SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

February 2017, Vol. 60 022302:1–022302:15
doi: 10.1007/s11432-015-0756-1

Period analysis of the Logistic map for the finite field

Bo YANG & Xiaofeng LIAO*

College of Electronic and Information Engineering, Southwest University, Chongqing 400715*, China*

Received January 18, 2016; accepted March 19, 2016; published online November 9, 2016

Abstract Usually, the security of traditional cryptography which works on integer numbers and chaotic cryptosystem which works on real numbers is worthy of study. But the classical chaotic map over the real domain has a disadvantage that the calculation accuracy of the floating point number can be doubled when the map is implemented by computer. This is a serious drawback for practical application. The Logistic map is a classical chaotic system and it has been used as a chaotic cipher in the real number field. This inevitably leads to the degradation of finite precision under computer environment, and it is also very difficult to guarantee security. To solve these drawbacks, we extend the Logistic map to the finite field. In this paper, we consider the Logistic map for the finite field $N = 3^n$, and analyze the period property of sequences generated by the Logistic map over $\boldsymbol{Z}_N$. Moreover, we discuss the control parameters which may influence the behavior of the mapping, and show that the Logistic map over $\boldsymbol{Z}_N$ may be suitable for application by performance analysis. Ultimately, we find that there exists an automorphic map between two Logistic maps with the different control parameters, which makes them suitable for sequence generator in cryptosystem. The automorphic sequence generated algorithm based on the Logistic map over $\boldsymbol{Z}_N$ is designed and analyzed in detail. These sequences can be used in the pseudorandom number generator, the chaotic stream cipher, and the chaotic block cipher, etc.

Keywords chaos, Logistic map, period analysis, sequence generated algorithm, Galois ring

Citation Yang B, Liao X F. Period analysis of the Logistic map for the finite field. Sci China Inf Sci, 2017, 60(2): 022302, doi: 10.1007/s11432-015-0756-1

1 Introduction

In the practical world, the nonlinear phenomenon is far more extensive than the linear one. Chaos phenomenon is a kind of random-like behavior which appears in the deterministic system. It is a complex motion form that is common in nature. Chaos is an interesting phenomenon which has been observed in various fields such as weather and climate, dynamics of satellites, population growth, electrical circuits, lasers, chemical reactions, fluid dynamics, mechanical systems, and so on. In 1954, Kolmogorov [1] explored the origin of probability and proposed the KAM theorem. In 1963, American meteorologist Lorenz [2] published the first numerical observations on a simplified model of thermal convection, called the Lorenz equation . He discovered that in this completely deterministic system of three ordinary differential equations, all non-periodic solutions were bounded but unstable. In 1964, Henon [3] used the

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

KAM theory as the backgrounds, and proposed a two-dimensional mapping with a strange attractor, and named it as Henon attractor. In 1975, Li and York proposed that period 3 implies chaos, which was considered as the first formal indication of chaos, and it was used from then on. In 1976, May [4] paid attention to the very complicated dynamics including period-doubling and chaos in some very simple population models, and described firstly the chaotic behavior of the Logistic mapping. Then, Feigenbaum [5] discovered that the values of the parameter of the period-doubling bifurcation were convergent in the geometric series, thus called the Feigenbaum constant. The work of Feigenbaum triggered an upsurge of chaos research interest among scientists. In 1980s and 1990s, researchers focused on how the system caused the new chaos and the characteristics of chaos, and entered into the application stage of chaos theory [6, 7]. Chaos theory has also found numerous applications in electrical and communication engineering, information and communication technologies [8], biology and medicine, and so on. At first, chaos is difficult to tame, but more recently, researchers have found the means to explain chaos phenomenon, control chaotic dynamic systems and make use of chaotic properties. Since chaotic systems have many important and good features such as mixing, being sensitive to initial conditions and random-like, continuous broadband power spectrum, and so on, they have been applied to information security and called as Chaotic Cryptography [9]. However, in practical application, the state space of a chaotic system may be discrete because of the limited computation, memory and communication capabilities [10]. How to select the chaotic map which satisfies the requirements of the cryptographic properties is a key problem to be solved. Kocarev [11] proposed some guiding methods that the selected chaotic map must at least satisfy with mixing property, robust and large parameter set.

In recent years, there are considerable attempts to study the dynamical behaviors of chaotic systems or maps [12–18]. There are many discrete chaotic maps such as Logistic map [4], Henon map [3], Arnold map [19], and so on. A traditional Logistic map over the real domain is given as $L_{\mathrm{R}}(x) = \mu x(1-x)$, and μ is a control parameter. It is well known that for $\mu = 4$, the Logistic map is chaotic. Recently, the Logistic map is commonly used as block cipher and sequence cipher. The concept of chaotic sequence cipher was first proposed by British mathematician Matthews who had studied the problem of Logistic chaotic map as a sequence key stream generator [6]. At present, there have been a large number of reports on how to design cipher by using chaotic properties and Logistic map, and most of them are in the light of block cipher algorithms [20–23], and there are also some for sequence cipher algorithms [24–27].

The traditional chaotic map over the real domain has a disadvantage that the calculation accuracy of the floating point number can be doubled when the map is implemented by computer. This is a serious drawback for practical application. To solve this problem, there are some researchers who consider encryption algorithm using chaotic system over the finite field [18,28–30]. Pseudorandom number plays a very important role in cryptography. Pseudorandom number generator has been studied for the design of applications such as cipher. There are many methods to generate a pseudorandom number, for example, a finite state machine [4]. It is well-known that the long period of password in a limited number domain can guarantee the security of the cryptosystem so that it is not easy to be attacked. Many studies have demonstrated that the Logistic map can provide long periodic sequences. The Logistic map over integers is based on a rounding, and the Logistic map over prime field is based on a remainder. In addition, the values of variant maps are integers. However, there exist some drawbacks in conventional methods, such as finite precision, low complexity, low randomness, and so on. In [31], to solve these drawbacks, the authors considered some properties of the maximum period on the Logistic map over the finite field $\boldsymbol{Z}_{2^n}$, and conjectured that the control parameters would influence the behavior of the mapping, but they did not give any theoretical proof. It is well-known that the analysis for the Logistic map over $\boldsymbol{Z}_{3^n}$ is more complicated than that for the Logistic map over $\boldsymbol{Z}_{2^n}$ because the value of the Logistic map over $\boldsymbol{Z}_{3^n}$ has more complexes than the Logistic map over $\boldsymbol{Z}_{2^n}$. For example, the control parameter $\mu \bmod 2 = 0$ or 1, $\mu \bmod 3 = 0$ or 1 or 2, which may influence the value of Logistic map when it mod 2^nor 3^n. We will discuss the Logistic map over the finite field $\boldsymbol{Z}_{3^n}$. We can expand the mapping range of this map from 0 to $3^n - 1$ by performing this expansion. Furthermore, some statistical properties of the period for this map are studied with arithmetic theory handling with dynatomic polynomial in detail. Moreover, we discuss the control parameters which will influence the behavior of the mapping over the finite field.

The maximum period of the generated sequence could be greatly changed by the control parameters. At the same time, some numerical examples are provided to verify the correctness and effectiveness of our analysis. Therefore, we have effectively overcome the above-mentioned drawbacks by using the Logistic map over $\boldsymbol{Z}_{3^n}$. In [32], the authors have proven there exists an automorphism between two maps with different control values for the Logistic map over prime field. Furthermore, we will prove that there also exists an automorphism map between two Logistic maps with the different control parameters over the finite field $\boldsymbol{Z}_{3^n}$, and finally an automorphic sequence generated algorithm based on the Logistic map over $\boldsymbol{Z}_{3^n}$ is designed.

The remaining part of this paper is organized as follows. In Section 2, we will give some preliminaries which are essential in understanding our analysis. Details of the period analysis of sequences generated by Logistic map over $\boldsymbol{Z}_{3^n}$ will be presented in Section 3. In Section 4, we will design an automorphic sequence generated algorithm of the Logistic map over $\boldsymbol{Z}_{3^n}$. Based on the period property, we will give, in Section 5, some performance analysis based on Logistic map over $\boldsymbol{Z}_{3^n}$. Finally, conclusion will be drawn in Section 6, with suggestions of the future work.

2 Preliminaries

In this section, we first review the typical Logistic map over the real domain and integers, and describe the Logistic map over the finite field $\boldsymbol{Z}_{3^n}$. Then, we will present some arithmetic methods, handling with the dynatomic polynomial over finite field, which play a key role in analyzing the period for polynomials. These methods are also useful in the analysis of chaotic cipher.

2.1 Logistic maps and their variants

A typical Logistic map over the real domain is given as

$$L_{\mathrm{R}}(x) = \mu x(1-x), \tag{1}$$

where x is a real number in the interval $0 \leqslant x \leqslant 1$, and μ is a control parameter in the interval $0 < \mu \leqslant 4$ [4]. It is well known that for $\mu = 4$, the Logistic map is chaotic. Let x_i be an input, where i acts as the discrete time. The iterative mapping for Eq. (1) can be written by

$$x_{i+1} = L_{\mathrm{R}}(x_i) = \mu x_i(1-x_i). \tag{2}$$

The above Logistic map in the real number field has a drawback that the calculation accuracy of the floating point number can be doubled under computer environment for implementing. This is a serious drawback for practical application. To solve this problem, in [33], the authors derived the Logistic map over integers from Eq. (1) as

$$L_{\mathrm{R}}^{(n)}(x') = \mu x'(2^n - x')/2^n, \tag{3}$$

where n is the precision for elements of the Logistic map, and $x' = 2^n x$ and $L_{\mathrm{R}}^{(n)}(x') = 2^n L_{\mathrm{R}}(x)$.

