SCIENCE CHINA
Information Sciences

• LETTER •

March 2019, Vol. 62 039104:1–039104:3
https://doi.org/10.1007/s11432-017-9438-8

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

Received 1 December 2017/Accepted 19 April 2018/Published online 10 October 2018

Citation Yang B, Liao X F. Some characteristics of logistic map over the finite field. Sci China Inf Sci, 2019, 62(3): 039104, https://doi.org/10.1007/s11432-017-9438-8

Dear editor,

Chaotic maps have good characteristics, which include randomness, sensitivity to the initial value, and unpredictability. Hence, there have been many attempts to discuss the dynamic behavior of chaotic maps in the field of chaotic cryptography. However, the limited computation, finite memory, and restricted communication capabilities in application causes the state space of the chaotic map to possibly be discrete [1]. How to choose a chaos system that conforms to the cryptographic conditions is a very important issue of study.

There are many discrete chaos maps that contain a Logistic map. Two typical Logistic maps used in the real field are defined as $L1_R(x) = \mu x(1-x)$, $L2_R(x) = 1-\mu x^2$. However, traditional chaos maps in the real domain have a particular drawback, i.e., the computational complexity is two-fold when we implement a floating point number of a map in a computer. In addition, this leads to a significantly critical problem in actual engineering application. To overcome this problem, many researchers have considered chaotic systems over the finite field [2, 3]. Determining the length is considerably important in various applications such as sequence design and cryptography. A number of researches have also proved that a Logistic map over a finite field can generate a long sequences [4, 5]. For the security of a cryptosystem, long passwords can make an attack difficult to conduct. Although the computing of a traditional Logistic map on a computer with limited precision is bound to degenerate the result to limited precision, restricted complexity, and finite randomness, among others, these drawbacks are detrimental to the security of a password system.

In [6], to overcome these problems, the authors discussed some characteristics of sequences generated from a Logistic map $L1_R(x) = \mu x(1-x)$ over the finite field $\mathcal{Z}_{2^n}$, but provided an incomprehensive theoretical proof. We continue to analyze this Logistic map over $\mathcal{Z}_{2^n}$ using a theoretical analysis. The above two Logistic maps over the real domain have similar properties, whereas the specific characteristics of the Logistic maps over the finite field are not involved. In [7], the authors considered Logistic map-1, $L1_R(x) = \mu x(1-x)$, over $\mathcal{Z}_{3^n}$, and analyzed the period features of the sequences generated over $\mathcal{Z}_{3^n}$. In this study, we generalize Logistic map-2, $L2_R(x) = 1-\mu x^2$, over $\mathcal{Z}_{3^n}$. In addition, we find their efficiently computational form and describe the period features of the sequences generated from Logistic map-2 over $\mathcal{Z}_{3^n}$ through an theoretical analysis.

We define $N = q^n$ as a modulo, where q is a small prime number and n is a natural number. Logistic map-1 over $\mathcal{Z}_N$ can then be defined as [6]

$$L1_{\mathcal{Z}_N}(X_i) = \mu_N X_i(X_i+1) \pmod N, \qquad (1)$$

where $\mu_N \in [1, N-1]$, $X_i \in [0, N-1]$.

Logistic map-2 over a real field can be written as $L2_R(x_i) = 1-\mu x_i^2$, where $\mu \in [0, 2]$, $x_i \in [-1, 1]$.

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

It is well known that when $\mu = 2$ the Logistic mapping enters into chaos. We provide Logistic mapping over the integer field as $L2_R^{(n)}(x'_i) = 2^n - \mu(x'_i)^2/2^n$, where n is the element precision of the map, $x'_i = 2^n x_i$, and $L2_R^{(n)}(x'_i) = 2^n L2_R(x_i)$. We then derive a function for the Logistic mapping over the integer field as $L2_{\text{Int}}^{(n)}(X_i) = \lfloor 2^n - \mu X_i^2/2^n \rfloor$, where $X_i \in [0, 2^n]$ is the integral part of x'_i, and $\lfloor \cdot \rfloor$ is the bracket function. The Logistic mapping over a prime field can be defined as $L2_{\mathcal{Z}_p}(X_i) = (p-1) - (\mu_p X_i^2)/(p-1) (\text{mod } p)$, where p is a prime number, $\mathcal{Z}_p$ is a field for modulo p, $X_i \in [0, p-1]$, and $\mu_p \in [0, p-1]$.

