SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Some characteristics of logistic map over the finite field

Bo YANG & XiaoFeng LIAO*

Chongqing Key Laboratory of Nonlinear Circuits and Intelligent Information Processing, College of Electronic and Information Engineering, Southwest University, Chongqing 400715*, China*

Appendix A Lemma 1 proof

By (2), and $-1 \equiv N-1 (\mathrm{mod}\ N)$,

$$\begin{aligned} L2_{\mathbf{Z}_N}(X_i) &= (N-1) - \tfrac{\mu_N X_i^2}{N-1} \pmod N, \\ &\equiv -1 - \tfrac{\mu_N X_i^2}{-1} \pmod N, \\ &\equiv \mu_N X_i^2 - 1 \pmod N. \end{aligned}$$

Example 1. When $\mu_N = 122, X_0 = 1, n = 7$, the sequences of $L1_{\mathbf{Z}_N}(X_i)$ are (1, 116, 104, 16, 32, 64, 0, 0, 0, $\cdots$).

Appendix B Theorem 2 proof

Let

$$f(z) = \frac{2z - B}{2A}, \tag{B1}$$

and

$$f^{-1}(z) = \frac{2Az + B}{2}, \tag{B2}$$

then

$$\phi^f(z) = (f^{-1} \circ \phi \circ f)(z) = z^2 + (AC - \frac{1}{4}B^2 + \frac{1}{2}B). \tag{B3}$$

We define $c = AC - \frac{1}{4}B^2 + \frac{1}{2}B$, and $\phi(z) = Az^2 + Bz + C$ can be changed into the form $\phi^f(z) = z^2 + c$ with a simple entirely transformation in the field K. And we have that $f(z_i)$ is a n periodic point of $\phi^f(z)$ when z_i just is a n periodic point of ϕ.

Appendix C Theorem 3 proof

Suppose that $|c| > 2$, $z_n = \phi_c^n(0)$ where ϕ^n is the iterates of ϕ.

$$|z_{n+1}| \geqslant |z_n^2| - |c| = (|z_n| - |c|) + |z_n| \cdot (|z_n| - 1). \tag{C1}$$

We get $|z_1| = |c| > 2$ with supposing, then (C1) and mathematical induction tells us first that the sequence $|z_n|$ may be increasing, and indeed that

$$|z_{n+1}| \geqslant |z_1|(|z_1| - 1)^2 = |c|(|c| - 1)^n.$$

So $|z_n| \to \infty$, and c is not in M.

* Corresponding author (email: xfliao@swu.edu.cn)

Appendix D Theorem 4 proof

According to Theorem 3, for simplicity, firstly we discuss $\mu_N = 3$, then $c = \frac{1}{4}(2\mu_N - \mu_N^2) = -\frac{3}{4}$. Letting $\phi_c(z) = \phi^f(z) = z^2 + c$, if $c = -\frac{3}{4}$, $\phi_c(z) = z^2 - \frac{3}{4}$, so the resultant $\mathrm{Res}(\Phi_m^*(z), \Phi_n^*(z)) = \mathrm{Res}(\Phi_1^*, \Phi_2^*) = 0$ where Φ^* is a nth dynatomic polynomial, and it indicates that $\phi_c(z) = z^2 - \frac{3}{4}$ has the period form as the type (m, n) which is (1, 2) as we know in Definition 2. If $\phi_c^n(z_i) = z_i$, thus z_i is a fixed point of ϕ_c^n. Then the solution of equation $z^2 - \frac{3}{4} = z$ is the fixed point of $\phi_c(z)$, so we get two fixed points $z' = -\frac{1}{2}$ and $z'' = \frac{3}{2}$.

Thus when $c = -\frac{3}{4}$ and $z' = -\frac{1}{2}$, we have

$$-\frac{1}{2} \xrightarrow{\phi_{-\frac{3}{4}}} -\frac{1}{2} \xrightarrow{\phi_{-\frac{3}{4}}} -\frac{1}{2} \xrightarrow{\phi_{-\frac{3}{4}}} \cdots, \tag{D1}$$

and when $c = -\frac{3}{4}$ and $z'' = \frac{3}{2}$, we have

$$\frac{3}{2} \xrightarrow{\phi_{-\frac{3}{4}}} \frac{3}{2} \xrightarrow{\phi_{-\frac{3}{4}}} \frac{3}{2} \xrightarrow{\phi_{-\frac{3}{4}}} \cdots. \tag{D2}$$

But when $z_0 = -\frac{1}{2}$, $X_0 = f^{-1}(z_0) = \mu_N z_0 + \frac{1}{2}\mu_N = 0$. In order to avoid the initial value of $L_{\mathbf{Z}_N}(X_i)$ is 0, we calculate $\phi_c^{-1}(-\frac{1}{2}) = \frac{1}{2}$ or $-\frac{1}{2}$, and we take $\phi_c^{-1}(-\frac{1}{2}) = \frac{1}{2}$, then $X_0 = f^{-1}(z_0) = f^{-1}(\frac{1}{2}) = \frac{1}{2}\mu_N + \frac{1}{2}\mu_N = \mu_N = 3$.

And when $z_0 = \frac{3}{2}$, $X_0 = f^{-1}(z_0) = \mu_N z_0 + \frac{1}{2}\mu_N = 2\mu_N$, where the value of X_0 is 2 times μ_N, so we take $X_0 = \mu_N = 3$.