We can define a function of Eq. (3) over integers as

$$L_{\mathrm{Int}}^{(n)}(X) = \lfloor \mu X(2^n - X)/2^n \rfloor, \tag{4}$$

where X is the integer part of x' in the interval $0 \leqslant X \leqslant 2^n$, and $\lfloor \cdot \rfloor$ is the floor function. $L_{\mathrm{Int}}^{(n)}(X)$ can directly specify the calculation accuracy and its calculation accuracy does not depend on the implementation. Accordingly, it is practicable because of the integer of mapped values.

In [34], the authors defined the Logistic map over prime field as follows:

$$L_{\boldsymbol{Z}_p}(X) = \frac{\mu_p X(p-1-X)}{p-1} \pmod p, \tag{5}$$

where p is an odd prime, $\boldsymbol{Z}_p$ is a prime field modulo p, X is an element in $\boldsymbol{Z}_p$ in the interval $0 \leqslant X \leqslant p-1$, and μ_p is a control parameter such that $1 \leqslant \mu_p \leqslant p-1$.

With a similar method, the iterative mapping for Eq. (5) can be rewritten as follows:

$$X_{i+1} = L_{\boldsymbol{Z}_p}(X_i) = \frac{\mu_p X_i(p-1-X_i)}{p-1} \pmod{p}, \tag{6}$$

$L_{\boldsymbol{Z}_p}(X_i)$ may generate a long periodic sequence which has good randomness.

In [31], the authors considered some properties of the maximum period on the Logistic map over $\boldsymbol{Z}_{2^n}$, and conjectured that the control parameters may influence the behavior of the mapping, but they did not give any theoretical proof. The analysis of the maximum period on the Logistic map over $\boldsymbol{Z}_{3^n}$ is more complicated than $\boldsymbol{Z}_{2^n}$. We will discuss the period properties of Logistic map for general composite N. Finally, numerical examples are provided to verify the correctness and effectiveness of our analysis.

Definition 1. Let N be a modulo with $N = 3^n$, where n is an arbitrary natural number, and we define the Logistic map over the finite field $\boldsymbol{Z}_{3^n}$ as follows:

$$X_{i+1} = L_{\boldsymbol{Z}_N}(X_i) = \frac{\mu_N X_i(N-1-X_i)}{N-1} \pmod{N}, \tag{7}$$

where μ_N is a control parameter in the interval $1 \leqslant \mu_N \leqslant N-1$, and $X_i \in [0, N-1]$ for all $i = 1, 2, 3 \ldots$.

By the above Definition 1, we have the following result.

Lemma 1.

$$X_{i+1} = L_{\boldsymbol{Z}_N}(X_i) = \mu_N X_i(X_i+1) \pmod{N}. \tag{8}$$

Proof. Because $N-1 \equiv -1 (\mathrm{mod}\ N)$, with Eq. (7),

$$X_{i+1} = \frac{\mu_N X_i(N-1-X_i)}{N-1} \pmod{N} \equiv \frac{\mu_N X_i(-1-X_i)}{-1} \pmod{N} \equiv \mu_N X_i(X_i+1) \pmod{N}.$$

By Lemma 1, the calculation X_i with Eq. (8) is more efficiently than with Eq. (7).

2.2 Arithmetic theory handling with dynatomic polynomial

A rational map ϕ is given by a pair of homogeneous polynomials

$$\phi = [A(X,Y), B(X,Y)] = A(X,Y)/B(X,Y),$$

where $A(X,Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_{n-1}XY^{n-1} + a_nY^n$ and $B(X,Y) = b_0X^m + b_1X^{m-1}Y + \cdots + b_{m-1}XY^{m-1} + b_mY^m$ are homogeneous polynomials of degrees n and m with coefficients in a number field K respectively. The rational map ϕ has no nontrivial common roots. However, they may obtain some common roots in the residue field if we reduce the coefficients of A and B with a modulo. This phenomenon helps understand that it is useful to have a tool called the resultant which characterizes the existence of common roots in terms of the coefficients of A and B. The resultant of A and B is a polynomial $\mathrm{Res}(a_0, \ldots, a_n, b_0, \ldots, b_m) \in \boldsymbol{Z}[a_0, \ldots, a_n, b_0, \ldots, b_m]$. If $a_0b_0 \neq 0$ and we define the factors A and B as

$$A = a_0 \prod_{i=1}^{n} (X - \alpha_i Y),$$

and

$$B = b_0 \prod_{j=1}^{m} (X - \beta_j Y),$$

respectively, then the resultant of A and B is

$$\mathrm{Res}(A,B) = a_0^m b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j).$$

Therefore, A and B have a common zero, if and only if $\mathrm{Res}(A,B) = 0$. The resultant is equal to the $(m+n) \times (m+n)$ determinant,

$$\mathrm{Res}(A,B)=\det\begin{vmatrix} a_0a_1a_2\cdots a_n & & & & \\ & a_0a_1a_2\cdots a_n & & & \\ & & a_0a_1a_2\cdots a_n & & \\ & & & \cdots\cdot & \\ & & & & a_0a_1a_2\cdots a_n \\ b_0b_1b_2\cdots b_m & & & & \\ & b_0b_1a_2\cdots b_m & & & \\ & & b_0a_1b_2\cdots b_m & & \\ & & & \cdots\cdot & \\ & & & & b_0a_1b_2\cdots b_m \end{vmatrix}.$$

In particular, $\mathrm{Res}(A,B)$ is homogeneous of degree m in the variables $a_0,\ldots,a_n$ and simultaneously homogeneous of degree n in the variables $b_0,\ldots,b_m$ [35].

Let $\phi(z)\in K(z)$ be a rational polynomial of degree d. Then the fixed points of ϕ are the roots of $\phi(z)-z$, and more generally, the points of period n for ϕ are the roots of $\phi^n(z)-z$ and the point z is periodic for some $n\geqslant 1$, where $\phi^n=\phi\circ\phi\circ\cdots\circ\phi$ is the n-th iterate of ϕ and $\circ$ is composite function, for example $f\circ g=f(g(\cdot))$.

Definition 2. The point z is periodic point if $\phi^n(z)=z$ for some $n\geqslant 1$, such that the smallest n is called the exact period of z. The point z is preperiodic point if some iteration $\phi^m(z)$ is periodic. The sets of periodic and preperiodic points of ϕ are denoted respectively by $\mathrm{Per}(\phi)=\{\phi^n(z)=z \text{ for some } n\geqslant 1\}$ and $\mathrm{PrePer}(\phi)=\{\phi^{m+n}(z)=\phi^m(z) \text{ for some } n\geqslant 1, m\geqslant 0\}$.

It is natural to focus on the points of exact period n. We may define the n-th dynatomic polynomial by the formula

$$\Phi_n(z)=\prod(\phi^n(z)-z)^{u(\eta)},$$

where u is the Mobius function [36] defined by $u(1)=1$ and $p_1\cdots p_r$ are prime numbers,

$$u(p_1^{e_1}\cdots p_r^{e_r})=\begin{cases}(-1)^r, & \text{if } e_1=\cdots=e_r=1,\\ 0, & \text{if any } e_i\geqslant 2.\end{cases}$$

The roots of the polynomial $YA(X,Y)-XB(X,Y)$ are precisely the fixed points of ϕ. If we count each fixed point according to the multiplicity of the root, then ϕ has exactly $d+1$ fixed points. We can apply the same reasoning to an iteration ϕ^n of ϕ and assign multiplicities to the n-periodic points.

Definition 3. Let $\phi(z)\in K(z)$ be a rational function of degree d, and for any $n\geqslant 0$, write

$$\phi^n=[A_n(X,Y),B_n(X,Y)]=A_n(X,Y)/B_n(X,Y),$$

with homogeneous polynomials $A_n,B_n\in K$ of degree d^n. The n-period polynomial of ϕ is the polynomial

$$\Phi_{\phi,n}(X,Y)=YA_n(X,Y)-XB_n(X,Y).$$

Notice that $\Phi_{\phi,n}(P)=0$ if and only if $\phi^n(P)=P$, which justifies the name assigned to the polynomial $\Phi_{\phi,n}$. The polynomial $\Phi_{\phi,n}$ is homogeneous of degree d^n+1, so counted with multiplicity, the map ϕ has exactly d^n+1 points of period n.

