Another Look at a Proposed Quartic Chaotic Mapping

Another Look at a Proposed Quartic Chaotic Mapping

Qi Wu

School of Information Technology, Jiangxi University of Finance & Economics, Nanchang, Jiangxi, 330032, China

wuqiocjzd@126.com

Abstract. In this paper, we take another look at a quartic chaotic mapping proposed before, in which two cases were left unconcerned. For these two cases, we could form a quartic mapping easily almost as same as we did before. Analysis illustrates that the mapping formed for the two cases demonstrates different chaotic properties: one with vast chaotic area, the other with broad periodic area. That is to say, they could be applied to anti-control of chaos and control of chaos, respectively. Both cases are quite efficient, and easy to use.

1. Introduction

Among chaotic systems, 1-dimensional discrete chaotic mappings (abbreviated as **1DDCM** hereafter) are of the easiest form and highest efficiency [1]. However, in terms of our experiments [2-9], classic 1DDCM, such as piecewise linear mapping (skew tent mapping in most cases), Logistic mapping, and Chebyshev mapping, are defective: The chaotic area of Logistic mapping is highly narrow and incontinuous, which makes it difficult to select strong parameters; Although skew tent mapping owns broad chaotic area, when applied to devising pseudorandom bit generators, its strong cipher space is confined in a small adjacent area of 0.5; Chebyshev mapping invokes cosine and arccosine functions once respectively during each iteration, which makes it inefficient, as cosine and arccosine functions are usually implemented by means of Taylor Expansion.

Nowadays, research on 1DDCM focuses on analysis, comparison and application of existing mappings [10-13], whereas novel ones are seldom proposed. Though 1DDCM owns too few parameters, is apt to reveal its phase trajectory, and had better not be put into use directly [14], we persist that design and analysis of novel 1DDCM are significant. On one hand, owing to its simple computation and lucid chaotic properties, 1DDCM is the best tutorial for beginners of chaos. On the other hand, thanks to its high efficiency, 1DDCM provides a sound base for high-dimensional mappings, for instance, coupling several 1-dimensional ones.

In the literature, many efforts have been made via making a 1DDCM piecewise [15-17]. Although this way could bring more parameters easily and enlarge the cipher space naturally, it dramatically decreases the efficiency. In terms of our experiments, skew tent mapping is much slower than Logistic mapping, due to its need for branch structure when implemented. In our opinion, another way for bringing more parameters is much more efficient, namely, degree raising.

In Ref. [18], a cubic chaotic mapping is constructed by us by means of raising the degree of Logistic mapping while keeping it a unimodal surjection. In Ref. [19], we continue our way of raising the degree so as to attain a quartic chaotic mapping. However, some cases in Ref. [19] are left unconcerned, to which will be paid attention in this paper.

The rest of this paper is organized as follows. Section 2 takes another look at a proposed quartic chaotic mapping, which is analyzed in detail in section 3. Section 4 concludes.

2. A quartic chaotic mapping revisited

Given (0, 0) and (1, 0), due to imaginary roots of equations with real coefficients always come out in pairs, the quartic equation must have another 2 real roots or another 2 imaginary roots. Either way, the quartic mapping could be written as:

$$\mathrm{f(x)} = \mathrm{cx(1-x)}(x^2 + \mathrm{ax} + \mathrm{b}) \tag{1}$$

in which Δ of $\mathrm{g(x)} = x^2 + \mathrm{ax} + \mathrm{b} = 0$ determines whether it has imaginary roots or not. Here, we only take into account the case when the equation has 4 real roots $0,1, d_1, d_2$.

To make the quartic mapping unimodal in the interval (0, 1), d_1 and/or d_2 shouldn't lie in (0, 1). Therefore, we have one of the following:

① $d_1 \in [1, +\infty)$ and $d_2 \in [1, +\infty)$;
② $d_1 \in (-\infty, 0]$ and $d_2 \in (-\infty, 0]$;
③ $d_1 \in [1, +\infty)$ and $d_2 \in (-\infty, 0]$;
④ $d_1 \in (-\infty, 0]$ and $d_2 \in [1, +\infty)$.

In Ref. [19], only ③ and ④ are taken into account. In this paper, we focus on ① and ②.