When $\mu_N = 3$, $X_0 = 3$, $n = 1$, with (1), $X_0 + 1 = 4 = 2N$, so the final value of $L1_{\mathbf{Z}_N}(X_i)$ is 0. When $\mu_N = 3$, $X_0 = 3$, $n = 2$, by using (1), $X_0 + 1 = 4 = N$, so the final value of $L1_{\mathbf{Z}_N}(X_i)$ is 0. When $\mu_N = 3$, $X_0 = 3$, $n = 3$, the sequences of $L1_{\mathbf{Z}_N}(X_i)$ are (3, 4, 4, 4, 4, 4, $\cdots$). When $\mu_N = 3$, $X_0 = 3$, $n = 4$, the sequences of $L1_{\mathbf{Z}_N}(X_i)$ are (3, 4, 12, 4, 12, 4, $\cdots$). When $\mu_N = 3$, $X_0 = 3$, $n = 5$, the sequences of $L1_{\mathbf{Z}_N}(X_i)$ are (3, 4, 28, 4, 28, 4, $\cdots$).

When $\mu_N = 3$, $X_0 = 3$, $n > 5$, let $L1_{\mathbf{Z}_N}^T(X_i)$ be the period transformation of $L1_{\mathbf{Z}_N}(X_i)$, by Lemma 2,

$$\begin{aligned}
&L1_{\mathbf{Z}_N}^T(3) = L_{\mathbf{Z}_N}(N - 1 - 3),\\
&L1_{\mathbf{Z}_N}^T(3) = 3 \cdot (N - 1 - 3)(N - 1 - 3 + 1) \pmod N,\\
&L1_{\mathbf{Z}_N}^T(3) = 3 \cdot (N - 4)(N - 3) \pmod N,\\
&L1_{\mathbf{Z}_N}^T(3) = 3 \cdot (N^2 - 7 \cdot N + 12) \pmod N,\\
&L1_{\mathbf{Z}_N}^T(3) = 36 \pmod N,\\
&\qquad T = \tfrac{N}{16} = 2^{n-4}.
\end{aligned}$$

Because $c = \frac{1}{4}(2\mu_N - \mu_N^2) = \frac{1}{4} - \frac{1}{4}(\mu_N - 1)^2$, and $\mu_N \equiv 3 \bmod 4$, $\mu_N - 3 \equiv 0 \bmod 4$, $(\mu_N - 1)^2 = (\mu_N - 3 + 2)^2 = (\mu_N - 3)^2 + 4(\mu_N - 3) + 4 \equiv 0 \bmod 4$, the period of $L1_{\mathbf{Z}_N}(X_i)$ when $\mu_N \bmod 4 = 3$ is the same as that of $L1_{\mathbf{Z}_N}(X_i)$ when $\mu_N = 3$, and the maximum period of $L1_{\mathbf{Z}_N}(X_i)$ is $\frac{N}{16} = 2^{n-4}$.

Example 2. When $\mu_N = 19$, $X_0 = 3$, $n = 7$, the sequences of $L1_{\mathbf{Z}_N}(X_i)$ are (3, 100, 28, 68, 60, 36, 92, 4, 124, 100, 28, 68, $\cdots$), and the period of $L1_{\mathbf{Z}_N}(X_i)$ is 8.

Appendix E Theorem 5 proof

Firstly, we discuss $\mu_N = 1$, and $c = \frac{1}{4}(2\mu_N - \mu_N^2) = \frac{1}{4}$. Let $\phi_c(z) = \phi^f(z) = z^2 + c$, if $c = \frac{1}{4}$, $\phi_c(z) = z^2 + \frac{1}{4}$, then the solution of equation $z^2 + \frac{1}{4} = z$ is the fixed point of $\phi_c(z)$, so we get one fixed point $z' = \frac{1}{2}$.

Thus when $c = \frac{1}{4}$ and $z' = \frac{1}{2}$, we have

$$\frac{1}{2} \xrightarrow{\phi_{\frac{1}{4}}} \frac{1}{2} \xrightarrow{\phi_{\frac{1}{4}}} \frac{1}{2} \xrightarrow{\phi_{\frac{1}{4}}} \cdots. \tag{E1}$$

And when $z_0 = \frac{1}{2}$, $X_0 = f^{-1}(z_0) = \mu_N z_0 + \frac{1}{2}\mu_N = \mu_N$, so we take $X_0 = \mu_N = 1$.

When $\mu_N = 1$, $X_0 = 1$, $n = 1$, with (1), $X_0 + 1 = 2 = N$, so the final value of $L_{\mathbf{Z}_N}(X_i)$ is 0. When $\mu_N = 1$, $X_0 = 1$, $n = 2$, the sequences of $L1_{\mathbf{Z}_N}(X_i)$ are (1, 2, 2, 2, 2, 2, $\cdots$). When $\mu_N = 1$, $X_0 = 1$, $n > 2$, by Lemma 2,

$$\begin{aligned}
&L1_{\mathbf{Z}_N}^T(1) = L1_{\mathbf{Z}_N}(N - 1 - 1),\\
&L1_{\mathbf{Z}_N}^T(1) = 1 \cdot (N - 1 - 1)(N - 1 - 1 + 1) \pmod N,\\
&L1_{\mathbf{Z}_N}^T(1) = 1 \cdot (N - 2)(N - 1) \pmod N,\\
&L1_{\mathbf{Z}_N}^T(1) = 1 \cdot (N^2 - 3 \cdot N + 2) \pmod N,\\
&L1_{\mathbf{Z}_N}^T(1) = 2 \pmod N,\\
&\qquad T = \tfrac{N}{4} = 2^{n-2}.
\end{aligned}$$

Because $\mu_N \equiv 1 \bmod 4$, the period of $L1_{\mathbf{Z}_N}(X_i)$ when $\mu_N \bmod 4 = 1$ is the same as that of $L1_{\mathbf{Z}_N}(X_i)$ when $\mu_N = 1$, and the maximum period of $L1_{\mathbf{Z}_N}(X_i)$ is $\frac{N}{4} = 2^{n-2}$.

