permutation compositions [16]. These works demonstrate that discrete chaotic systems can maintain high complexity and unpredictability in practical environments for cryptography as well as PRNG.

Another widely used tool for evaluating chaotic behavior is the 0-1 test [17]. The 0-1 test is known as a method that distinguishes between chaos and regularity in deterministic time series without requiring phase space reconstruction or any preprocessing [17]. This method has been effectively applied

Received 21 April 2025; revised 4 June 2025; accepted 20 June 2025. Date of publication 4 July 2025; date of current version 29 August 2025. This work was supported by the Korea Research Institute for Defense Technology planning and advancement (KRIT) grant funded by the Korea Government (Defense Acquisition Program Administration), Aperiodic, non-predictable, randomness and denseness signaling ultra-low-probability-of-detection and covert communication technology, 2024 under Grant 11-202-205-010 (KRIT-CT-22-086). This brief was recommended by Associate Editor F. G. Moraes. *(Corresponding author: Hong-Yeop Song.)*

Hyojeong Choi, Gangsan Kim, and Hong-Yeop Song are with the Department of Electrical and Electronic Engineering, Yonsei University, Seoul 03722, South Korea (e-mail: hysong@yonsei.ac.kr).

Hongjun Noh is with the Department of C4I R&D Center, LIG Nex1, Yongin-si 333, South Korea.

Digital Object Identifier 10.1109/TCSII.2025.3585913

not only to continuous systems [18], [19], [20], [21], but also to discrete systems [22], and has been adopted in various studies.

In this brief, we are interested only in an L-stage linear feedback shift register (LFSR) with a primitive connection logic, which corresponds to a primitive polynomial of degree L over the binary field [23], [24], [25]. We call this an L-stage *primitive LFSR*. When it is initialized with any non-zero L-bit pattern, it generates a maximal-length sequence known as an m-sequence, with period $2^L - 1$. Due to their long periods and well-known pseudo-random properties–such as balance, span, run, constant-on-the-coset, ideal autocorrelation, and cycle-and-add properties [23], [24], [25]–m-sequences have been widely used in pseudo-random number generation and communication systems. We follow the convention illustrated in Fig. 1, where the LFSR performs a left shift at each clock cycle, and the connection logic defined by the given primitive polynomial determines a feedback bit as a linear combination of selected register bits, which is then inserted into the rightmost position. A key property of the resulting m-sequence is the *span property*, which ensures that every consecutive L-bit window in the sequence shows an L-bit pattern exactly once. This implies that the LFSR visits each of the $2^L - 1$ non-zero states exactly once, and hence, the m-sequence is sometimes regarded as a modified de Bruijn sequence [23], [24], [25].

Motivated by the question whether any chaotic behavior could arise in an L-stage primitive LFSR (due to well-known pseudo-random properties of m-sequences), we regard the internal states as integers and analyze the resulting integer sequences from a dynamical systems perspective. Each L-bit internal state corresponds to a window in the m-sequence and it is treated as an integer value, as illustrated in Fig. 1. This interpretation produces an integer sequence that captures the global evolution of the system.

We theoretically derive the dLE of the resulting integer sequences and show that it converges to a positive value as L increases, thereby satisfying the definition of discrete chaos [11], [12]. In addition, we verify the chaotic behavior of the sequence using the 0-1 test. In particular, the trajectory in the (p_c, q_c) plane demonstrates Brownian motion-like characteristics. Furthermore, the resulting correlation statistic K remains consistently close to 1, providing further empirical evidence of the discrete chaos.

The remainder of this brief is organized as follows. Section II provides a theoretical analysis of the dLE of the integer sequences derived from L-stage primitive LFSRs. Section III applies the 0-1 test to empirically evaluate their chaotic behavior. Finally, Section IV concludes the paper.

II. Discrete Lyapunov Exponent

Since we interpret each L-bit register state of the L-stage primitive LFSR as an integer, the resulting sequence traverses all non-zero L-bit integers $\{1, 2, \ldots, 2^L - 1\}$ exactly once. Therefore, it can be viewed as a permutation. This perspective allows us to investigate its dynamical behavior using permutation-based complexity measure. In this section, we evaluate its chaotic behavior by computing the dLE [11], [12], which quantifies the average divergence rate of divergence between neighboring elements.