Definition 1. According to (1), we define the Logistic map-2 over $\mathcal{Z}_N$ as

$$L2_{\mathcal{Z}_N}(X_i) = (N-1) - \frac{\mu_N X_i^2}{N-1} \pmod N, \quad (2)$$

where $\mu_N \in [0, N-1]$, $X_i \in [0, N-1]$.

Lemma 1.

$$L2_{\mathcal{Z}_N}(X_i) = \mu_N X_i^2 - 1 \pmod N. \quad (3)$$

According to Lemma 1, the computation of X_i of (3) is more available than that of (2).

The characteristics of the generation sequences from Logistic map-1 over $\mathcal{Z}_{2^n}$ are as follows.

Theorem 1. When $\mu_N \bmod 4 = 0$ or 2, the maximum period of $L1_{\mathcal{Z}_N}(X_i)$ is 1, and the final value of $L1_{\mathcal{Z}_N}(X_i)$ is 0 [6].

Lemma 2 ([6]). $L1_{\mathcal{Z}_N}(N - X_i - 1) = L1_{\mathcal{Z}_N}(X_i)$.

Theorem 2. Suppose that a field K does not have a characteristic value 2, and a quadratic polynomial $\phi(z) = Az^2 + Bz + C$ can be transformed into $z^2 + c$ with a simple variable transformation in K.

Theorem 3. A Mandelbrot set is included in the disk of radius 2, and thus $M \subset c \in C : |c| \leqslant 2$.

Definition 2. When a point 0 is sternly preperiodic with $\phi_c(z) = z^2 + c$, then the point c can be defined as a Misiurewicz point. We have point c, which can be a Misiurewicz point, as a fixed periodic point, and the period can be described as the type (m, n) when $m \geqslant 1$ is the minimum integer number, and in this way $\phi_c^m(0)$ is periodic, but only if n is a primitive period of $\phi_c^m(0)$.

Let $A = \mu_N$, $B = \mu_N$, $C = 0$. We have $f(z) = (2z - \mu_N)/(2\mu_N)$, and $f^{-1}(z) = (2\mu_N z + \mu_N)/2$. Then $L1^f_{\mathcal{Z}_N}(X_i) = (f^{-1} \circ L1_{\mathcal{Z}_N} \circ f)(X_i) = X_i^2 + c$, where $c = \frac{1}{4}(2\mu_N - \mu_N^2)$. Therefore, periodic property of $L1_{\mathcal{Z}_N}(X_i)$ is the same as that of $L1^f(X_i)$.

Theorem 4. When $\mu_N \bmod 4 = 3$, the maximum period of $L1_{\mathcal{Z}_N}(X_i)$ is $\frac{N}{16} = 2^{n-4}$.

Theorem 5. When $\mu_N \bmod 4 = 1$, the maximum period of $L1_{\mathcal{Z}_N}(X_i)$ is $\frac{N}{4} = 2^{n-2}$.

Lemma 3. According to Theorem 2, Eq. (3) can be changed into $L2^f(X_i) = X_i^2 - \mu_N$.

Therefore, the periodic property of $L2_{\mathcal{Z}_N}(X_i)$ is the same as that of $L2^f(X_i)$. The characteristics of the generation sequences from Logistic map-2 over $\mathcal{Z}_{3^n}$ are as follows.

Theorem 6. When $\mu_N \bmod 9 = 0$ or 3 or 6, the maximum period of $L2_{\mathcal{Z}_N}(X_i)$ is 1.

Theorem 7. When $\mu_N \bmod 9 = 1$ or 4 or 7, the maximum period of $L2_{\mathcal{Z}_N}(X_i)$ is 2.