For ①, we have conditions $\begin{cases} \Delta \geq 0 \\ -\frac{a}{2} \geq 1 \\ g(1) \geq 0 \end{cases}$, namely,

$$\begin{cases} a \leq -2 \\ -a - 1 \leq b \leq \frac{a^2}{4}. \end{cases} \tag{2}$$

For ②, we have conditions $\begin{cases} \Delta \geq 0 \\ -\frac{a}{2} \leq 0 \\ g(0) \geq 0 \end{cases}$, namely,

$$\begin{cases} a \geq 0 \\ 0 \leq b \leq \frac{a^2}{4}. \end{cases} \tag{3}$$

Next, let's find what c should follow given a and b.

From equation (1), we could easily get

$$f^{'}(\mathrm{x}) = -4\mathrm{c}x^3 + 3(1-a)cx^2 + 2(a-b)cx + bc. \tag{4}$$

Let $f^{'}(x) = 0$, extract from the 3 roots the one locating in (0, 1), say x_3. (This step could be done in several ways, such as setting $\mathrm{r} = 0.75 * (\mathrm{a} - 1)$, $\mathrm{s} = \frac{b-a}{2}$, $\mathrm{t} = -\frac{b}{4}$, $\mathrm{p} = \frac{r^2-3s}{9}$, $\mathrm{q} = \frac{2r^3-9rs+27t}{54}$, $\mathrm{u} = \arccos(\frac{q}{p^{\frac{3}{2}}})$, then $x_3 = \begin{cases} -2\sqrt{p}cos\frac{u}{3} - \frac{r}{3}, & for ① \\ -2\sqrt{p}cos\frac{u+2\pi}{3} - \frac{r}{3}, for ② \end{cases}$.)

To make the quartic mapping a surjection in (0, 1), we have $\mathrm{f}(x_3) = 1$, which gives us

$$\mathrm{c} = \frac{1}{x_3(1-x_3)({x_3}^2+ax_3+b)}. \tag{5}$$

In a word, to form a quartic mapping f(.), we could select a and b at will as long as equation (2) or equation (3) is satisfied. After that, we should follow the aforementioned steps to get c. Then, a concrete quartic mapping $\mathrm{f(x)} = \mathrm{cx(1-x)}(x^2 + \mathrm{ax} + \mathrm{b})$ is obtained. To distinguish it from the one in Ref. [19], hereafter, the mapping is named as *quartic chaotic mapping 2*, sometimes abbreviated as **QCM2**.

3. Analysis of QCM2

Next, we depict the bifurcation graph of QCM2 (for ①).

Let $x_0 = 0.1$, a goes from -100 to -2 with step=1; For each a, b goes from $-\mathrm{a}-1$ to $\frac{a^2}{4}$ with step=0.1. For all the pairs of parameters, we iterate QCM2 500 times, filtering the first 200 times, the value of x for the last 300 times is depicted, as shown in figure 1.

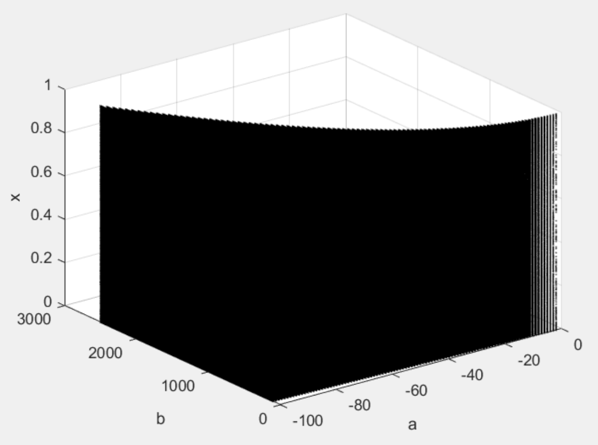

Figure 1. Bifurcation graph of QCM2 (for ①).

Clearly, for all the pairs of parameters, no periodic area could be seen.

Then, we depict the Lyapunov exponent graph of QCM2 (for ①).

Let $x_0 = 0.1$, a goes from -100 to -2 with step=1; For each a, b goes from $-\mathrm{a}-1$ to $\frac{a^2}{4}$ with step=0.1. For all the pairs of parameters, we iterate QCM2 1999 times, filtering the first 999 times, the Lyapunov exponent is computed from the last 1000 times, as shown in figure 2.