The n-th dynatomic polynomial of ϕ is the polynomial

$$\Phi^*_{\phi,n}(X,Y)=\prod(YA_k(X,Y)-XB_k(X,Y))^{u(\eta)}=\prod(\Phi_{\phi,k}(X,Y))^{u(\eta)}.$$

If ϕ is fixed, we write Φ_n and Φ^*_n. If $\phi(z)\in K(z)$ is a polynomial, then we generally dehomogenize $[X,Y]=\frac{X}{Y}=[z,1]=z$ and write $\Phi_n(z)$ and $\Phi^*_n(z)$.

The roots of the period polynomials $\Phi_n(z)=\phi_c^n(z)-z$ and associated dynatomic polynomial $\Phi^*_n(z)$ are the periodic points of the map $\phi_c(z)=z^2+c$. In order to investigate how the periodic points of

$\phi_c(z)$ vary as a function of c, we observe that $\Phi_n^*(z)$ is a polynomial in the two variables z and c. Thus in studying quadratic polynomial maps, it is natural to write $\Phi_n^*(c,z)$ and treat Φ_n^* as a polynomial in $\boldsymbol{Z}[c,z]$. The first few period and dynatomic polynomials for $\phi(z)=z^2+c$ are listed as follows [35]:

$$\Phi_1(c,z)=\phi^1(z)-z=z^2-z+c,$$

$$\Phi_2(c,z)=\phi^2(z)-z=z^4+2cz^2-z+(c^2+c),$$

$$\Phi_3(c,z)=\phi^3(z)-z=z^8+4cz^6+(6c^2+2c)z^4+(4c^3+4c^2)z^2-z+(c^4+2c^3+c^2+c),$$

$$\Phi_1^*(c,z)=\phi^1(z)-z=z^2-z+c,$$

$$\Phi_2^*(c,z)=\frac{\phi^2(z)-z}{\phi^1(z)-z}=z^2+z+(c+1),$$

$$\Phi_3^*(c,z)=\frac{\phi^3(z)-z}{\phi^1(z)-z}=z^6+z^5+(3c+1)z^4+(2c+1)z^3+(3c^2+3c+1)z^2+(c^2+2c+1)z+(c^3+2c^2+c+1).$$

This occurs if and only if $\Phi_m^*(z)$ and $\Phi_n^*(z)$ have a common root, i.e., if and only if c is a root of the resultant equation $\mathrm{Res}(\Phi_m^*(z),\Phi_n^*(z))=0$.

Note that this is a polynomial equation for the parameter c. So we list the first few examples as follows:

$$\mathrm{Res}(\Phi_2^*,\Phi_1^*)=4c+3,\quad \mathrm{Res}(\Phi_3^*,\Phi_1^*)=-16c^2-4c-7.$$

Example 1. The polynomial $\phi(z)=z^2+c$, $c=-\frac{3}{4}$, $\mathrm{Res}(\Phi_2^*,\Phi_1^*)=4c+3=0$, so $\phi(z)=z^2-\frac{3}{4}$ is the only example with a fixed point of period as type (m,n) that is $(2,1)$.

Thus, given a polynomial $\phi(z)\in K[z]$ of degree 2 and a point P of exact period n, we make a change to a formula $\phi(z)=Az^2+Bz+C$ to $\phi^f(z)=z^2+c$. Note that this entire procedure takes place within the field K. Thus the solutions to the equation $\Phi_n^*(y,z)=0$ parameterize pairs (ϕ,P), where ϕ is a conjugate class of quadratic polynomials and P is a point of formal period n for ϕ. Further, the solution is K-rational if and only if ϕ and P are K-rational.

Definition 4. Let ϕ be a map from a metric space to itself. The Fatou set of ϕ is the maximal open set on which ϕ is equicontinuous. The Julia set is the complement of the Fatou set [37].

Definition 5. Let $\phi_c(z)=z^2+c$. If 0 is strictly preperiodic, and $\phi_c^{n+m}(0)=\phi_c^m(0)$, then c is called a Misiurewicz point [38].

3 Period analysis of sequences generated by Logistic map

In this section, we characterize our analysis for the period property of sequences generated by Logistic map when X_i traverses all elements in the finite field $\boldsymbol{Z}_{3^n}$, and prove the following theorems using the arithmetic methods handling with the dynatomic polynomial. The background of arithmetic theory and number theory involved in the analysis can be found in the relevant textbooks such as [35].

Theorem 1. When $\mu_N \bmod 9=0$ or 3 or 6, the maximum period of $L_{\boldsymbol{Z}_N}(X_i)$ is 1 and the final value of $L_{\boldsymbol{Z}_N}(X_i)$ is 0.

Proof. We define $\mu_N=3^k m$, where k is a positive integer, and m is also a positive integer. With Eq. (8), for any $X_0\in Z_{3^n}$, $X_1=L_{\boldsymbol{Z}_N}(X_0)\equiv 3^k mX_0(X_0+1)\pmod N$. Therefore, X_1 is the multiple of 3^k, and X_1 can write $X_1=3^k l$, where l is a natural number. Then, we calculate $X_2=L_{\boldsymbol{Z}_N}(X_1)\equiv 3^k mX_1(X_1+1)(\mathrm{mod}\ N)\equiv 3^k m(3^k l)(3^k l+1)(\mathrm{mod}\ N)\equiv 3^{2k}ml(3^k l+1)(\mathrm{mod}\ N)\equiv 3^{2k}l'(\mathrm{mod}\ N)$. Therefore, $L_{\boldsymbol{Z}_N}(X_1)$ is the multiple of 3^{2k}. Using the same method, we can also calculate $X_3=L_{\boldsymbol{Z}_N}(X_2)\equiv 3^{3k}ml'(3^{2k}l'+1)(\mathrm{mod}\ N)\equiv 3^{3k}l''(\mathrm{mod}\ N)$. When the Logistic mapping Eq. (8) is repeated i times, $X_{i+1}=L_{\boldsymbol{Z}_N}(X_i)$ is the multiple of $3^{(i+1)k}$. Therefore, if $(i+1)k\geqslant n$, $3^{(i+1)k}=3^n\cdot 3^{(i+1)k-n}\equiv 0\pmod N$. We can derive the conclusion that the mapped final value converges to 0. Since 0 is mapped into itself, the period of $L_{\boldsymbol{Z}_N}(X_i)$ is 1 if $\mu_N \bmod 9=0$ or 3 or 6.

Example 2. (1) When $\mu_N=3, X_0=1, n=5$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1,6,126,135,162,0,\ldots)$.

(2) When $\mu_N=6, X_0=1, n=5$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1,12,207,27,162,0,\ldots)$.

(3) When $\mu_N = 6, X_0 = 1, n = 7$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 12, 936, 270, 1620, 972, 1458, 0, \ldots)$.
(4) When $\mu_N = 6, X_0 = 11, n = 7$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(11, 792, 135, 810, 486, 729, 0, \ldots)$.
(5) When $\mu_N = 9, X_0 = 11, n = 7$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(11, 1188, 1944, 0, \ldots)$.
(6) When $\mu_N = 27, X_0 = 1, n = 7$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 54, 1458, 0, \ldots)$.
(7) When $\mu_N = 39, X_0 = 1, n = 7$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 78, 1935, 2079, 162, 1944, 1458, 0, \ldots)$.
(8) When $\mu_N = 51, X_0 = 1, n = 7$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 102, 2178, 1485, 1377, 243, 1458, 0, \ldots)$.

In the following, we will discuss the mapped values and the period properties of $L_{\boldsymbol{Z}_N}(X_i)$ in other circumstances when $\mu_N \bmod 9 \neq 0$ and 3 and 6, and $\mu_N \bmod 9 = 1$ or 2 or 4 or 5 or 7 or 8.

Theorem 2. The field K does not have characteristic 2, then any quadratic polynomial

$$\phi(z) = Az^2 + Bz + C \tag{9}$$

can be changed into $z^2 + c$ by a simple transformation of variables working entirely within the field K.

Proof. We let $f(z) = \frac{2z-B}{2A}$, and $f^{-1}(z) = \frac{2Az+B}{2}$, then

$$\phi^f(z) = (f^{-1} \circ \phi \circ f)(z) = z^2 + \left(AC - \frac{1}{4}B^2 + \frac{1}{2}B\right); \tag{10}$$

let $c = AC - \frac{1}{4}B^2 + \frac{1}{2}B$, then Eq. (9) can be put into the form $\phi^f(z) = z^2 + c$.

If z_0 is an n periodic point of ϕ, then $f(z_0)$ just is a n periodic point of $\phi^f(z)$.

Lemma 2. Because of the above Theorem 2, Eq. (8) can be transformed into $L^f(X_i) = X_i^2 + c$.

Proof. With Eq. (8) and Theorem 2,

$$L_{\boldsymbol{Z}_N}(X_i) = \mu_N X_i(X_i + 1) = \mu_N X_i^2 + \mu_N X_i.$$

Let $A = \mu_N$, $B = \mu_N$, $C = 0$, then $f(z) = \frac{1}{\mu_N}z - \frac{1}{2}$, and $f^{-1}(z) = \mu_N z + \frac{1}{2}\mu_N$,

$$L^f(X_i) = L^f_{\boldsymbol{Z}_N}(X_i) = (f^{-1} \circ L_{Z_N} \circ f)(X_i) = X_i^2 + \frac{1}{4}(2\mu_N - \mu_N^2).$$

Let $c = \frac{1}{4}(2\mu_N - \mu_N^2)$,

$$L^f(X_i) = X_i^2 + c. \tag{11}$$

Therefore, the periodic property of $L_{\boldsymbol{Z}_N}(X_i)$ is the same as that of $L^f(X_i)$.