Example 3. When $\mu_N = 5$, $X_0 = 1$, $n = 5$, the sequences of $L1_{\mathbf{Z}_N}(X_i)$ are (1, 10, 6, 18, 14, 26, 22, 2, 30, 10, 6, 18, $\cdots$), and the period of $L1_{\mathbf{Z}_N}(X_i)$ is 8.

Appendix F Lemma 3 proof

With Lemma 1, Theorem 2 and (B3), let $A = \mu_N$, $B = 0$, $C = -1$, then

$$f(z) = \frac{1}{\mu_N} z, \tag{F1}$$

and

$$f^{-1}(z) = \mu_N z, \tag{F2}$$

then

$$\begin{aligned} L2^f(X_i) = L2^f_{\mathbf{Z}_N}(X_i) &= (f^{-1} \circ L_{Z_N} \circ f)(X_i), \\ &= X_i^2 - \mu_N. \end{aligned} \tag{F3}$$

Let $c = -\mu_N$,

$$L2^f(X_i) = X_i^2 + c.$$

Appendix G Theorem 6 proof

Firstly, we discuss $\mu_N = 0$, and $c = -\mu_N = 0$. Let $\phi_c(z) = \phi^f(z) = z^2 + c$, if $c = 0$, $\phi_c(z) = z^2$. Thus for $c = 0$, we get

$$0 \xrightarrow{\phi_0} 0 \xrightarrow{\phi_0} 0 \xrightarrow{\phi_0} \cdots, \tag{G1}$$

and

$$1 \xrightarrow{\phi_0} 1 \xrightarrow{\phi_0} 1 \xrightarrow{\phi_0} \cdots, \tag{G2}$$

so $\phi_c(z)$ has period as the type $(1, 1)$ as we know in Definition 2. So the periodic properties of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N = 0$ are the same of $\phi_c(z) = z^2$, and because $\mu_N \equiv 0 \bmod 9$, the period of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N \bmod 9 = 0$ is the same as that of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N = 0$. The period of $L2_{\mathbf{Z}_N}(X_i)$ is 1, and the final value of $L2_{\mathbf{Z}_N}(X_i)$ is a constant C when $\mu_N \bmod 9 = 0$.

When $\mu_N = 6$, then $c = -\mu_N = -6$, $\phi_c(z) = z^2 - 6$. Thus for $c = -6$, we have

$$-2 \xrightarrow{\phi_{-6}} -2 \xrightarrow{\phi_{-6}} -2 \xrightarrow{\phi_{-6}} \cdots, \tag{G3}$$

and

$$3 \xrightarrow{\phi_{-6}} 3 \xrightarrow{\phi_{-6}} 3 \xrightarrow{\phi_{-6}} \cdots, \tag{G4}$$

so $\phi_c(z)$ has period as the type $(1, 1)$ as we know in Definition 2. So the periodic properties of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N = 6$ are the same of $\phi_c(z) = z^2 - 6$, and because $\mu_N \equiv 6 \bmod 9$, the period of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N \bmod 9 = 6$ is the same as that of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N = 6$. The period of $L2_{\mathbf{Z}_N}(X_i)$ is 1, and the final value of $L2_{\mathbf{Z}_N}(X_i)$ is a constant C when $\mu_N \bmod 9 = 6$.

When $\mu_N \bmod 9 = 3$, then $c = -\mu_N = -3$, $\phi_c(z) = z^2 - 3$. Because $-\mu_N \bmod 9 = -3$ and $-3 \equiv 6 \bmod 9$, $-\mu_N \bmod 9 \equiv 6$. We have the period of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N \bmod 9 = 3$ is the same as the period of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N \bmod 9 = 6$. Finally, the period of $L_{\mathbf{Z}_N}(X_i)$ is 1 if $\mu_N \bmod 9 = 0$ or 3 or 6.

Example 4. When $\mu_N = 39, X_0 = 1, n = 7$, the sequences of $L2_{\mathbf{Z}_N}(X_i)$ are (1, 38, 1640, 1505, 857, 371, 1100, 1100, $\cdots$), and the period of $L2_{\mathbf{Z}_N}(X_i)$ is 1.

Appendix H Theorem 7 proof

Firstly, we discuss $\mu_N = 1$, then $c = -\mu_N = -1$. Letting $\phi_c(z) = \phi^f(z) = z^2 + c$, if $c = -1$, $\phi_c(z) = z^2 - 1$. Thus for $c = -1$, we have

$$0 \xrightarrow{\phi_{-1}} -1 \xrightarrow{\phi_{-1}} 0 \xrightarrow{\phi_{-1}} -1 \xrightarrow{\phi_{-1}} \cdots, \tag{H1}$$

so $\phi_c(z)$ has period as the type $(1, 2)$ as we know in Definition 2. So the periodic properties of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N = 1$ are the same of $\phi_c(z) = z^2 - 1$, and because $\mu_N \equiv 1 \bmod 9$, the period of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N \bmod 9 = 1$ is the same as that of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N = 1$. The period of $L2_{\mathbf{Z}_N}(X_i)$ is 2 when $\mu_N \bmod 9 = 1$.

When $\mu_N = 4$, $\mu_N = 13 \bmod 9$ and $\mu_N \bmod 9 \equiv 13$ then $c = -\mu_N = -13$, $\phi_c(z) = z^2 - 13$. Thus for $c = -13$, we have

$$3 \xrightarrow{\phi_{-13}} -4 \xrightarrow{\phi_{-13}} 3 \xrightarrow{\phi_{-13}} -4 \xrightarrow{\phi_{-13}} \cdots, \tag{H2}$$

so $\phi_c(z)$ has period as the type $(1, 2)$ as we know in Definition 2. So the periodic properties of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N = 13$ are the same of $\phi_c(z) = z^2 - 13$, and because $\mu_N \equiv 4 \bmod 9$, the period of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N \bmod 9 = 4$ is the same as that of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N = 4$. The period of $L2_{\mathbf{Z}_N}(X_i)$ is 2 when $\mu_N \bmod 9 = 4$.