Lemma 4. $L2_{\mathcal{Z}_N}(N - X_i) = L2_{\mathcal{Z}_N}(X_i)$.

Theorem 8. When $\mu_N \bmod 9 = 2$, the maximum period of $L2_{\mathcal{Z}_N}(X_i)$ is $\frac{N}{9} = 3^{n-2}$.

Theorem 9. When $\mu_N \bmod 9 = 8$, the maximum period of $L2_{\mathcal{Z}_N}(X_i)$ is $\frac{N}{9} = 3^{n-2}$.

Theorem 10. When $\mu_N \bmod 9 = 5$, the maximum period of $L2_{\mathcal{Z}_N}(X_i)$ is $\frac{N}{3} = 3^{n-1}$.

We designed an experiment to prove the characteristics of the period range of sequences generated from Logistic map-2 over $\mathcal{Z}_{3^n}$. We selected 1000 random initial values, and calculated Logistic map-2 until it entered into the period range. Figure 1(a) describes the maximum period length of Logistic map-2 over $\mathcal{Z}_{3^n}$ where $10 \leqslant n \leqslant 20$, and $1 \leqslant \mu_N \leqslant N - 1$. In Figure 1(a), the lines of $\mu_N = 5$ and $\mu_N = 212$ are overlapped, as are the lines of $\mu_N = 74$, $\mu_N = 80$, $\mu_N = 254$, and $\mu_N = 305$. This is because the length of the maximum period of $L2_{\mathcal{Z}_{3^n}}(X_i)$ at $\mu_N = 5$ is the same as that when $\mu_N = 212$ according to Theorem 10, and the length of the maximum period of $L2_{\mathcal{Z}_{3^n}}(X_i)$ at $\mu_N = 74$ is the same as that when $\mu_N = 80$, $\mu_N = 254$, and $\mu_N = 305$ according to Theorems 8 and 9.

Another experiment was designed using two Logistic mappings over different fields, the results of which are shown in Figure 1(b). In Figure 1(b), the period of $L2_{\mathcal{Z}_{3^n}}(X_i)$ is 3 times longer than that of $L1_{\mathcal{Z}_{3^n}}(X_i)$ in [7], reaching the order of 10^4–10^9. The period of $L2_{\mathcal{Z}_{3^n}}(X_i)$ is increased on the order of 10^2–10^4 compared with that of $L1_{\mathcal{Z}_{2^n}}(X_i)$ in [6]. The period of $L2_{\mathcal{Z}_{3^n}}(X_i)$ is increased on the order of 10^4–10^6 compared with that of $L2_{\mathcal{Z}_{\text{Int}}}(X_i)$, which is not expanded to the finite field. Therefore, our proposed method is able to generate a pseudorandom sequence that obtains a much longer length, and is much more suitable for practical engineering application.

The generation time is a very significant index to judge the performance of a pseudorandom generation method. We designed an experiment to measure the generation time of the generation sequences from Logistic mappings over $\mathcal{Z}_N$. We iterate the Logistic mapping by repeating it 1000 times, where the length of the sequence is