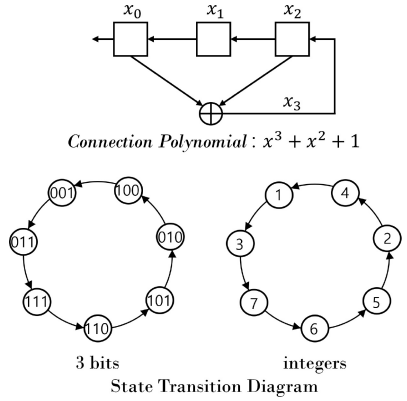

Fig. 1. Three-stage primitive LFSR and its state transition diagram with non-zero initial condition.

To clarify the notion of neighborhood in a discrete ordered set, consider the set of positive integers $\mathcal{M} := \{1, 2, \ldots, M\}$. Here, the neighbors of $i \in \mathcal{M}$ are $i-1$ and $i+1$ for $i = 2, 3, \ldots, M-1$. It is to be noted that $1 \in \mathcal{M}$ has only one neighbor 2, and $M \in \mathcal{M}$ also has only one neighbor $M-1$. Then, the dLE λ_Γ of a permutation Γ on the set of positive integers $\mathcal{M}$ is defined as follows [11], [12]:

$$\lambda_\Gamma = \frac{1}{M} \sum_{i=1}^{M} \ln d\big[\Gamma(z_i), \Gamma(z_{i+1})\big], \tag{1}$$

where $d[x, y] = |x-y|$ and $z_i = i$ for $i \in \mathcal{M}$ and $z_{M+1} = M-1$ as in [12].

A permutation Γ is said to be *discretely chaotic* if its dLE satisfies $\lim_{M\to\infty} \lambda_\Gamma > 0$, indicating persistent divergence in the transformed domain as M increases indefinitely [11], [12].

Theorem 1: Consider an L-stage primitive LFSR with a non-zero initial condition. The state transition of this LFSR as integers produces a sequence of integers in the set of $2^L - 1$ positive integers $\{1, 2, \ldots, 2^L - 1\}$, which induces a permutation F on the same set. Then, the dLE λ_F of the permutation F satisfies the following:

$$\ln\left(\sqrt{3}\right) \le \lim_{L\to\infty} \lambda_F \le \ln(2). \tag{2}$$

Proof: We begin by examining the local distances $d[F(z+1), F(z)]$ for $z \in \mathcal{S} := \{1, 2, \ldots, 2^L - 1\}$. We claim the following three items:

1) Let $\mathcal{D} := \mathcal{S} \setminus \{2^{L-1} - 1, 2^{L-1}, 2^L - 1\}$. For all $z \in \mathcal{D}$, the local distance $d[F(z+1), F(z)] \in \{1, 2, 3\}$. Moreover,
$$|\{z \in \mathcal{D} \mid d[F(z+1), F(z)] = 3\}| = |\{z \in \mathcal{D} \mid d[F(z+1), F(z)] = 1\}|. \tag{3}$$
2) For $z = 2^{L-1} - 1$, we have $F(z) = 2^L - 1$ and $F(z+1) = 1$, so that $d[F(z+1), F(z)] = 2^L - 2$.
3) For $z = 2^{L-1}$, we have $d[F(z+1), F(z)] \in \{1, 2\}$. For $z = 2^L - 1$, we have $d[F(z+1), F(z)] = d[F(z), F(z+1)] = d[F(z), F(z-1)] \in \{1, 2\}$.

To prove the first claim, we examine the update rule of the left-shifting L-stage primitive LFSR with a feedback bit determined by the connection logic. When each L-bit state is interpreted as an integer z, the update rule defines the map F as follows:

$$
\begin{aligned}
1 &= 0\,0\,0\,\cdots\,0\,0\,1\\
2 &= 0\,0\,0\,\cdots\,0\,1\,0\\
&\ \ \vdots\\
2^{L-1}-1 &= 0\,1\,1\,\cdots\,1\,1\,1\\
2^{L-1} &= 1\,0\,0\,\cdots\,0\,0\,0\\
2^{L-1}+1 &= 1\,0\,0\,\cdots\,0\,0\,1\\
2^{L-1}+2 &= 1\,0\,0\,\cdots\,0\,1\,0\\
&\ \ \vdots\\
2^{L}-1 &= 1\,1\,1\,\cdots\,1\,1\,1
\end{aligned}
$$