Theorem 3. When $\mu_N \bmod 9 = 2$ or 5 or 8, the maximum period of $L_{\boldsymbol{Z}_N}(X_i)$ is 1 and the final value of $L_{\boldsymbol{Z}_N}(X_i)$ is a constant C.

Proof. By using Lemma 2 and Eq. (11), for any $X_i \in \boldsymbol{Z}_N$, we let $c = \frac{1}{4}(2\mu_N - \mu_N^2) = \frac{1}{4} - \frac{1}{4}(\mu_N - 1)^2$, then

$$\mu_N \equiv 2 \bmod 9,\ \mu_N - 2 \equiv 0 \bmod 9,\ (\mu_N - 1)^2 = (\mu_N - 2 + 1)^2 = (\mu_N - 2)^2 + 2(\mu_N - 2) + 1 \equiv 1 \bmod 9,$$

$$\mu_N \equiv 5 \bmod 9,\ \mu_N - 5 \equiv 0 \bmod 9,\ (\mu_N - 1)^2 = (\mu_N - 5 + 4)^2 = (\mu_N - 5)^2 + 8(\mu_N - 5) + 16 \equiv 7 \bmod 9,$$

$$\mu_N \equiv 8 \bmod 9,\ \mu_N - 8 \equiv 0 \bmod 9,\ (\mu_N - 1)^2 = (\mu_N - 8 + 7)^2 = (\mu_N - 8)^2 + 14(\mu_N - 8) + 49 \equiv 4 \bmod 9,$$

while

$$\mu_N \equiv 0 \bmod 9,\ (\mu_N - 1)^2 = \mu_N^2 + 2\mu_N + 1 \equiv 1 \bmod 9,$$

$$\mu_N \equiv 3 \bmod 9,\ \mu_N - 3 \equiv 0 \bmod 9,\ (\mu_N - 1)^2 = (\mu_N - 3 + 2)^2 = (\mu_N - 3)^2 + 4(\mu_N - 3) + 4 \equiv 4 \bmod 9,$$

$$\mu_N \equiv 6 \bmod 9,\ \mu_N - 6 \equiv 0 \bmod 9,\ (\mu_N - 1)^2 = (\mu_N - 6 + 5)^2 = (\mu_N - 6)^2 + 10(\mu_N - 6) + 25 \equiv 7 \bmod 9.$$

Therefore, we have $c_{\mu \equiv 2 \bmod 9} = c_{\mu \equiv 0 \bmod 9}$, and $c_{\mu \equiv 5 \bmod 9} = c_{\mu \equiv 6 \bmod 9}$, and $c_{\mu \equiv 8 \bmod 9} = c_{\mu \equiv 3 \bmod 9}$. So we can draw the following conclusion that,

1. The period of $L_{\boldsymbol{Z}_N}(X_i)$ when $\mu_N \bmod 9 = 2$ is the same as the period of $L_{\boldsymbol{Z}_N}(X_i)$ when $\mu_N \bmod 9 = 0$.
2. The period of $L_{\boldsymbol{Z}_N}(X_i)$ when $\mu_N \bmod 9 = 5$ is the same as the period of $L_{\boldsymbol{Z}_N}(X_i)$ when $\mu_N \bmod 9 = 6$.
3. The period of $L_{\boldsymbol{Z}_N}(X_i)$ when $\mu_N \bmod 9 = 8$ is the same as the period of $L_{\boldsymbol{Z}_N}(X_i)$ when $\mu_N \bmod 9 = 3$.
4. When $\mu_N \bmod 9 = 2$ or 5 or 8, the period of $L_{\boldsymbol{Z}_N}(X_i)$ is 1 and its final value is a constant C.

Example 3. (1) When $\mu_N = 2$, $X_0 = 1$, $n = 5$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 4, 40, 121, 121, \ldots)$.
(2) When $\mu_N = 5, X_0 = 1, n = 5$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 10, 64, 145, 145, \ldots)$.
(3) When $\mu_N = 8$, $X_0 = 1$, $n = 5$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 16, 232, 151, 151, \ldots)$.
(4) When $\mu_N = 8$, $X_0 = 1$, $n = 7$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 16, 2176, 880, 2095, 1366, 1366, \ldots)$.
(5) When $\mu_N = 29$, $X_0 = 1$, $n = 7$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 58, 823, 904, 904, \ldots)$.
(6) When $\mu_N = 41$, $X_0 = 1$, $n = 7$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 82, 1297, 2026, 2026, \ldots)$.
(7) When $\mu_N = 71$, $X_0 = 1$, $n = 7$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 142, 493, 1060, 1303, 2032, 2032, \ldots)$.

Lemma 3.

$$L_{\boldsymbol{Z}_N}(X_i) = L_{\boldsymbol{Z}_N}(N - 1 - X_i).$$

Proof. By using Eq. (8), we have $L_{\boldsymbol{Z}_N}(N-1-X_i) \equiv \mu_N(N-1-X_i)((N-1-X_i)+1) (\mathrm{mod}\ N) \equiv \mu_N(N-1-X_i)(N-X_i) (\mathrm{mod}\ N) \equiv \mu_N(N^2 - N\cdot X_i - N + X_i - N\cdot X_i + X_i^2) (\mathrm{mod}\ N) \equiv \mu_N(X_i + X_i^2) (\mathrm{mod}\ N) \equiv \mu_N X_i(X_i+1) (\mathrm{mod}\ N) = L_{\boldsymbol{Z}_N}(X_i)$.

Theorem 4. When $\mu_N \bmod 9 = 4$, the maximum period of $L_{\boldsymbol{Z}_N}(X_i)$ is $\frac{N}{27} = 3^{n-3}$.

Proof. For simplicity, firstly we discuss $\mu_N = 4$, then $c = \frac{1}{4}(2\mu_N - \mu_N^2) = -2$. Letting $\phi_c(z) = \phi^f(z) = z^2 + c$, if $c = -2$, $\phi_c(z) = z^2 - 2$. We write $z = e^{it} + e^{-it} = 2\cos(t)$, then

$$\phi(z) \ = (2\cos(t))^2 - 2 = 2(2\cos^2(t) - 1) = 2\cos(2t),$$

$$\phi^2(z) = (2\cos(2t))^2 - 2 = 2(2\cos^2(2t) - 1) = 2\cos(4t) = 2\cos(2^2 t),$$

$$\phi^3(z) = (2\cos(2^2 t))^2 - 2 = 2(2\cos^2(2^2 t) - 1) = 2\cos(2^{2+1} t) = 2\cos(2^3 t),$$

so that $\phi^n(z) = 2\cos(2^n t)$. Because $2\cos(\cdot) \in [-2, 2]$, the Julia set of ϕ is the closed interval on the real axis between -2 and 2, and $\mathrm{J}(\phi)$ is equal to the closure of $\mathrm{Per}(\phi)$. If $\phi^n(z_0) = z_0$, z_0 is a fixed point of ϕ^n. In particular, z_0 is a point of period n for ϕ. Then $\phi^n(z_0) = 2\cos(2^n t) = z_0 = 2\cos(t)$, and $\cos(2^n t) - \cos(t) = 0$. So $t = 2k\pi \pm \frac{\pi}{2}$, $z_0 = 0$, $\phi(z_0) = -2, \phi^2(z_0) = 2, \phi^3(z_0) = 2, \phi^3(z_0) = 2, \ldots, \phi^n(z_0) = 2$.

Definition 6. A point c is called a Misiurewicz point if 0 is strictly preperiodic for $\phi_c(z) = z^2 + c$. We say that c is a Misiurewicz point as a fixed point of period as type (m, n) if $m \geqslant 1$ is the smallest integer such that $\phi_c^m(0)$ is periodic, and if n is the primitive period of $\phi_c^m(0)$.

Thus for $c = -2$, we have $0 \to -2 \to 2 \to 2 \to \cdots$, so $\phi_c(z)$ has period as type $(2, 1)$. So the periodic properties of $L_{\boldsymbol{Z}_N}(X_i)$ when $\mu_N = 4$ are the same of $\phi_c(z) = z^2 - 2$.