When $\mu_N = 7$, then $c = -\mu_N = -7$, $\phi_c(z) = z^2 - 7$. Thus for $c = -7$, we have

$$2 \xrightarrow{\phi_{-7}} -3 \xrightarrow{\phi_{-7}} 2 \xrightarrow{\phi_{-7}} -3 \xrightarrow{\phi_{-7}} \cdots, \tag{H3}$$

so $\phi_c(z)$ has period as the type $(1, 2)$ as we know in Definition 2. So the periodic properties of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N = 7$ are the same of $\phi_c(z) = z^2 - 7$, and because $\mu_N \equiv 7 \bmod 9$, the period of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N \bmod 9 = 7$ is the same as that of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N = 7$. The period of $L2_{\mathbf{Z}_N}(X_i)$ is 2 when $\mu_N \bmod 9 = 7$. Finally, the period of $L2_{\mathbf{Z}_N}(X_i)$ is 2 when $\mu_N \bmod 9 = 1$ or 4 or 7.

Example 5. When $\mu_N = 40$, $X_0 = 1$, $n = 7$, the sequences of $L2_{\mathbf{Z}_N}(X_i)$ are (1, 39, 1790, 1425, 2006, 426, 386, 264, 1601, 1479, 143, 21, 143, 21, $\cdots$), and the period of $L2_{\mathbf{Z}_N}(X_i)$ is 2.

Appendix I Lemma 4 proof

According Lemma 1, we have

$$\begin{aligned} L2_{\mathbf{Z}_N}(N-X_i) &\equiv (\mu_N(N-X_i)^2-1) \pmod N,\\ &\equiv (\mu_N(N-X_i)(N-X_i)-1) \pmod N,\\ &\equiv (\mu_N(N^2-2N\cdot X_i+X_i^2)-1) \pmod N,\\ &\equiv (\mu_N X_i^2-1) \pmod N,\\ &= L2_{\mathbf{Z}_N}(X_i). \end{aligned}$$

Appendix J Theorem 8 proof

Firstly, we discuss $\mu_N = 2$, and when $\mu_N = 2$, $X_0 = |c| = 2$, $n \geqslant 3$, with Lemma 4,

$$\begin{aligned} L2^T_{\mathbf{Z}_N}(2) &= L_{\mathbf{Z}_N}(N-2),\\ L2^T_{\mathbf{Z}_N}(2) &= (2N^2-8N+7) \pmod N,\\ L2^T_{\mathbf{Z}_N}(2) &= 7 \pmod N,\\ T &= \tfrac{N}{9} = 3^{n-2}. \end{aligned}$$

According to $\mu_N \equiv 2 \bmod 9$, so the period of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N \bmod 9 = 2$ is the same as that of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N = 2$, and the maximum period of $L2_{\mathbf{Z}_N}(X_i)$ is $\frac{N}{9} = 3^{n-2}$.

Example 6. When $\mu_N = 74$, $X_0 = 5$, $n = 5$, the sequences of $L2_{\mathbf{Z}_N}(X_i)$ are (5, 148, 85, 49, 40, 58, 103, 175, 31, 157, 67, 4, 211, 202, 220, 22, 94, 193, 76, 229, 166, 130, 121, 139, 184, 13, 112, 238, 148, 85, $\cdots$), and the period of $L2_{\mathbf{Z}_N}(X_i)$ is 27.

Appendix K Theorem 9 proof

Firstly, we discuss $\mu_N = 8$, and when $\mu_N = 8$, $X_0 = |c| = 8$, $n \geqslant 3$, with Lemma 4,

$$\begin{aligned} L2^T_{\mathbf{Z}_N}(8) &= L_{\mathbf{Z}_N}(N-8),\\ L2^T_{\mathbf{Z}_N}(8) &= (8N^2-128N+511) \pmod N,\\ L2^T_{\mathbf{Z}_N}(8) &= 511 \pmod N,\\ T &= \tfrac{N}{9} = 3^{n-2}. \end{aligned}$$

According to $\mu_N \equiv 8 \bmod 9$, so the period of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N \bmod 9 = 8$ is the same as that of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N = 8$, and the maximum period of $L2_{\mathbf{Z}_N}(X_i)$ is $\frac{N}{9} = 3^{n-2}$.

Example 7. When $\mu_N = 80$, $X_0 = 213$, $n = 5$, the sequences of $L2_{\mathbf{Z}_N}(X_i)$ are (213, 71, 142, 85, 145, 196, 58, 118, 7, 31, 91, 61, 4, 64, 115, 220, 37, 169, 193, 10, 223, 166, 226, 34, 139, 199, 88, 112, 172, 142, 85, 145, $\cdots$), and the period of $L2_{\mathbf{Z}_N}(X_i)$ is 27.

Appendix L Theorem 10 proof

Firstly, we discuss $\mu_N = 5$, then when $\mu_N = 5$, $X_0 = |c| = 5$, $n \geqslant 3$, with Lemma 4,

$$\begin{aligned} L2^T_{\mathbf{Z}_N}(5) &= L_{\mathbf{Z}_N}(N-5),\\ L2^T_{\mathbf{Z}_N}(5) &= (5N^2-50N+124) \pmod N,\\ L2^T_{\mathbf{Z}_N}(5) &= 124 \pmod N,\\ T &= \tfrac{N}{3} = 3^{n-1}. \end{aligned}$$

Because $\mu_N \equiv 5 \bmod 9$, the period of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N \bmod 9 = 5$ is the same as that of $L2_{\mathbf{Z}_N}(X_i)$ when $\mu_N = 5$, and the maximum period of $L2_{\mathbf{Z}_N}(X_i)$ is $\frac{N}{3} = 3^{n-1}$.