Fig. 2. Binary representation of $z \in \mathcal{S} = \{1, 2, \ldots, 2^L - 1\}$.

$$
\begin{aligned}
F(z) &\equiv 2z \mod 2^L \quad \text{when the feedback is 0}\\
F(z) &\equiv 2z+1 \mod 2^L \quad \text{when the feedback is 1.}
\end{aligned}
$$

Similarly, we see that $F(z+1)$ also takes the form $2(z+1)$ or $2(z+1)+1$ modulo 2^L depending on the feedback. Therefore, the difference $d[F(z+1), F(z)]$ must fall into one of the following four cases:

(i) $|2z - 2(z+1)| = 2$,
(ii) $|2z - (2(z+1)+1)| = 3$,
(iii) $|(2z+1) - 2(z+1)| = 1$,
(iv) $|(2z+1) - (2(z+1)+1)| = 2$.

Therefore, for all $z \in \mathcal{D}$, the local distance $d[F(z+1), F(z)] \in \{1, 2, 3\}$. Here, we note that $2(z+1)$ or $2(z+1)+1$ is more than 2^L if and only if $2z$ or $2z+1$ is more than 2^L, and hence, the modular reduction can be ignored in the difference $F(z+1) - F(z)$.

Now, we observe the binary representation of $z \in \mathcal{S} = \{1, 2, \ldots, 2^L - 1\}$ as shown in Fig. 2. For $z \in [1, 2^{L-1} - 1]$, the lower $L-1$ bits of z and $z + 2^{L-1}$ are the same, while the most significant bits (MSBs) of them are different. Since the MSB corresponds to the x^0 term in the connection polynomial, which always contributes to the feedback bit, it follows that for all $z \in \mathcal{D}$, $F(z)$ and $F(z + 2^{L-1})$ differ only in the least significant bit (LSB). Consequently, if $d[F(z+1), F(z)] = 3$, then $d[F(z+2^{L-1}+1), F(z+2^{L-1})] = 1$, and vice versa. This one-to-one correspondence implies (3).

To prove the second claim, we analyze the local distance for $z = 2^{L-1} - 1$. A primitive polynomial over the binary field always has an odd number of nonzero terms, and the feedback bit is computed by XORing the register bits corresponding to the nonzero coefficients, excluding the highest-degree term x^L. The binary representation of $2^{L-1} - 1$ has a 0 in the MSB (which always contributes to the feedback) and 1s in the remaining $L-1$ positions. Since the number of contributing terms excluding x^L is even, the feedback bit is given by the XOR of the MSB (which is 0) and an odd number of 1s among the remaining bits. Thus, the feedback bit becomes 1, and we obtain $F(2^{L-1} - 1) = 2^L - 1$.

In contrast, the binary representation of the next value $z + 1 = 2^{L-1}$ has a 1 in the MSB and 0s elsewhere, clearly yielding $F(2^{L-1}) = 1$. Therefore, the local distance is $d[F(2^{L-1}), F(2^{L-1} - 1)] = 2^L - 2$.

Next, we consider the third case with $z = 2^{L-1}$. As previously determined, $F(2^{L-1}) = 1$. The binary representation of the next value, $z + 1 = 2^{L-1} + 1$, has 1s in both the MSB and LSB. The LSB corresponds to the x^{L-1} term and contributes to the feedback only if the coefficient of x^{L-1} in the connection polynomial is 1. If so, the feedback bit becomes 0 and $F(2^{L-1} + 1) = 2$; otherwise, the feedback bit is 1 and $F(2^{L-1} + 1) = 3$. Therefore, the $d[F(2^{L-1} + 1), F(2^{L-1})] = 1$ if the coefficient of x^{L-1} is 1, and $d[F(2^{L-1}+1), F(2^{L-1})] = 2$ otherwise.

The case for $z = 2^L - 1$ can be analyzed in a similar manner. By the same logic, $d[F(2^L - 2), F(2^L - 1)]$ becomes 1 if the coefficient of x^{L-1} is 1, and 2 otherwise.

As a summary, we classify the values $d[F(z+1), F(z)]$ for $z \in \mathcal{S} = \{1, 2, \ldots, 2^L - 1\}$ according to whether the coefficient of x^{L-1} is 1 or 0.