Example 4. (1) When $\mu_N = 4$, $X_0 = 1$, $n = 3$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are (1, 8, 18, 18, 18, 18, ...).
(2)When $\mu_N = 4$, $n > 3$, with Lemma 3 and $z_0 = 0$,

$$X_0 = f^{-1}(z_0) = \mu_N z_0 + \frac{1}{2}\mu_N = 2,$$

$$L^T_{\boldsymbol{Z}_N}(2) = L_{\boldsymbol{Z}_N}(N - 1 - 2),$$

$$L^T_{\boldsymbol{Z}_N}(2) = 4 \cdot (N - 1 - 2)(N - 1 - 2 + 1) \pmod N,$$

$$L^T_{\boldsymbol{Z}_N}(2) = 4 \cdot (N - 3)(N - 2) \pmod N,$$

$$L^T_{\boldsymbol{Z}_N}(2) = 4 \cdot (N^2 - 5 \cdot N + 6) \pmod N,$$

$$L^T_{\boldsymbol{Z}_N}(2) = 24 \pmod N,$$

$$T = \frac{N}{27} = 3^{n-3}.$$

Because $c = \frac{1}{4} - \frac{1}{4}(\mu_N - 1)^2$, and $\mu_N \equiv 4 \bmod 9$, $\mu_N - 4 \equiv 0 \bmod 9$, $(\mu_N - 1)^2 = (\mu_N - 4 + 3)^2 = (\mu_N - 4)^2 + 6(\mu_N - 4) + 9 \equiv 0 \bmod 9$, the period of $L_{\boldsymbol{Z}_N}(X_i)$ when $\mu_N \bmod 9 = 4$ is the same as that of $L_{\boldsymbol{Z}_N}(X_i)$ when $\mu_N = 4$, and the maximum period of $L_{\boldsymbol{Z}_N}(X_i)$ is $\frac{N}{27} = 3^{n-3}$.

Example 5. (1) When $\mu_N = 4$, $X_0 = 1$, $n = 4$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 8, 45, 18, 72, 45, 18, 72, 45, \ldots)$, and the period of $L_{\boldsymbol{Z}_N}(X_i)$ is 3.

(2) When $\mu_N = 4$, $X_0 = 1$, $n = 5$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 8, 45, 18, 153, 207, 180, 72, 126, 99, 234, 45, 18, 153, 207, 180, 72, 126, 99, 234, 45, \ldots)$, and the period of $L_{\boldsymbol{Z}_N}(X_i)$ is 9.

(3) When $\mu_N = 76$, $X_0 = 1$, $n = 5$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 152, 117, 225, 171, 198, 63, 9, 36, 144, 90, 117, 225, 171, 198, 63, 9, 36, 144, 90, 117, \ldots)$, and the period of $L_{\boldsymbol{Z}_N}(X_i)$ is 9.

(4) When $\mu_N = 211$, $X_0 = 1$, $n = 10$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 422, 50553, 52767, 41454, 48204, 50661, 27198, \ldots, 58005, 55602, 58626, 50553, \ldots)$, and the period of $L_{\boldsymbol{Z}_N}(X_i)$ is 2187.

Theorem 5. When $\mu_N \bmod 9 = 7$, the maximum period of $L_{\boldsymbol{Z}_N}(X_i)$ is $\frac{N}{27} = 3^{n-3}$.

Proof. When $\mu_N \equiv 7 \bmod 9, c = \frac{1}{4}(2\mu_N - \mu_N^2) = \frac{1}{4} - \frac{1}{4}(\mu_N - 1)^2, (\mu_N - 1)^2 = (\mu_N - 7 + 6)^2 = (\mu_N - 7)^2 + 12(\mu_N - 7) + 36 \equiv 0 \bmod 9$. Because of $c_{\mu_N \equiv 7 \bmod 9} = c_{\mu_N \equiv 4 \bmod 9}$, the period of $L_{\boldsymbol{Z}_N}(X_i)$ when $\mu_N \equiv 7 \bmod 9$ is the same as the period of $L_{\boldsymbol{Z}_N}(X_i)$ when $\mu_N \equiv 4 \bmod 9$. When $\mu_N \bmod 9 = 7$, the maximum period of $L_{\boldsymbol{Z}_N}(X_i)$ is 3^{n-3}.

Example 6. (1) When $\mu_N = 7$, $X_0 = 1$, $n = 3$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 14, 12, 12, 12, 12, \ldots)$, and the period of $L_{\boldsymbol{Z}_N}(X_i)$ is 1.

(2) When $\mu_N = 7$, $X_0 = 1$, $n = 4$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 14, 12, 39, 66, 12, 39, 66, 12, \ldots)$, and the period of $L_{\boldsymbol{Z}_N}(X_i)$ is 3.

(3) When $\mu_N = 7$, $X_0 = 1$, $n = 5$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 14, 12, 120, 66, 93, 201, 147, 174, 39, 228, 12, 120, 66, 93, 201, 147, 174, 39, 228, 12, \ldots)$, and the period of $L_{\boldsymbol{Z}_N}(X_i)$ is 9.

(4) When $\mu_N = 79$, $X_0 = 1$, $n = 5$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 158, 57, 192, 3, 219, 111, 165, 138, 30, 84, 57, 192, 3, 219, 111, 165, 138, 30, 84, 57, \ldots)$, and the period of $L_{\boldsymbol{Z}_N}(X_i)$ is 9.

(5) When $\mu_N = 214$, $X_0 = 1$, $n = 10$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 428, 25383, 16851, 13827, 42312, 40098, 12045, \ldots, 55839, 32241, 58620, 25383, \ldots)$, and the period of $L_{\boldsymbol{Z}_N}(X_i)$ is 2187.

Theorem 6. When $\mu_N \bmod 9 = 1$, the maximum period of $L_{\boldsymbol{Z}_N}(X_i)$ is $\frac{N}{9} = 3^{n-2}$.

Proof. For simplicity, firstly we discuss $\mu_N = 10$, then when $\mu_N = 10$, $n \geqslant 3$, by using Lemma 3 and $z_0 = 0$,

$$X_0 = f^{-1}(z_0) = \mu_N z_0 + \frac{1}{2}\mu_N = 5,$$

$$L^T_{\boldsymbol{Z}_N}(5) = L_{\boldsymbol{Z}_N}(N - 1 - 5),$$

$$L^T_{\boldsymbol{Z}_N}(5) = 10 \cdot (N - 1 - 5)(N - 1 - 5 + 1) \pmod N,$$

$$L^T_{\boldsymbol{Z}_N}(5) = 10 \cdot (N - 6)(N - 5) \pmod N,$$

$$L^T_{\boldsymbol{Z}_N}(5) = 10 \cdot (N^2 - 11 \cdot N + 30) \pmod N,$$

$$L^T_{\boldsymbol{Z}_N}(5) = 300 \pmod N,$$

$$T = \frac{N}{9} = 3^{n-2}.$$

Because $\mu_N \equiv 1 \bmod 9$, the period of $L_{\boldsymbol{Z}_N}(X_i)$ when $\mu_N \bmod 9 = 1$ is the same as that of $L_{\boldsymbol{Z}_N}(X_i)$ when $\mu_N = 10$, and the maximum period of $L_{\boldsymbol{Z}_N}(X_i)$ is $\frac{N}{9} = 3^{n-2}$.

Example 7. (1) When $\mu_N = 1$, $X_0 = 1$, $n = 3$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are $(1, 2, 6, 15, 24, 6, \ldots)$, and the period of $L_{\boldsymbol{Z}_N}(X_i)$ is 3.

(2) When $\mu_N = 1$, $X_0 = 1$, $n = 4$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are (1, 2, 6, 42, 24, 33, 69, 51, 60, 15, 78, 6, ...), and the period of $L_{\boldsymbol{Z}_N}(X_i)$ is 9.

(3) When $\mu_N = 1$, $X_0 = 1$, $n = 5$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are (1, 2, 6, 42, 105, 195, 69, 213, 141, 96, 78, 87, 123, 186, 33, 150, 51, 222, 177, 159, 168, 204, 24, 114, 231, 132, 60, 15, 240, 6, ...), and the period of $L_{\boldsymbol{Z}_N}(X_i)$ is 27.

(4) When $\mu_N = 73$, $X_0 = 1$, $n = 5$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are (1, 146, 105, 141, 204, 51, 168, 69, 240, 195, 177, 186, 222, 42, 132, 6, 150, 78, 33, 15, 24, 60, 123, 213, 87, 231, 159, 114, 96, 105, ...), and the period of $L_{\boldsymbol{Z}_N}(X_i)$ is 27.

(5) When $\mu_N = 208$, $X_0 = 1$, $n = 10$, the sequences of $L_{\boldsymbol{Z}_N}(X_i)$ are (1, 416, 3237, 43368, 6495, 32829, 19824, 50829, ..., 132, 49659, 58632, 3237, ...), and the period of $L_{\boldsymbol{Z}_N}(X_i)$ is 6561.

But there are some special cases, for example, when $\mu_N = 4$, $X_0 = 3$, the period of $L_{\boldsymbol{Z}_N}(X_i)$ is 3^{n-2}, and the initial value $X_0 = j \cdot 3^i$ or $j \cdot 3^i - 1$, where $i \geqslant 2$ and j is any integer. Since the period of $L_{\boldsymbol{Z}_N}(X_i)$ is very complex, we will discuss them in the future.

4 Automorphic sequences generated algorithm based on Logistic map

In this section, we will find that there exists an automorphic map between two mappings which are $L_{\boldsymbol{Z}_N}(X_i)$ with the different control parameters. And we design a sequence generated algorithm based on the Logistic map for $N = 3^n$.