Example 8. When $\mu_N = 77$, $X_0 = 123$, $n = 5$, the sequences of $L2_{\mathbf{Z}_N}(X_i)$ are (123, 233, 166, 178, 190, 22, 88, 208, 40, 241, 64, 220, 151, 1, 76, 61, 19, 94, 214, 118, 31, 124, 55, 130, 34, 73, 148, 187, 172, 85, 97, 109, 184, 7, 127, 202, 160, 226, 139, 70, 163, 238, 223, 181, 13, 133, 37, 193, 43, 217, 49, 196, 235, 67, 106, 91, 4, 16, 28, 103, 169, 46, 121, 79, 145, 58, 232, 82, 157, 142, 100, 175, 52, 199, 112, 205, 136, 211, 115, 154, 229, 25, 10, 166, 178, 190, 22, 88, $\cdots$), and the period of $L2_{\mathbf{Z}_N}(X_i)$ is 81.

Appendix M Some other characteristics

Appendix M.1 Pseudorandom sequence

Through two Logistic maps, we can generate the sequences over the finite field. Some long periodic sequences exist that are quite useful for practical application. Thus, we generate pseudorandom sequences with different initial and control

Table M1 NIST test results

Test index	P value of $L1_{\mathbf{Z}_{3^n}}(X_i)$	P value of $L2_{\mathbf{Z}_{3^n}}(X_i)$	Results
approximate entropy	0.9599	0.8235	success
block frequency	0.4987	0.4942	success
cumulative sums	0.1302	0.1282	success
fast Fourier transform	0.4465	0.6202	success
frequency	0.4427	0.7111	success
random excursions	0.9970	0.9626	success
random excursions variant	0.6831	0.4795	success
longest runs of ones	0.2209	0.7492	success
rank	0.2919	0.2919	success
runs	0.4704	0.8791	success
serial	0.2389	0.4142	success
universal statistical	0.7467	0.6070	success

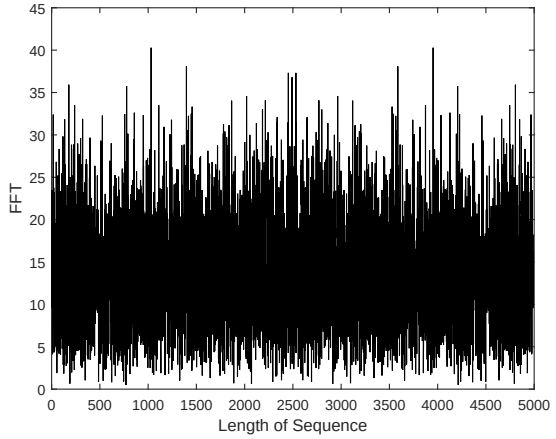

Figure M1 Power spectrum of $L1_{\mathbf{Z}_N}(X_i)$.

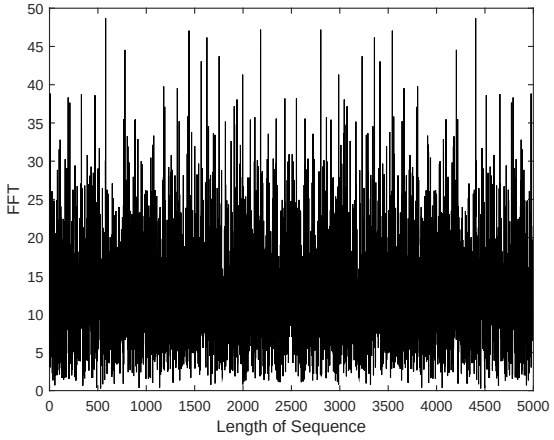

Figure M2 Power spectrum of $L2_{\mathbf{Z}_N}(X_i)$.

parameters where $L1_{\mathbf{Z}_N}(X_i)$ with $q = 3$, $N = 3^n$, $n = 13$, $X_0 = 1$, $\mu_N = 13$, and $L2_{\mathbf{Z}_N}(X_i)$ with $q = 3$, $N = 3^n$, $n = 13$, $X_0 = 1$, $\mu_N = 5$.

The NIST test is the most important norm for randomness testing, and contains a number of nearly independent statistical tests. These methods focus on many kinds of different molds of non-randomness that may exist in a particular sequence. In NIST, the important level of each method can be set at 0.01 which tells us that 99% of the test specimens pass the tests only if the random number is really random. If the P value is $\geqslant 0.01$, it tells us that the sequence will be random and its probability is 0.99. In this appendix, we use several versions of the NIST test. Table M1 shows that the sequences generated from the Logistic mapping over a finite field have good random properties that have proven to be available for a secure application.

Appendix M.2 Power spectrum

Usually, the description of a signal in the time and frequency domains is one by one. An analysis for the power spectrum (PS) can provide some information of the signal frequency domain.

Figure M1 shows a power spectrum diagram of Logistic map $L1_{\mathbf{Z}_N}(X_i)$ where $q = 3$, $N = 3^n$, $n = 13$, $X_0 = 1$, $\mu_N = 16$. Figure M2 shows the power spectrum diagram of Logistic map $L2_{\mathbf{Z}_N}(X_i)$ where $q = 3$, $N = 3^n$, $n = 13$, $X_0 = 1$, $\mu_N = 8$.

From Figure M1 and M2, we can see that the power spectrum of the Logistic mapping over the finite field has a noise background and wide peak, and is continuous, which satisfies the chaotic characteristics.