- For the case where the coefficient of x^{L-1} is 1, let

$$
\begin{aligned}
\alpha_1 &= |\{z \in \mathcal{S} \mid d[F(z+1), F(z)] = 3\}|,\\
\beta_1 &= |\{z \in \mathcal{S} \mid d[F(z+1), F(z)] = 2\}|.
\end{aligned}
$$

  Then,

$$
|\{z \in \mathcal{S} \mid d[F(z+1), F(z)] = 1\}| = \alpha_1 + 2.
$$

  Since there is one instance of $d[F(z+1), F(z)] = 2^L - 2$, we have

$$
2\alpha_1 + \beta_1 + 3 = 2^L - 1.
$$

- For the case where the coefficient of x^{L-1} is 0, let

$$
\begin{aligned}
\alpha_0 &= |\{z \in \mathcal{S} \mid d[F(z+1), F(z)] = 3\}|,\\
\beta_0 &= |\{z \in \mathcal{S} \mid d[F(z+1), F(z)] = 2\}|.
\end{aligned}
$$

  Then,

$$
|\{z \in \mathcal{S} \mid d[F(z+1), F(z)] = 1\}| = \alpha_0.
$$

  Since there is also one instance of $d[F(z+1), F(z)] = 2^L - 2$, we have

$$
2\alpha_0 + \beta_0 + 1 = 2^L - 1.
$$

Finally, the dLE λ_F can be expressed as:

$$
\begin{aligned}
\lambda_F &= \frac{\alpha \ln 3 + \beta \ln 2 + \ln\left(2^L - 2\right)}{2^L - 1}\\
&= \frac{\ln\left(3^\alpha 2^\beta\right) + \ln\left(2^L - 2\right)}{2^L - 1},
\end{aligned}
$$

where $\alpha = \alpha_1$, $\beta = \beta_1$ when the coefficient of x^{L-1} is 1, and $\alpha = \alpha_0$, $\beta = \beta_0$ when the coefficient is 0. Since $\sqrt{3} < 2$ and $3 < 2^2$, we can express λ_F as follows:

$$
\frac{\ln\left(\sqrt{3}^{2\alpha+\beta}\right) + \ln\left(2^L - 2\right)}{2^L - 1} < \lambda_F < \frac{\ln\left(2^{2\alpha+\beta}\right) + \ln\left(2^L - 2\right)}{2^L - 1}
$$

Since $2\alpha + \beta = 2\alpha_1 + \beta_1 = 2^L - 4$ or $2\alpha + \beta = 2\alpha_0 + \beta_0 = 2^L - 2$, as $L \to \infty$ we have the inequality (2). ■

Therefore, the dLE of F is guaranteed to be asymptotically positive as L increases. This ensures that the integer sequence generated by an L-stage primitive LFSR inherently possesses the fundamental property of discrete chaos, namely, asymptotic divergence in the discrete phase space [11], [12].

An m-sequence can also be generated using the reciprocal of a given primitive polynomial [23], [24], [25]. This implementation produces the m-sequence in reverse order compared to the one generated by the original polynomial. However, this symmetry does not carry over to the corresponding integer sequences. Since the integer value depends on each L-bit state, reversing the state transition results in different permutation. This implies that the integer sequence is not simply the

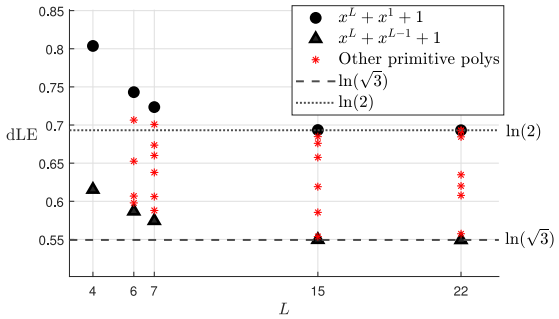

Fig. 3. Discrete Lyapunov exponents of the integer sequences generated by L-stage primitive LFSRs for $L = 4, 6, 7, 15, 22$, using various primitive polynomials.

reversed version of the original, but rather a distinct permutation determined by the choice of the connection polynomial.

The dLE λ_F of the integer sequence derived from an L-stage primitive LFSR depends on the choice of the primitive polynomial used in the LFSR. Specifically, if the primitive polynomial used in the LFSR is of the form $x^L + x^{L-1} + 1$, then $\lim_{L\to\infty} \lambda_F = \ln(\sqrt{3})$. On the other hand, if it is of the form $x^L + x + 1$, then $\lim_{L\to\infty} \lambda_F = \ln(2)$. These two polynomials are reciprocal to each other and generate reversed m-sequences. However, the permutations defined by the corresponding integer sequences are different and thus yield different dLE values.