Theorem 7. Assuming h and h' are two automorphic maps, G and G' are the periodic sequences generated by h and h'. They can be given by

$$G = \{x_0, x_1, x_2, \ldots\}, \quad x_{i+1} = h(x_i), \quad i = 0, 1, 2, \ldots,$$

$$G' = \{x'_0, x'_1, x'_2, \ldots\}, \quad x'_{i+1} = h'(x'_i), \quad i = 0, 1, 2, \ldots,$$

when $i = 0, 1, 2, \ldots$, and if there is an equation $x'_i = f(x_i)$, the period of G is the same as G'.

Proof. Assume T is the length of period for G and there exist subsequences $\{x_0, x_1, x_2, \ldots, x_{T-1}\}$ and $\{x_l, x_{l+1}, x_{l+2}, \ldots, x_{l+T-1}\}$. Accordingly, $x_l = x_{l+T}$ and $x_j \neq x_{j+T}$, where $j = 0, 1, 2, \ldots, l-1$. For any x_i, there is $x'_i = f(x_i)$, so G' must contain the periodic sequence $\{x'_0, x'_1, x'_2, \ldots, x'_{T-1}\}$ and $\{x'_l, x'_{l+1}, x'_{l+2}, \ldots, x'_{l+T-1}\}$. Therefore, the period of G is the same as the period of G'.

Theorem 8. When $\mu_N \bmod 9 = 0$ or 3 or 6, or $\mu_N \bmod 9 = 2$ or 5 or 8, or $\mu_N = 1$, there is not an automorphic map for $L_{\boldsymbol{Z}_N}(X_i)$.

Proof. According to Theorems 1 and 3, the maximum period of $L_{\boldsymbol{Z}_N}(X_i)$ is 1 and the final value of $L_{\boldsymbol{Z}_N}(X_i)$ is 0 when $\mu_N \bmod 9 = 0$ or 3 or 6, and the maximum period of $L_{\boldsymbol{Z}_N}(X_i)$ is 1 and the final value of $L_{\boldsymbol{Z}_N}(X_i)$ is a constant C when $\mu_N \bmod 9 = 2$ or 5 or 8, respectively. So there is no automorphic map for $L_{\boldsymbol{Z}_N}(X_i)$ when $\mu_N \bmod 9 = 0$ or 3 or 6, or $\mu_N \bmod 9 = 2$ or 5 or 8. When $\mu_N = 1$, there is only one fixed point 0. Therefore, there is no automorphic map for $L_{\boldsymbol{Z}_N}(X_i)$ when $\mu_N = 1$.

According to the above theorem, we present the following theorem.

Theorem 9. Let $N = 3^n$, μ_N is an integer in the interval $4 \leqslant \mu_N \leqslant N-1$, with $n \geqslant 3$ for $\mu_N \bmod 9 = 1$, or $n \geqslant 4$ for $\mu_N \bmod 9 = 4$ or 7. We define

$$X'_i = f(X_i) = pX_i + q \pmod N,$$

where $p, q \in Z_N$. When $\mu_N \neq \mu'_N$, if there is an automorphic map f between $L_{\boldsymbol{Z}_N}(X_i)$ with μ_N and $L_{\boldsymbol{Z}_N}(X'_i)$ with μ'_N, we have $p \equiv 2q + 1 \pmod N$.

Proof. Let f be an automorphic map, we define $L_{\boldsymbol{Z}_N}(X_i)_{\mu_N}$ as $L_{\boldsymbol{Z}_N}(X_i)$ with μ_N, and $L_{\boldsymbol{Z}_N}(X'_i)_{\mu'_N}$ as $L_{\boldsymbol{Z}_N}(X'_i)$ with μ'_N,

$$f(L_{\boldsymbol{Z}_N}(X_i)_{\mu_N}) \equiv L_{\boldsymbol{Z}_N}(f(X))_{\mu'_N} \pmod N, \tag{12}$$

then

$$X'_i = f(L_{\boldsymbol{Z}_N}(X_i)\mu_N = pL_{\boldsymbol{Z}_N}(X_i)_{\mu_N} + q = p\mu_N X_i^2 + p\mu_N X_i + q \pmod N, \tag{13}$$

and

$$X'_i = L_{\boldsymbol{Z}_N}(f(X_i))_{\mu'_N} = L_{\boldsymbol{Z}_N}(pX_i + q)_{\mu'_N} = p^2\mu'_N X_i^2 + \mu'_N(2pq + p)X_i + (q^2 + q)\mu'_N (\bmod N). \tag{14}$$

As Eqs. (12)–(14) must be the same, we get

$$p\mu_N = p^2\mu'_N \pmod N, \tag{15}$$

$$p\mu_N = \mu'_N(2pq + p) \pmod N, \tag{16}$$

$$q = (q^2 + q)\mu'_N \pmod N, \tag{17}$$

Obviously, there are $p \neq 0$ and $q \neq 0$. From Eqs. (15)–(17), we can get the following equations:

$$\mu_N = p\mu'_N \pmod N, \tag{18}$$

$$\mu_N = \mu'_N(2q + 1) \pmod N, \tag{19}$$

$$(q+1)\mu'_N = 1 \pmod N. \tag{20}$$

From Eqs. (18) and (19), we get

$$p \equiv 2q+1 \pmod N. \tag{21}$$

Lemma 4. According to Theorem 9, we can get $\mu_N + \mu'_N = kN + 2$, where k is a positive integer in the interval $k \geqslant 1$.

Proof. With Eq. (20), the following equation must exist

$$(2q+2)\mu'_N \equiv 2 \pmod N. \tag{22}$$

Then by Eq. (21), we get $p+1 \equiv 2q+2(\text{mod } N)$. By using Eq. (22), we get $(p+1)\mu'_N \equiv 2(\text{mod } N)$. Therefore, $p\mu'_N + \mu'_N \equiv 2(\text{mod } N)$. By using Eq. (18), we get

$$\mu_N + \mu'_N \equiv 2(\text{mod } N). \tag{23}$$

Finally, there exists a constant $k \geqslant 1$, and

$$\mu_N + \mu'_N = kN + 2. \tag{24}$$

Theorem 10. Letting $N = 3^n$, μ_N is a control parameter of $L_{\boldsymbol{Z}_N}(X_i)$ in the interval $4 \leqslant \mu_N \leqslant N-1$, with $n \geqslant 3$ for $\mu_N \bmod 9 = 1$, or $n \geqslant 4$ for $\mu_N \bmod 9 = 4$ or 7. $X_i, X'_i \in \boldsymbol{Z}_N$. We can get another control parameter μ'_N given by

$$\mu'_N = kN + 2 - \mu_N,$$

where k is a positive integer in the interval $k \geqslant 1$. The maps $L_{\boldsymbol{Z}_N}(X_i)_{\mu_N}$ and $L_{\boldsymbol{Z}_N}(X'_i)_{\mu'_N}$ with f are automorphic. It is also said that any X_i of $L_{\boldsymbol{Z}_N}(X_i)_{\mu_N}$ can be changed into X'_i of $L_{\boldsymbol{Z}_N}(X'_i)_{\mu'_N}$ with an automorphic map $\text{Aut}_{\mu_N} : \boldsymbol{Z}_N \to \boldsymbol{Z}_N$. Therefore,

$$X'_i = \text{Aut}_{\mu_N}(X_i) = \frac{\mu_N(X_i+1)-1}{2-\mu_N} \pmod N. \tag{25}$$

Proof. Using Eq. (23), we can get $\mu'_N \equiv 2 - \mu_N(\text{mod } N)$. According to Eqs. (18) and (20), we get $\mu_N = p(2-\mu_N)(\text{mod } N)$, and $(q+1)(2-\mu_N) \equiv 1(\text{mod } N)$. Using the above two equations, we can get $p = \frac{\mu_N}{2-\mu_N}(\text{mod } N)$, and $q = \frac{\mu_N - 1}{2-\mu_N}(\text{mod } N)$. According to Theorem 9, the automorphic map $\text{Aut}_{\mu_N}(X_i)$ is given by

$$X'_i = \text{Aut}_{\mu_N}(X_i) = pX_i + q = \frac{\mu_N(X_i+1)-1}{2-\mu_N} \pmod N.$$

According to Theorem 10, we can define an inverse map of $\text{Aut}_{\mu_N}(X_i)$ as $\text{Aut}^{-1}_{\mu_N} : \boldsymbol{Z}_N \to \boldsymbol{Z}_N$. By using Eq. (25), we get

$$\text{Aut}^{-1}_{\mu_N}(X'_i) = \frac{(2-\mu_N)X'_i + (1-\mu_N)}{\mu_N}. \tag{26}$$

Because of Eq. (23), $1-\mu_N \equiv \mu'_N - 1(\text{mod } N)$, and $2-\mu_N \equiv \mu'_N(\text{mod } N)$, and $2-\mu'_N \equiv \mu_N(\text{mod } N)$, Eq. (26) can be changed into

$$\text{Aut}^{-1}_{\mu_N}(X'_i) = \frac{\mu'_N(X'_i+1)-1}{2-\mu'_N} \equiv \text{Aut}_{\mu'_N}(X'_i) \pmod N. \tag{27}$$