Appendix M.3 Correlation property

The correlation property is a very significant factor in evaluating the performance of a sequence generated by a chaotic map. The typical auto-correlation function (ACF) and cross-correlation function (CCF) are under ideal conditions in which the sequence length approaches ∞, but the length of the sequence is usually finite in practical application.

We define $\{X_i\}$, $\{X_{i1}\}$ and $\{X_{i2}\}$ as chaotic sequences where the finite length is H. The auto-correlation function can be abbreviated as ACF for $\{X_i\}$. The cross-correlation function can be abbreviated as CCF for $\{X_{i1}\}$ and $\{X_{i2}\}$. And the auto-correlation function of $\{X_i\}$ can be written by

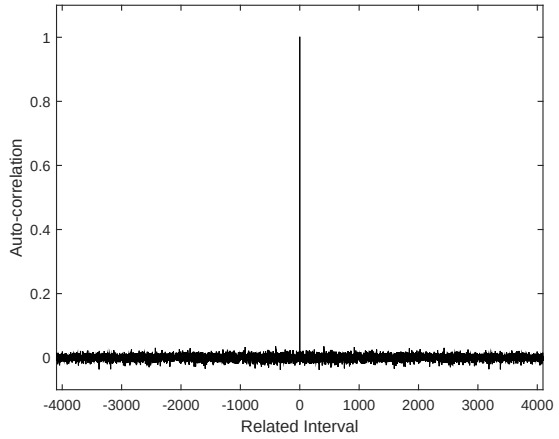

Figure M3 ACF of $L1_{\mathbf{Z}_N}(X_i)$.

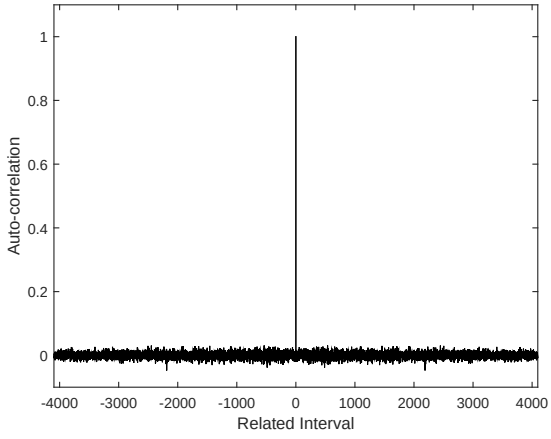

Figure M4 ACF of $L2_{\mathbf{Z}_N}(X_i)$.

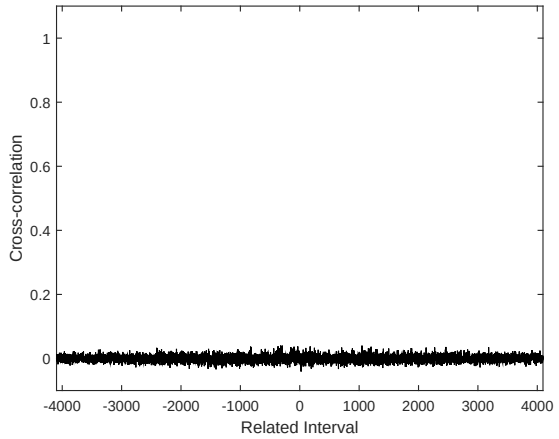

Figure M5 CCF of $L1_{\mathbf{Z}_N}(X_i)$.

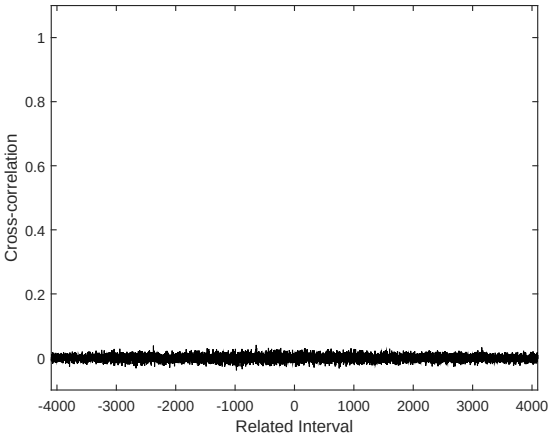

Figure M6 CCF of $L2_{\mathbf{Z}_N}(X_i)$.

$$ACF(m) = \begin{cases} \frac{1}{H-|m|}\sum_{i=0}^{H-1-|m|}(X_i - \overline{X})(X_{i+m} - \overline{X}), \\ \qquad\qquad 1-H \leqslant m \leqslant H-1, \\ 0, \qquad\qquad H \leqslant |m|. \end{cases} \tag{M1}$$

The cross-correlation function of $\{X_{i1}\}$ and $\{X_{i2}\}$ can be written by

$$CCF(m) = \begin{cases} \frac{1}{H-|m|}\sum_{i=0}^{H-1-|m|}(X_{i1} - \overline{X})(X_{(i+m)2} - \overline{X}), \\ \qquad\qquad 1-H \leqslant m \leqslant H-1, \\ 0, \qquad\qquad H \leqslant |m|. \end{cases} \tag{M2}$$

Any two different sequences $\{X_{i1}\}$ and $\{X_{i2}\}$ are relatively independent in virtue of the sensitive property of the initial parameter. If H is particularly large, and the clearance m is extremely small, the side parts of an auto-correlation, and the values of a cross-correlation of $\{X_{i1}\}$ and $\{X_{i2}\}$, approach a normal distribution when normalized.