Figure 3 shows the dLEs of the permutations defined by the integer sequences from L-stage primitive LFSRs with $L = 4, 6, 7, 15, 22$, using various primitive polynomials. These values of L are specifically chosen because both $x^L + x + 1$ and $x^L + x^{L-1} + 1$ are known to be primitive polynomials. As discussed above, the dLEs obtained from $x^L + x + 1$ and $x^L + x^{L-1} + 1$ approach from above the upper and lower bounds in (2), respectively, as L increases indefinitely. In contrast, the dLEs from other primitive polynomials approach some values in the range given in (2). Notably, we would like to concentrate on the dLEs for $L = 15$ and 22. The dLE values from $x^L + x + 1$ for $L = 15$ and 22 are the same as $\ln(2)$ within 3 and 4 decimal digits, respectively, from above. Also, those from $x^L + x^{L-1} + 1$ for these L are the same as $\ln(\sqrt{3})$ within 3 and 4 decimal digits, similarly. From Theorem 1 and some experimental results, we may say that dLE values for any finite L (at least 15) must be in the range between $\ln(\sqrt{3})$ and $\ln(2) + \epsilon$ for some small value of ϵ. Therefore, we may conclude that dLE $> \ln(\sqrt{3})$ for any finite L.

III. The 0-1 Test

To further verify the chaotic nature of the integer sequences derived from L-stage primitive LFSRs, we apply the 0-1 test, a widely used tool for detecting chaos in deterministic systems. This test directly evaluates a discrete dynamic system using only the time series, without requiring any preprocessing or transformation [17].

Given a time series $\{x_i\}$, $i = 1, 2, \ldots, N$, the test constructs a two-dimensional system $(p_c(n), q_c(n))$ as follows:

$$p_c(n) = \sum_{i=1}^{n} x_i \cos(ic), \quad q_c(n) = \sum_{i=1}^{n} x_i \sin(ic),$$

where $c \in (0, \pi)$ is a constant and $n = 1, 2, \ldots, N$.

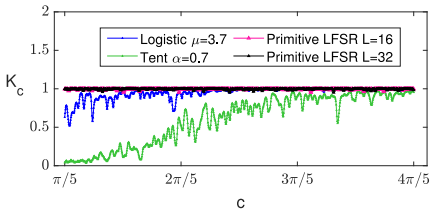

Fig. 4. Comparison of the 0-1 test results for the sequences generated by the Logistic map, Tent map, and L-stage primitive LFSRs (L=16 and L=32).

The mean square displacement $M_c(n)$ is defined as follows with the condition $n \ll N$. In practice, a choice $n \le N/10$ is recommended [17]:

$$M_c(n) = \frac{1}{N-n} \sum_{i=1}^{N-n} \Big[(p_c(i+n) - p_c(i))^2 + (q_c(i+n) - q_c(i))^2 \Big].$$

If the system is chaotic, $M_c(n)$ increases linearly with n; otherwise, it remains bounded [17]. To quantify the growth rate, the test computes the correlation coefficient K_c between the sequences $M_c(n)$ and n. Let $\xi = (1, 2, \ldots, n)$, $\Delta = (M_c(1), M_c(2), \ldots, M_c(n))$. Then, the correlation coefficient is defined as

$$K_c = \mathrm{corr}(\xi, \Delta) = \frac{\mathrm{cov}(\xi, \Delta)}{\sqrt{\mathrm{var}(\xi)\mathrm{var}(\Delta)}},$$

where $\mathrm{cov}(\cdot, \cdot)$ and $\mathrm{var}(\cdot)$ denote covariance and variance, respectively.

To ensure robustness against the choice of c, the test evaluates K_c for multiple values of c sampled from $(0, \pi)$. In practice, selecting 100 distinct values of c is considered sufficient to obtain a reliable estimate [17]. The final test statistic is defined as $K = \mathrm{median}(K_c)$. A value of K close to 1 indicates chaotic dynamics, while a value close to 0 suggests regular behavior [17].

Based on this framework, we apply the 0-1 test to the integer sequences generated by L-stage primitive LFSRs and evaluate their dynamical behavior in terms of the correlation statistic K and the trajectory pattern in the (p_c, q_c) plane.