Therefore, the maps $L_{\boldsymbol{Z}_N}(X'_i)_{\mu'_N}$ and $L_{\boldsymbol{Z}_N}(X_i)_{\mu_N}$ with f^{-1} are automorphic. It is also said that any X'_i of $L_{\boldsymbol{Z}_N}(X'_i)_{\mu'_N}$ can be changed into X_i of $L_{\boldsymbol{Z}_N}(X_i)_{\mu_N}$ with an automorphic map $\text{Aut}_{\mu'_N} : \boldsymbol{Z}_N \to \boldsymbol{Z}_N$ while $\text{Aut}_{\mu'_N} = \text{Aut}^{-1}_{\mu_N}$. Moreover, we get

$$\text{Aut}_{\mu_N}(L_{\boldsymbol{Z}_N}(X_i)_{\mu_N}) = \frac{\mu_N^2 X_i^2 + \mu_N^2 X_i + \mu_N - 1}{2-\mu_N}(\text{mod } N), \tag{28}$$

and

$$L_{\boldsymbol{Z}_N}(\text{Aut}_{\mu_N}(X_i))_{\mu'_N} = \frac{\mu_N^2 X_i^2 + \mu_N^2 X_i + \mu_N - 1}{2-\mu_N}(\text{mod } N), \tag{29}$$

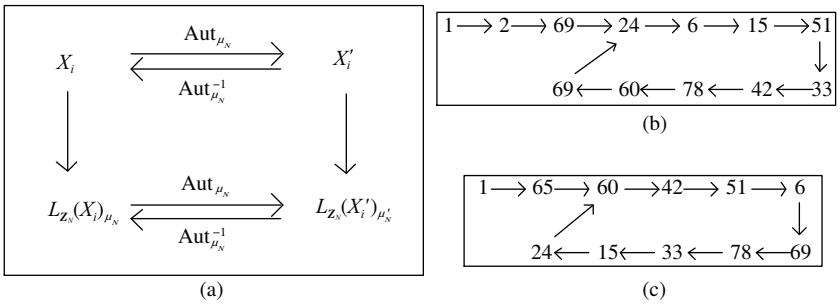

Figure 1 (a) The relations between maps and elements of $L_{\boldsymbol{Z}_N}$; (b) the trajectory of $L_{\boldsymbol{Z}_N}(X_i)$, where $\mu_N = 10$, $n = 4$, $N = 81$; (c) the trajectory of $L_{\boldsymbol{Z}_N}(X_i)$, where $\mu'_N = 73$, $n = 4$, $N = 81$, $k = 1$.

and

$$\mathrm{Aut}^{-1}_{\mu_N}(L_{\boldsymbol{Z}_N}(X'_i)_{\mu'_N}) = \frac{(\mu'_N)^2(X'_i)^2 + (\mu'_N)^2 X'_i + \mu'_N - 1}{2 - \mu'_N} (\mathrm{mod}\ N), \tag{30}$$

and

$$L_{\boldsymbol{Z}_N}(\mathrm{Aut}^{-1}_{\mu_N}(X'_i))_{\mu_N} = \frac{(\mu'_N)^2(X'_i)^2 + (\mu'_N)^2 X'_i + \mu'_N - 1}{2 - \mu'_N} (\mathrm{mod}\ N). \tag{31}$$

By Eqs. (28)–(31), we get

$$\mathrm{Aut}_{\mu_N}(L_{\boldsymbol{Z}_N}(X_i)_{\mu_N}) = L_{\boldsymbol{Z}_N}(\mathrm{Aut}_{\mu_N}(X_i))_{\mu'_N}, \tag{32}$$

$$\mathrm{Aut}^{-1}_{\mu_N}(L_{\boldsymbol{Z}_N}(X'_i)_{\mu'_N}) = L_{\boldsymbol{Z}_N}(\mathrm{Aut}^{-1}_{\mu_N}(X'_i))_{\mu_N}. \tag{33}$$

So we can get the following relations between maps and elements of $L_{\boldsymbol{Z}_N}$ (see Figure 1(a)).

Example 8. When $\mu_N = 10$, $n = 4$, $N = 81$, we have Figure 1(b) showing the trajectory of sequences generated by $L_{\boldsymbol{Z}_N}(X_i)$ over the finite field $N = 3^n$. When $\mu'_N = 73$, $n = 4$, $N = 81$, $k = 1$, we also have Figure 1(c) showing the trajectory of sequences generated by $L_{\boldsymbol{Z}_N}(X_i)$ for the finite field $N = 3^n$. From these figures, we can know that $\mathrm{Aut}_{\mu_N}(24) = 60$, $\mathrm{Aut}_{\mu_N}(6) = 42$, $\mathrm{Aut}_{\mu_N}(15) = 51$, $\mathrm{Aut}_{\mu_N}(51) = 6$, $\mathrm{Aut}_{\mu_N}(33) = 69$, $\mathrm{Aut}_{\mu_N}(42) = 78$, $\mathrm{Aut}_{\mu_N}(78) = 33$, $\mathrm{Aut}_{\mu_N}(60) = 15$, $\mathrm{Aut}_{\mu_N}(69) = 24$. Therefore, the results also verify that the formula of (32) and (33) are correct.

According to (28), we can define

$$T_{\mu_N}(x) = \mathrm{Aut}_{\mu_N}(L_{\boldsymbol{Z}_N}(x)_{\mu_N}), \tag{34}$$

and

$$T_{\mu'_N}(x) = \mathrm{Aut}^{-1}_{\mu_N}(L^{-1}_{\boldsymbol{Z}_N}(x)_{\mu'_N}). \tag{35}$$

Now, we can present an automorphic sequence generated algorithm by using the Logistic map with the different control parameters μ_N and μ'_N over the finite field $N = 3^n$, for example, Algorithm 1. This method has some advantages. One of them is that these maps always give two sequences which have the same period, while they are contained by different values. Another advantage is that these two sequences can replace each other. So, these two sequences have the same properties, and anyone can convert one of them into the other easily. The traditional cryptography which works on integer numbers and chaotic cryptosystem which works on real numbers the security of both is worthy of study. And the above method is suitable for the sequence generator in cryptosystem. These sequences can be used in the pseudorandom number generator, the chaotic stream cipher, and the chaotic block cipher, etc.

5 Performance analysis of Logistic map over $N = 3^n$

In this section, an experiment is designed to verify the properties of period distribution of sequences generated by Logistic map. We choose 1000 initial values at random, and iterate the mapping until it enters the period. Figure 2 shows the length of maximum period for the Logistic map over the finite field $N = 3^n$ where $10 \leqslant n \leqslant 20$, and $1 \leqslant \mu_N \leqslant N - 1$.

Algorithm 1 The automorphic sequence generated algorithm.

Input: μ_N, n, H, k, x_0;
$N = 3^n$;
$\mu'_N = kN + 2 - \mu_N$;
for i=1:1:H
$L_{\boldsymbol{Z}_N}(x_{i-1})_{\mu_N}$;
end
Output 1: x_0, x_1, x_2, ..., x_H,
We calculate the periodic sequence as Seq 1 from Output 1.
Then we select any one number as x_m from Seq 1.
$x'_1 = \mathrm{Aut}_{\mu_N}(x_m)$;
T=length(Seq 1);
for j=2:1:T
$L_{\boldsymbol{Z}_N}(x'_{j-1})_{\mu'_N}$;
end
Output 2: x'_1, x'_2, ..., x'_T
Output 2 as Seq 2 is the automorphic sequence of Seq 1.

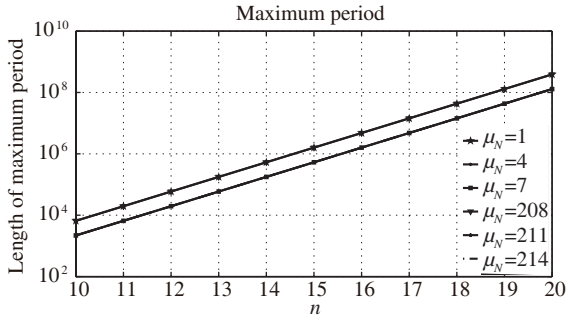

Figure 2 Length of maximum period.

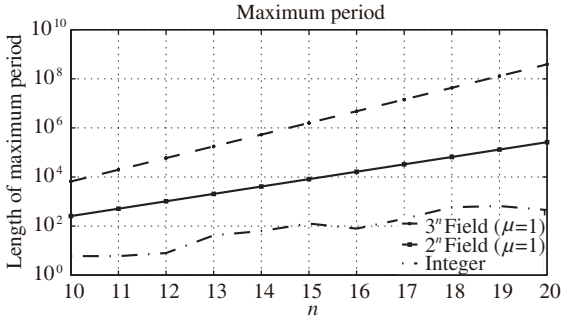

Figure 3 Maximum period of each mapping.