The simulation results of the auto-correlation function regarding $L1_{\mathbf{Z}_N}(X_i)$ are shown in Figure M3, where $q = 3$, $N = 3^n$, $n = 13$, $X_0 = 1$, $\mu_N = 13$ and the sequence length is 4096. The simulation results of the auto-correlation function regarding $L2_{\mathbf{Z}_N}(X_i)$ are shown in Figure M4, where $q = 3$, $N = 3^n$, $n = 13$, $X_0 = 1$, $\mu_N = 5$ and the sequence length is 4096. According to the above two figures, we can see that the auto-correlation function regarding the Logistic map over a finite field is weak except for near time 0, and has relatively good auto-correlation and uniform distribution properties.

The simulation results of the cross-correlation function for $L1_{\mathbf{Z}_N}(X_i)$ are shown in Figure M5, where $\{X_{i1}\}$ with $q = 3$, $N = 3^n$, $n = 13$, $X_0 = 1$, $\mu_N = 13$, and $\{X_{i2}\}$ with $q = 3$, $N = 3^n$, $n = 13$, $X_0 = 1$, $\mu_N = 16$, and the sequence length is 4096. The simulation results of the cross-correlation function for $L2_{\mathbf{Z}_N}(X_i)$ are shown in Figure M6, where $\{X_{i1}\}$ with $q = 3$, $N = 3^n$, $n = 13$, $X_0 = 1$, $\mu_N = 5$, and $\{X_{i2}\}$ with $q = 3$, $N = 3^n$, $n = 13$, $X_0 = 1$, $\mu_N = 8$, and the sequence length is 4096. According to the above two figures, we can see that the cross-correlation function for a Logistic map over a finite field is very close to 0 and has relatively good cross-correlation and well uniform distribution properties.

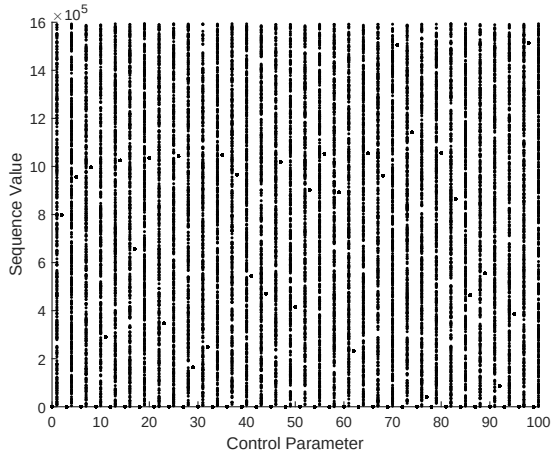

Figure M7 Phase diagram of $L1_{\mathbf{Z}_N}(X_i)$.

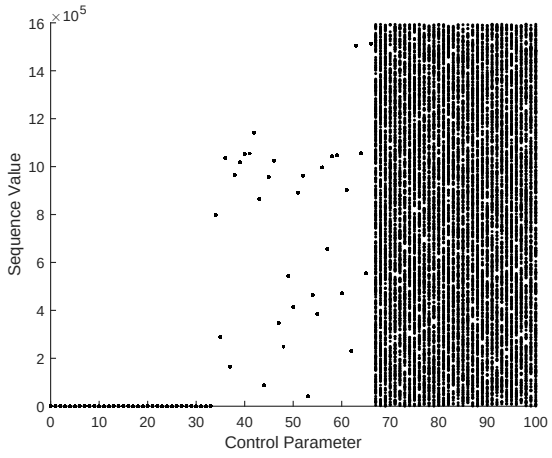

Figure M8 Phase diagram of $L1_{\mathbf{Z}_N}(X_i)$ after adjustment.

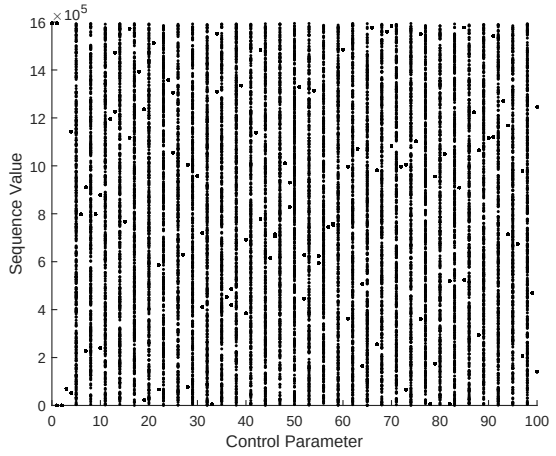

Figure M9 Phase diagram of $L2_{\mathbf{Z}_N}(X_i)$.

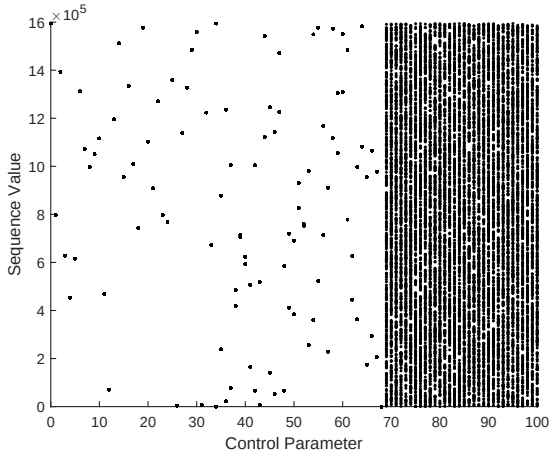

Figure M10 Phase diagram of $L2_{\mathbf{Z}_N}(X_i)$ after adjustment.

Appendix M.4 Phase diagram

The phase diagram can generally reveal the double-period process of dynamic systems, and the double-period process is one way, namely, from a nonlinear dynamic system to a state of chaos. Using the control parameter μ_N as the horizontal coordinate and the value of the mapping as the vertical coordinate, we can obtain the phase diagram of a Logistic map in a finite field.