Figure 4 shows the results of the 0-1 test applied to the integer sequences generated by L-stage primitive LFSR with $L = 16$ and 32, compared with time series produced by the logistic and tent maps under control parameters known to exhibit chaotic behavior. The control parameter μ of the logistic map is known to induce chaotic behavior when $3.57 < \mu \le 4$[13], while the tent map exhibits chaos when the control parameter α lies in the range $0.5 < \alpha < 1$[19]. Based on these known conditions, we select $\mu = 3.7$ for the logistic map and $\alpha = 0.7$ for the tent map. For each system, a sequence of length 5000 is generated. In the case of the L-stage primitive LFSR, we use $x^{16} + x^{12} + x^3 + x + 1$ for $L = 16$ and $x^{32} + x^{22} + x^2 + x + 1$ for $L = 32$ as the connection polynomials. The parameter c is uniformly sampled from $[\pi/5, 4\pi/5]$ with 1000 points, and K_c is computed for each c.

As shown in Fig. 4, the integer sequences generated by L-stage primitive LFSRs exhibits stable and high K_c values across all c, comparable to the chaotic maps. The median value

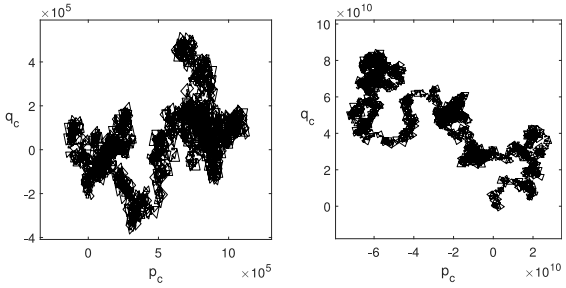

Fig. 5. Trajectories in the (p_c, q_c) plane for integer sequences generated by L-stage primitive LFSRs with $L = 16$ (left) and $L = 32$ (right).

of K_c, denoted by K, is 0.99813 for $L = 16$ and 0.99799 for $L = 32$, confirming that the integer sequences generated by L-stage primitive LFSRs can be regarded as chaotic.

Figure 5 shows the trajectories in the (p_c, q_c) plane for the integer sequences generated by L-stage primitive LFSRs with $L = 16$ and 32. The same primitive polynomials used in Fig. 4 are employed. In the 0-1 test, chaotic dynamics are indicated by unbounded and irregular trajectories in the (p_c, q_c) plane without a clear closed structure–resembling Brownian motion [17], [18]. This contrasts with regular dynamics, where trajectories are typically bounded and form repetitive or symmetric patterns. As shown in Fig. 5, both trajectories display this Brownian motion-like behavior: they are unbounded, irregular, and lack any closed structure. These results consistently suggest that the integer sequences generated by L-stage primitive LFSRs can be regarded as chaotic under the 0-1 test, even for finite L.

IV. Conclusion

This brief has investigated the chaotic nature of integer sequences derived from L-stage primitive LFSRs by interpreting the internal register states as integers. Although LFSRs are inherently deterministic and linear, the resulting integer sequences exhibit discrete chaotic behavior when viewed as permutations over the set of non-zero L-bit integers.

We analytically derived the discrete Lyapunov exponent of the induced permutation and showed that it converges to a positive value as the register length L increases. This satisfies the definition of discrete chaos and confirms that the integer sequences have an asymptotically positive spreading rate. In addition, the 0-1 test demonstrated high K values and Brownian motion-like behavior in the (p_c, q_c) plane, further validating the chaotic dynamics of the sequences.

References

[1] N. Masuda and K. Aihara, "Cryptosystems with discretized chaotic maps," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 49, no. 1, pp. 28–40, Jan. 2002.

[2] I. Öztürk and R. Kiliç, "Utilizing true periodic orbits in chaos-based cryptography," *Nonlin. Dyn.*, vol. 103, pp. 2805–2818, Feb. 2021.

[3] Y. Zhou, Z. Hua, C.-M. Pun, and C. P. Chen, "Cascade chaotic system with applications," *IEEE Trans. Cybern.*, vol. 45, no. 9, pp. 2001–2012, Sep. 2015.

[4] D. Wu, X. Zhang, J. Wang, L. Li, and G. Feng, "Novel robust video watermarking scheme based on concentric ring subband and visual cryptography with piecewise linear chaotic mapping," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 34, no. 10, pp. 10281–10298, Oct. 2024.