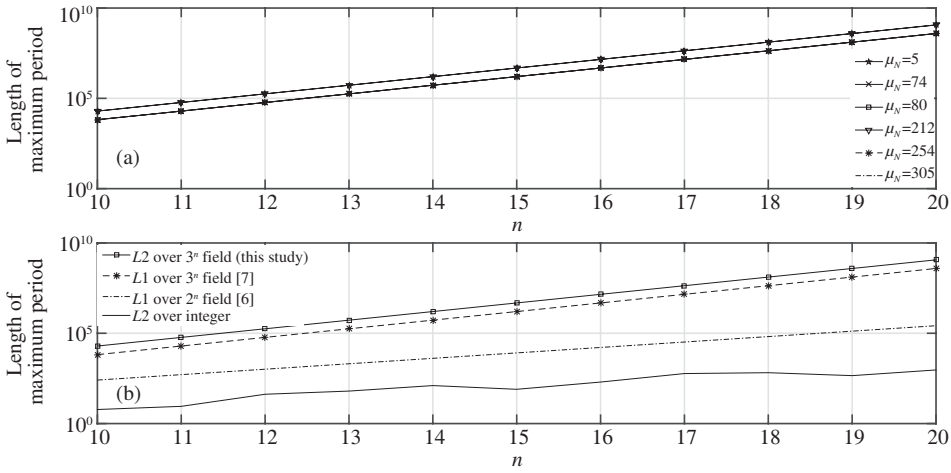

Figure 1 (a) Length of maximum period for $L2_{\mathcal{Z}_{3^n}}(X_i)$; (b) maximum period of each mapping.

10000000 when $n = 32$. In addition, we obtain the maximum, minimum, and average time for $L2_{\mathcal{Z}_{3^n}}(X_i)$ as $\mu_N = 5$ and $N = 3^{32}$, and as $\mu_N = 1$ and $N = 3^{32}$ for $L1_{\mathcal{Z}_{3^n}}(X_i)$ in [7]. The generation time (maximum time, 0.2869 s; minimum time, 0.2304 s; and average time, 0.2342 s) of $L2_{\mathcal{Z}_{3^n}}(X_i)$ in this study is faster than that (maximum time, 0.2887 s; minimum time, 0.2788 s; and average time, 0.2826 s) of $L1_{\mathcal{Z}_{3^n}}(X_i)$ in [7].

The proofs for all lemmas and theorems are included in Appendixes A–L. Some other characteristics of $L1_{\mathcal{Z}_N}(X_i)$ and $L2_{\mathcal{Z}_N}(X_i)$ regarding pseudorandom sequence, power spectrum, correlation property, phase diagram, and Lyapunov exponent are presented in Appendix M.

Conclusion. We generalized two Logistic maps to a finite field and found their efficiently computational forms using different parameters of the mapping over this field $\mathcal{Z}_N$. We analyzed the period features regarding the sequences generated from Logistic map-1 over $\mathcal{Z}_{2^n}$ and Logistic map-2 over $\mathcal{Z}_{3^n}$, and studied the statistical characteristics of the period features for the maps. We analyzed the behavior of a Logistic map, which can be changed based on the parameters, and found that the maximum period of sequences generated over $\mathcal{Z}_N$ can be changed according to the different control parameters. The length of sequences generated from Logistic map-2 over $\mathcal{Z}_{3^n}$ is much longer than that from Logistic map-2 over an integer field, and much longer than that from Logistic map-1 over $\mathcal{Z}_{3^n}$. The generation time of Logistic map-2 is faster than that of Logistic map-1. In addition, the length of these sequences is much longer, and is available for the pseudorandom number generation, chaotic encryption. Simulations of other characteristics have shown that a Logistic map over a finite field has non-periodic, random, noise-like properties, a continuous spectrum, good correlation, good uniform distribution, controllable length of the generated sequence, and positive Lyapunov exponent. Therefore, the Logistic map over a finite field has a higher prospect of practical application and may be suitable for cryptographic application.

Acknowledgements This work was supported by National Key Research and Development Program of China (Grant No. 2016YFB0800601), and National Natural Science Foundation of China (Grant No. 61472331).

Supporting information Appendixes A–M. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Kocarev L, Lian S G. Chaos-Based Cryptography. Berlin: Springer, 2011
2 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
3 Lima J B, Novaes L F G. Image encryption based on the fractional Fourier transform over finite fields. Signal Process, 2014, 94: 521–530
4 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
5 Li C Q, Li S J, Lo K T. Breaking a modified substitution-diffusion image cipher based on chaotic standard and logistic maps. Commun Nonlinear Sci Numer Simul, 2011, 16: 837–843
6 Yoshida K, Miyazaki T, Uehara S, et al. Some properties of the maximum period on the Logistic map over Z_{2^n}. In: Proceedings of International Symposium on Information Theory and its Applications, Melbourne, 2014. 665–668
7 Yang B, Liao X F. Period analysis of the Logistic map for the finite field. Sci China Inf Sci, 2017, 60: 022302