The phase diagram of $L1_{\mathbf{Z}_N}(X_i)$ is shown in Figure M7, where $q = 3$, $N = 3^n$, $n = 13$, $X_0 = 1$, $\mu_N \in [0, 100]$. The phase diagram of $L1_{\mathbf{Z}_N}(X_i)$ after an adjustment is shown in Figure M8, where $q = 3$, $N = 3^n$, $n = 13$, $X_0 = 1$, μ_N is [$\mu_N \bmod 9 = 0$ or 3 or 6, $\mu_N \bmod 9 = 2$ or 5 or 8, $\mu_N \bmod 9 = 4$ or 7 or 1] which is [0, 9, 18, 27, 36, 45, 54, 63, 72, 81, 90, 99, 3, 12, 21, 30, 39, 48, 57, 66, 75, 84, 93, 6, 15, 24, 33, 42, 51, 60, 69, 78, 87, 96, 2, 11, 20, 29, 38, 47, 56, 65, 74, 83, 92, 5, 14, 23, 32, 41, 50, 59, 68, 77, 86, 95, 8, 17, 26, 35, 44, 53, 62, 71, 80, 89, 98, 4, 13, 22, 31, 40, 49, 58, 67, 76, 85, 94, 7, 16, 25, 34, 43, 52, 61, 70, 79, 88, 97, 1, 10, 19, 28, 37, 46, 55, 64, 73, 82, 91, 100].

The phase diagram of $L2_{\mathbf{Z}_N}(X_i)$ is shown in Figure M9, where $q = 3$, $N = 3^n$, $n = 13$, $X_0 = 1$, $\mu_N \in [0, 100]$. The phase diagram of $L2_{\mathbf{Z}_N}(X_i)$ after an adjustment is shown in Figure M10, where $q = 3$, $N = 3^n$, $n = 13$, $X_0 = 1$, μ_N is [$\mu_N \bmod 9 = 0$ or 3 or 6, $\mu_N \bmod 9 = 1$ or 4 or 7, $\mu_N \bmod 9 = 2$ or 8 or 5] which is [0, 9, 18, 27, 36, 45, 54, 63, 72, 81, 90, 99, 3, 12, 21, 30, 39, 48, 57, 66, 75, 84, 93, 6, 15, 24, 33, 42, 51, 60, 69, 78, 87, 96, 1, 10, 19, 28, 37, 46, 55, 64, 73, 82, 91, 100, 4, 13, 22, 31, 40, 49, 58, 67, 76, 85, 94, 7, 16, 25, 34, 43, 52, 61, 70, 79, 88, 97, 2, 11, 20, 29, 38, 47, 56, 65, 74, 83, 92, 8, 17, 26, 35, 44, 53, 62, 71, 80, 89, 98, 5, 14, 23, 32, 41, 50, 59, 68, 77, 86, 95].

A Logistic map in a finite field has a controllable length of the generated sequence.

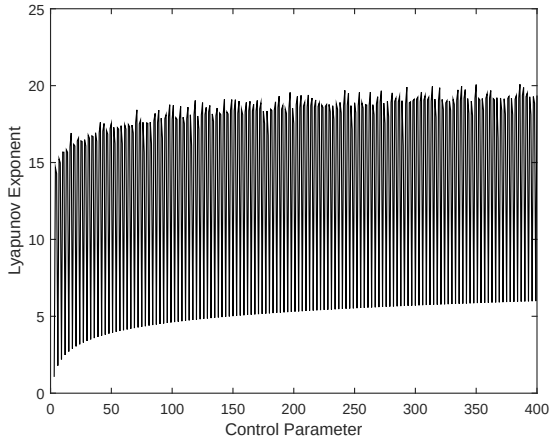

Figure M11 Lyapunov exponent of $L1_{\mathbf{Z}_N}(X_i)$.

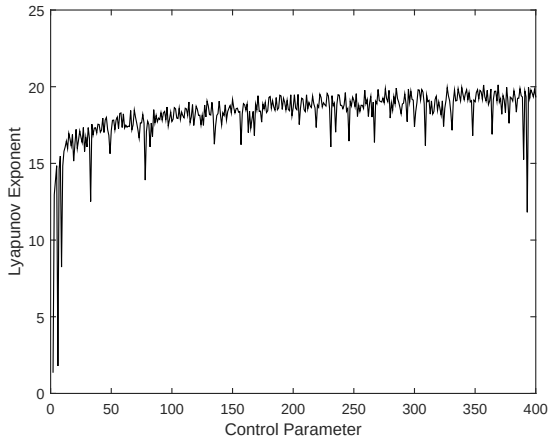

Figure M12 Lyapunov exponent of $L2_{\mathbf{Z}_N}(X_i)$.

Appendix M.5 Lyapunov exponent

The Lyapunov exponent plays a very significant role in studying the characteristics of bifurcation and the chaos motion of the dynamics. We designed programs for calculating the Lyapunov exponents of a Logistic map over a finite field.

The maximum Lyapunov exponent of $L1_{\mathbf{Z}_N}(X_i)$ is shown in Figure M11, where $q = 3$, $N = 3^n$, $n = 13$, $X_0 = 1$, $\mu_N \in [\,0, 400\,]$, and the Jacobian matrix is $[\,(2\mu_N X_i + \mu_N) \bmod N\,]$.

The maximum Lyapunov exponent of $L2_{\mathbf{Z}_N}(X_i)$ is shown in Figure M12, where $q = 3$, $N = 3^n$, $n = 13$, $X_0 = 1$, $\mu_N \in [\,0, 400\,]$, and the Jacobian matrix is $[\,(2\mu_N X_i) \bmod N\,]$.

The positive Lyapunov exponents imply that these sequences are chaotic.