[5] G. Yuan, Z. Chen, X. Gao, and Y. Zhang, "Enhancing the security of chaotic direct sequence spread spectrum communication through WFRFT," *IEEE Commun. Lett.*, vol. 25, no. 9, pp. 2834–2838, Sep. 2021.

[6] M. Delgado-Restituto and A. Rodriguez-Vazquez, "Integrated chaos generators," *Proc. IEEE*, vol. 90, no. 5, pp. 747–767, May 2002.

[7] C. Li, B. Feng, S. Li, J. Kurths, and G. Chen, "Dynamic analysis of digital chaotic maps via state-mapping networks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 66, no. 6, pp. 2322–2335, Jun. 2019.

[8] C. E. C. Souza, D. P. B. Chaves, and C. Pimentel, "One-dimensional pseudo-chaotic sequences based on the discrete Arnold's cat map over $\mathbb{Z}_{3^m}$," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 1, pp. 491–495, Jan. 2021.

[9] C. Fan and Q. Ding, "Analysis and resistance of dynamic degradation of digital chaos via functional graphs," *Nonlin. Dyn.*, vol. 103, no. 1, pp. 1081–1097, Jan. 2021.

[10] Z. Galias, "Dynamics of the Hénon map in the digital domain," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 70, no. 1, pp. 388–398, Jan. 2023.

[11] L. Kocarev and J. Szczepanski, "Finite-space Lyapunov exponents and pseudochaos," *Phys. Rev. Lett.*, vol. 93, Dec. 2004, Art. no. 234101.

[12] L. Kocarev, J. Szczepanski, J. M. Amigo, and I. Tomovski, "Discrete chaos-I: Theory," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 53, no. 6, pp. 1300–1309, Jun. 2006.

[13] S.-L. Chen, T. Hwang, and W.-W. Lin, "Randomness enhancement using digitalized modified logistic map," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 57, no. 12, pp. 996–1000, Dec. 2010.

[14] A. Broumandnia, "Image encryption algorithm based on the finite fields in chaotic maps," *J. Inf. Secur. Appl.*, vol. 54, Oct. 2020, Art. no. 102553.

[15] A. Broumandnia, "Designing digital image encryption using 2D and 3D reversible modular chaotic maps," *J. Inf. Secur. Appl.*, vol. 47, pp. 188–198, Aug. 2019.

[16] D. Lambic, "A new discrete chaotic map based on the composition of permutations," *Chaos, Solitons Fractals*, vol. 78, pp. 245–248, Sep. 2015.

[17] G. A. Gottwald and I. Melbourne, *The 0-1 Test for Chaos: A Review.*. Berlin, Germany: Springer, 2016, pp. 221–247.

[18] M. Nazish and M. T. Banday, "A novel fibonacci-sequence-based chaotification model for enhancing chaos in one-dimensional maps," *IEEE Internet Things J.*, vol. 11, no. 24, pp. 40268–40277, Dec. 2024.

[19] J. Tang, Z. Zhang, P. Chen, Z. Huang, and T. Huang, "A simple chaotic model with complex chaotic behaviors and its hardware implementation," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 70, no. 9, pp. 3676–3688, Sep. 2023.

[20] J. Tang, Z. Zhang, and T. Huang, "Two-dimensional cosine-sine interleaved chaotic system for secure communication," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 71, no. 4, pp. 2479–2483, Apr. 2024.

[21] X. Wang, N. Guan, and J. Yang, "Image encryption algorithm with random scrambling based on one-dimensional logistic self-embedding chaotic map," *Chaos, Solitons Fractals*, vol. 150, Sep. 2021, Art. no. 111117.

[22] D. Lambic, "A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design," *Nonlin. Dyn.*, vol. 100, no. 1, pp. 699–711, Mar. 2020.

[23] S. W. Golomb, *Shift Register Sequences*, 3rd ed. Hackensack, NJ, USA: World Sci., 2017.

[24] S. W. Golomb and G. Gong, *Signal Design for Good Correlation for Wireless Communications, Cryptography, and Radar*. New York, NY, USA: Cambridge Univ. Press, 2005.

[25] H.-Y. Song, "Feedback shift register sequences," in *Wiley Encyclopedia of Telecommunications*. Hoboken, NJ, USA: Wiley, 2003.