Table 1 Generation time (s)

	$L_{\boldsymbol{Z}_{3^n}}(X_i)$	$L_{\boldsymbol{Z}_{2^n}}(X_i)$	$L_{\boldsymbol{Z}_{\mathrm{Int}}}(X_i)$
Maximum	0.3890	0.3280	0.1667
Minimum	0.2674	0.2816	0.1444
Average	0.2757	0.2873	0.1476

A similar experiment is carried out in other Logistic maps about the finite field $N = 3^n$, $N = 2^n$ and the integer field respectively. Figure 3 shows the experimental results. In Figure 3, the period of $L_{\boldsymbol{Z}_{3^n}}(X_i)$ is increased on the order of $10^2 \sim 10^4$ compared with that of $L_{\boldsymbol{Z}_{2^n}}(X_i)$, and the period of $L_{\boldsymbol{Z}_{3^n}}(X_i)$ is increased on the order of $10^3 \sim 10^7$ compared with that of $L_{\boldsymbol{Z}_{\mathrm{Int}}}(X_i)$. Therefore, it is possible to obtain a longer period than the conventional one, and it is useful for cryptographic application.

The generation time is an important indicator to measure the performance of a pseudorandom number generator for cryptographic application. So we design another experiment to test the generation time of sequences generated by Logistic map over $\boldsymbol{Z}_N$. We choose the initial values at random, iterate the mapping 10000000 times, and the number of n is 32. Then we calculate the maximum time, the minimum time, and the average time with repeating 1000 times, where the control parameters fixed by each map are as follows:

$$L_{\boldsymbol{Z}_{3^n}}(X_i) : \mu_N = 1, N = 3^{32},$$

$$L_{\boldsymbol{Z}_{2^n}}(X_i) : \mu_N = 1, N = 2^{32},$$

$$L_{\boldsymbol{Z}_{\mathrm{Int}}}(X_i) : \mu = 4.0.$$

The results are shown in Table 1. The generation time of $L_{\boldsymbol{Z}_{3^n}}(X_i)$ is almost the same fast as $L_{\boldsymbol{Z}_{2^n}}(X_i)$, and the generation time of $L_{\boldsymbol{Z}_{\mathrm{Int}}}(X_i)$ is faster than the above two mappings.

6 Conclusion

In this paper, we have made analysis for period of sequences generated by the Logistic map for the finite field $N = 3^n$, and have studied the statistical properties of the period for the map. Moreover, we discuss the control parameters which can change the behavior of the mapping. We show that the period of the Logistic map over $\boldsymbol{Z}_{3^n}$ is longer than that of previous variants, and we also have found that the maximum period can be changed by the control parameter. In addition, the property of generated sequences by the Logistic map over $\boldsymbol{Z}_{3^n}$ is greatly changed by a parity of the control parameter. We have also found that there exists an automorphic map between two Logistic maps with the different control parameters, and have designed an automorphic sequence generated algorithm based on the Logistic map over $\boldsymbol{Z}_{3^n}$. This algorithm is suitable for the sequence generator in cryptosystem. And these sequences can be used in the pseudorandom number generator, the chaotic stream cipher, and the chaotic block cipher, etc. We show that Logistic map over $\boldsymbol{Z}_{3^n}$ may be suitable for cryptographic application by performance analysis. In the future, we will discuss other properties about period of sequences with different initial values of Logistic map for the finite field.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 61472331), Research Fund of Preferential Development Domain for the Doctoral Program of Ministry of Education of China (Grant No. 20110191130005), Talents of Science and Technology Promote Plan (Chongqing Science & Technology Commission), and Fundamental Research Funds for the Central Universities (Grant No. XDJK2015C078).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Kolmogorov A N. On conservation of conditionally periodic motions under small perturbations of the Hamiltonian. Dokl Akad Nauk SSSR, 1954, 98: 527–530
2 Lorenz E N. Deterministic non-periodic follow. J Atmos Sci, 1963, 20: 130–141
3 Henon M. Two-dimensional mapping with a strange attractor. Comm Math Phys, 1976, 50: 69–77
4 May R. Simple mathematical model with very complicated dynamics. Nature, 1976, 261: 459–467
5 Feigenbaum M. Quantitative universality for a class of nonlinear transformations. J Stat Phys, 1978, 19: 25–52
6 Robert A, Matthews J. On the derivation of a chaotic encryption algorithm. Cryptologia, 1989, 13: 29–42
7 Pecora L, Carroll T. Synchronization in chaotic systems. Phys Rev Lett, 1989, 64: 821–824
8 El Gamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Inf Theory, 1985, 31: 469–472
9 Kohda T, Tsuneda A. Statistics of chaotic binary sequences. IEEE Trans Inf Theory, 1997, 43: 104–112
10 Kocarev L, Lian S. Chaos-Based Cryptography: Theory, Algorithms and Applications. New York: Springer-Verlag, 2011
11 Kocarev L. Chaos-based cryptography: a brief overview. IEEE Circ Syst Mag, 2001, 1: 6–21
12 Gong G, Ham L. Public-key cryptosystems based on cubic finite field extensions. IEEE Trans Inf Theory, 1999, 45: 2601–2605
13 Kolumban G, Kennedy M. The role of synchronization in digital communications using chaos-part III: performance bounds for correlation receivers. IEEE Trans Circ Syst, 2000, 47: 1673–1683
14 Jakimoski G, Kocarev L. Chaos and cryptography: block encryption ciphers based on chaotic maps. IEEE Trans Circ Syst I: Fundam Theory Appl, 2001, 48: 163–169
15 Chen G, Mao Y, Chui C. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Soliton Fract, 2004, 21: 749–761
16 Pisarchik A N, Flores-Carmona N J, Carpio-Valadez M. Encryption and decryption of images with chaotic map lattices. Chaos Interdisciplinary J Nonlinear Sci, 2006, 16: 033118
17 Hasimoto-Beltran R. High-performance multimedia encryption system based on chaos. Chaos Interdisciplinary J Nonlinear Sci, 2008, 18: 023110
18 Liao X F, Chen F, Wong K W. On the security of public-key algorithms based on chebyshev polynomials over the finite field Z_N. IEEE Trans Comput, 2010, 59: 1392–1401
19 Arnold V, Avez A. Ergodic Problems of Classical Mechanics. New York: Benjamin, 1968
20 Wong W K, Lee L P, Wong K W. A modified chaotic cryptographic method. Comput Phys Commun, 2001, 138: 234–236
21 Wong K W. A fast chaotic cryptographic scheme with dynamic look-up table. Phys Lett A, 2002, 298: 238–242

22 Wong K W, Ho S W, Yung C K. A chaotic cryptography scheme for generating short ciphertext. Phys Lett A, 2003, 310: 67–73
23 Xiang T, Liao X F. A novel block cryptosystem based on iterating a chaotic map. Phys Lett A, 2006, 349: 109–115
24 Tong X J, Cui M G. Feedback image encryption algorithm with compound chaotic stream cipher based on perturbation. Sci China Inf Sci, 2010, 53: 191–202
25 Yin R M, Wang J, Yuan J, et al. Weak key analysis for chaotic cipher based on randomness properties. Sci China Inf Sci, 2012, 55: 1162–1171
26 Arroyo D, Alvarez G, Amigó J, et al. Cryptanalysis of a family of self-synchronizing chaotic stream ciphers. Original Res Article Commun Nonlinear Sci Numer Simulat, 2011, 16: 805–813
27 Li C, Li S, Lo K. Breaking a modified substitution-diffusion image cipher based on chaotic standard and logistic maps. Original Res Article Commun Nonlinear Sci Numer Simulat, 2011, 16: 837–843
28 Chen F, Wong K W, Liao X F, et al. Period distribution of generalized discrete arnold cat map for $N = p^e$. IEEE Trans Inf Theory, 2012, 58: 445–452
29 Chen F, Wong K W, Liao X F, et al. Period distribution of the generalized discrete arnold cat map for $N = 2^e$. IEEE Trans Inf Theory, 2013, 59: 3249–3255
30 Chen F, Liao X F, Xiang T, et al. Security analysis of the public key algorithm based on Chebyshev polynomials over the integer ring $\boldsymbol{Z}_N$. Inf Sci, 2011, 181: 5110–5118
31 Yoshida K, Miyazaki T, Uehara S, et al. Some properties of the maximum period on the Logistic map over $\boldsymbol{Z}_{2^n}$. In: Proceedings of International Symposium on Information Theory and its Applications, Melbourne, 2014. 665–668
32 Miyazaki T, Araki S, Uehara S, et al. A study of an automorphism on the Logistic maps over prime fields. In: Proceedings of International Symposium on Information Theory and its Applications, Melbourne, 2014. 714–718
33 Miyazaki T, Araki S, Uehara S. Some properties of Logistic maps over integers. IEICE Trans Fundamentals, 2010, 93: 2258–2265
34 Miyazaki T, Araki S, Uehara S, et al. A study on the pseudorandom number generator for the Logistic map over prime fields. In: Proceedings of the 30th Symposium on Cryptography and Information Security, Japanese, 2013
35 Silverman J H. The Arithmetic of Dynamical Systems. New York: Springer-Verlag, 2007
36 Ireland K, Rosen M. A Classical Introduction to Modern Number Theory. Volume 84 of Graduate Texts in Mathematics. 2nd ed. New York: Springer-Verlag, 1990
37 Keen L. Julia sets of rational maps. Comp Dyn Syst, 1994, 49: 71–90
38 Carleson L, Gamelin T W. Complex dynamics. In: Universitext: Tracts in Mathematics. New York: Springer-Verlag, 1993