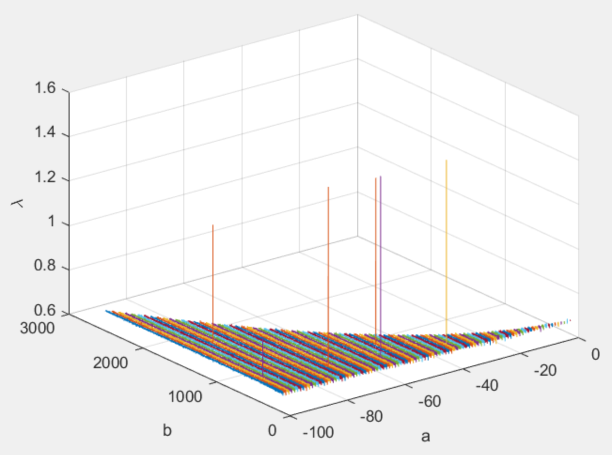

Figure 2. Lyapunov exponent graph of QCM2 (for ①).

Obviously, for all the pairs of paremeters, QCM2 (for ①) resides in chaotic area.

Next, we depict the bifurcation graph of QCM2 (for ②).

Let $x_0 = 0.1$, a goes from 0 to 99 with step=1; For each a, b goes from 0 to $\frac{a^2}{4}$ with step=0.1. For all the pairs of parameters, we iterate QCM2 500 times, filtering the first 200 times, the value of x for the last 300 times is depicted, as shown in figure 3.

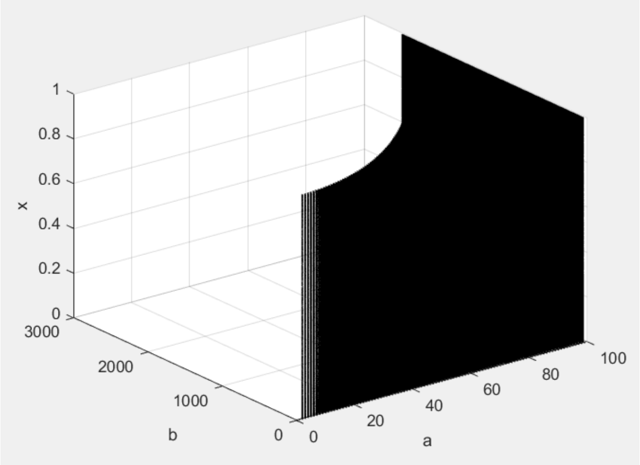

Figure 3. Bifurcation graph of QCM2 (for ②).

Apparently, for all the pairs of parameters, no periodic area could be seen.

Then, we depict the Lyapunov exponent graph of QCM2 (for ②).

Let $x_0 = 0.1$, a goes from 0 to 99 with step=1; For each a, b goes from 0 to $\frac{a^2}{4}$ with step=0.1. For all the pairs of parameters, we iterate QCM2 1999 times, filtering the first 999 times, the Lyapunov exponent is computed from the last 1000 times, as shown in figure 4.

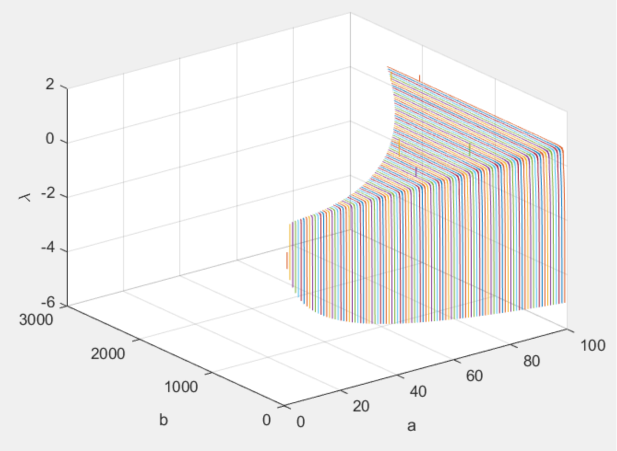

Figure 4. Lyapunov exponent graph of QCM2 (for ②).

Here, we get a large part of periodic area when a is small. When a increases, the chaotic area increases as well.

Therefore, QCM2 (for ①) is quite suitable for applications requiring anti-control of chaos, such as pseudorandom bit generator and cryptographic hash function. QCM2 (for ②) is very suitable for applications requiring control of chaos, such as synchronization of chaos.

The running time of QCM2 is approximately the same as QCM and we tend to omit it in this paper. But, we have to announce again here, the impact of degree raising on efficiency is negligible.

4. Conclusion

In this paper, we focus on a quartic chaotic mapping, in which two cases are left unconcerned in Ref. [19]. For either case, we could form a quartic mapping easily in a way almost as same as Ref. [19]. Analysis shows the mapping formed for the two cases possesses different chaotic properties: one with broad chaotic area, and the other with vast periodic area. Both cases are of high efficiency. In the future, we tend to apply these chaotic mappings to many fields, such as pseudorandom bit generator, cryptographic hash function, and synchronization of chaos.

Acknowledgments

This research is financially supported by the National Natural Science Foundation of China under Grant No. 61862028 & No.61762041, Natural Science Foundation of Jiangxi Province under Grant No. 20181BAB202016, the Science and Technology Project of Provincial Education Department of Jiangxi (GJJ160430), the Science and Technology Project of Provincial Education Department of Jiangxi for Youth (GJJ180288). Thanks to my supervisors Changxuan Wan & Zuowen Tan.

References

[1] Hao, B. (1993) Starting with Parabolas: an Introduction to Chaotic Dynamics. Shanghai Science and Technology Education Press, Shanghai.
[2] Tan, Z., Wu, Q. (2008) Study of Linearly Cross-Coupled Chaotic Systems for a Random Bit Generator. In: 2008 International Conference on Computational Intelligence and Security. Suzhou.
[3] Tan, Z., Wu, Q. (2008) Study of Exponentially Cross-Coupled Chaotic Systems for a Random Bit Generator. In: 2008 International Symposium on Intelligent Information Technology Application. Shanghai. pp. 224-227.
[4] Wu, Q., Tan, Z., Wan, C. (2011) A Harmonically Coupled Chaotic System for a Pseudo-Random Bit Generator. Journal of Chinese Computer Systems, 32: 639-643.
[5] Wu, Q. (2016) Independent Variable Exclusively Coupled Chaotic Pseudorandom Bit Generator. Computer Engineering & Science, 38: 2197-2201.
[6] Wu, Q. (2016) An Independent Variable Exclusively Coupled Chaotic System for a Pseudorandom Bit Generator. In: 2016 International Conference on Industrial Informatics – Computing Technology, Intelligent Technology, Industrial Information Integration. Wuhan. pp. 341-344.
[7] Wu, Q. (2018) A Dependent Variable Harmonically Coupled Chaotic System for a Pseudorandom Bit Generator. In: 2018 International Conference on Smart Materials, Intelligent Manufacturing and Automation. Hangzhou.
[8] Wu, Q. (2018) A Dependent Variable Exclusively Coupled Chaotic System for a Pseudorandom Bit Generator. In: 2018 International Conference on Network and Information Systems for Computers. Wuhan.
[9] Wu, Q. (2018) A Pseudorandom Bit Generator based on a Dependent Variable Exclusively Coupled Chaotic System. In: 2018 International Conference on Intelligent Information Processing. Guilin. pp. 11-16.
[10] Zhao, X. (2012) Research on Optimization Performance Comparison of Different One-Dimensional Chaotic Maps. Application Research of Computers, 29: 913-915.
[11] Liu, L., Song, H. (2014) Parameter Estimation of One-Dimensional Discrete Chaotic System based on Chaotic Synchronization. Electronic Design Engineering, 22: 123-125.
[12] Li, C., Li, Y., Zhao, L., et al. (2014) Research on Statistical Characteristics of Chaotic Pseudorandom Sequence for One-Dimensional Logistic Map. Application Research of Computers, 31: 1403-1406.
[13] Chen, W. (2015) The Iterations of a Class of Level Top Unimodal Mappings. Journal of Sichuan Normal University (Natural Science), 38: 391-397.
[14] Li, S., Mou, X., Cai, Y. (2001) Pseudo-Random Bit Generator based on Couple Chaotic Systems and its Applications in Stream-Cipher Cryptography. In: 2nd International Conference on Cryptology in India. Chennai. pp. 316-329.
[15] Guo, Z., Liu, D. (2015) Image Encryption and Compression Algorithm based on 2D Phased Linear Chaotic Map Coupling Chinese Remainder Theorem. Computer Applications and Software, 32: 288-291, 329.
[16] Cai, D., Ji, X., Shi, H., et al. (2016) Method for Improving Piecewise Logistic Chaotic Map and its Performance Analysis. Journal of Nanjing University (Natural Sciences), 52: 809-815.

[17] Xu, H., Li, Q., Ning, M., et al. (2016) Analysis of the Chaotic Boundary in a Class of Piecewise Nonlinear Mapping. Journal of Hainan Normal University (Natural Science), 29: 363-368, 383.

[18] Wu, Q. (2015) A Chaos-based Hash Function. In: 2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. Xi’an.

[19] Wu, Q. (2016) A Quartic Chaotic Mapping. In: 2016 International Conference on Computer Science and Information Security. Nanjing.