Construction and Chaos Properties Analysis of a Quadratic Polynomial Surjective Map

Jun Tang, Jianghong Shi, Zhenmiao Deng

Abstract**—**In this paper, a kind of quadratic polynomial surjective map (QPSM) is constructed, and the topological conjugation of the QPSM and tent map is proven. With the probability density function (PDF) of the QPSM being deduced, an anti-trigonometric transform function is proposed to homogenize the QPSM. The information entropy, Kolmogorov entropy (KE), and discrete entropy (DE) of the QPSM are calculated for both the original and homogenized maps with respect to different parameters. Simulation results show that the information entropy of the homogenized sequence is close to the theoretical limit and the discrete entropy remains unchanged, which suggest that the homogenization method is effective. Thus, the homogenized map not only inherits the diverse properties of the original QPSM but also possesses better uniformity. These features make it more suitable to secure communication and noise radar.

Keywords**—**chaotic map, entropy, topological conjugation, homogenization.

I. Introduction

CHAOS is seemingly random and irregular movement that occurs in a deterministic system without any random factors [1]–[3]. As a new science, chaology is usually thought to have begun with the publication of "Period three implies chaos" by Li and Yorke in 1975 [4], which is the first use of "chaos" as scientific terminology. As a complex dynamic phenomenon in a nonlinear system, chaos exists throughout nature. Because of its complex behaviour, chaos has attracted great interest from scholars in various fields [5]–[8].

Because of ergodicity and mixing [9], chaos can be characterized by methods of probability and statistics. That is, the probability density function (PDF) of a chaotic map can be used to analysis the properties of chaos. So far, however, only a few simple chaotic maps have known PDFs [10], [11]. Reference [12] demonstrated that the logistic map and Chebyshev map are topologically conjugate to the tent map and presented PDFs of the logistic and Chebyshev maps. Producing chaotic sequences with good uniformity and randomness is a very important subject [13–[15]. At present, there are many ways to transform chaotic sequences into uniformly and randomly distributed sequences [16]–[18].

In this paper, we deduce the relationships between the coefficients of a quadratic polynomial surjective map (QPSM) and prove the topological conjugacy of the QPSM and tent map. We give the PDF of the QPSM, which is then used to design a transform function to homogenize the QPSM sequence. Finally, we estimate entropies of the QPSM such as the information, Kolmogorov, and discrete entropies for both the original and homogenized map.

This paper is organized as follows. Section II presents a method for determining the QPSM coefficients, and the topological conjugation of the QPSM and tent map is proven. Section III gives the derivation for the PDF of the QPSM and presents a homogenization method. Section IV presents an analysis on the statistical and chaos characteristics of the QPSM and the results of some simulations. Finally, Section V concludes the paper.

II. The construction of the QPSM

A. The Relationships between the Coefficients of the QPSM

Reference [19] proposed an equivalent proposition for the determination of period-3 points of a real coefficient polynomial by decomposing it into a complex field and presented a necessary and sufficient condition of determining period-3 points of a quadratic polynomial.

Lemma 2.1 [19]: *The necessary and sufficient condition of determination 3-periodic points of a quadratic polynomial map* $f(x)=ax^2+bx+c, a\neq 0$ *is*

$$b^2-4ac-2b\geq 7 \tag{1}$$

If the quadratic polynomial is a surjective map, we can further conclude the following:

i. One of the fixed points x^* of f is the boundary of the map interval I;

ii. Let (x_c, y_c) be the vertex coordinate of f; then, $f(y_c)=x^*$ should hold.

Without loss of generality, if we suppose $a<0$, then we can obtain the following equation according to the above conditions:

The research was supported in part by the National Natural Science Foundation of China under Grant 61471012, in part by the Open-End Fund of BITTT Key Laboratory of Space Object Measurement.

Jun Tang is with the School of Information Science and engineering, Xiamen University, Xiamen, China (corresponding author to provide e-mail: jtang@xmut.edu.cn).

Jianghong Shi is with the School of Information Science and engineering, Xiamen University, Xiamen, China (e-mail: shijh@xmu.edu.cn).

Zhenmiao Deng is with the School of Information Science and engineering, Xiamen University, Xiamen, China (e-mail: dzm_ddb@xmu.edu.cn).

$$\begin{cases} x^* = f\left(x^*\right) \\ f\left(\left(4ac-b^2\right)/4a\right) = x^* \end{cases} \tag{2}$$

By solving the above equation, we can get one fixed point $x^* = \left(\sqrt{b^2-4ac-2b+1}-b+1\right)/2a$ and $c = \left(b^2-2b-8\right)/4a$. In this case of $b^2-4ac-2b \equiv 8$, the condition of lemma 2.1 is met. Therefore, the QPSM is chaotic, and its map interval is $I = \left[(4-b)/2a, -(4+b)/2a\right]$. Thus, the QPSM can be expressed as

$$f(x) = ax^2+bx+c(a,b),\ x \in \left[\frac{4-b}{2a}, \frac{-4-b}{2a}\right] \tag{3}$$

where $c(a,b) = \left(b^2-2b-8\right)/4a$.

B. Topological Conjugation of the QPSM

In order to prove that Eq. (3) is topologically conjugate to the tent map, we first introduce the definition of a topological conjugation.

Definition 2.2 [20] (Topological Conjugation): Two maps $f: I \to I$ and $g: J \to J$ are topological conjugate if there exists a homeomorphism $h: I \to J$ such that

$$h \circ f = g \circ h \tag{4}$$

Lemma 2.3: *The QPSM $f(x) = ax^2+bx+c(a,b)$ is topologically conjugate to the tent map.*

Proof: The tent map is given by

$$g(x) = \begin{cases} 2x, & 0 \le x \le \frac{1}{2} \\ 2-2x, & \frac{1}{2} \le x \le 1 \end{cases} \tag{5}$$

Let $h(x) = k_1\cos(\pi x)+k_2,\ x \in [0,1]$. Obviously, $h(x)$ is a continuous and reversible function.

According to definition 2.2,

$$\begin{aligned} h\left(g(x)\right) &= \begin{cases} k_1\cos(2\pi x)+k_2, & 0 \le x \le \frac{1}{2} \\ k_1\cos(2\pi-2\pi x)+k_2, & \frac{1}{2} \le x \le 1 \end{cases} \\ &= k_1\cos(2\pi x)+k_2 \\ &= h(2x) \end{aligned} \tag{6}$$

On the other hand,

$$\begin{aligned} f\left(h(x)\right) &= ah^2(x)+bh(x)+c(a,b) \\ &= a\left[k_1\cos(\pi x)+k_2\right]^2 \\ &\quad +b\left[k_1\cos(\pi x)+k_2\right]+c(a,b) \\ &= a\left[k_1^2\cos^2(\pi x)+k_2^2+2k_1k_2\cos(\pi x)\right] \\ &\quad +bk_1\cos(\pi x)+bk_2+c(a,b) \\ &= a\left[k_1^2\frac{\cos(2\pi x)+1}{2}+k_2^2+2k_1k_2\cos(\pi x)\right]+ \\ &\quad bk_1\cos(\pi x)+bk_2+c(a,b) \end{aligned} \tag{7}$$

If we let $f\left(h(x)\right) = h(2x)$, we get

$$\begin{cases} k_1 = \dfrac{2}{a} \\ k_2 = -\dfrac{b}{2a} \end{cases}$$

In other words, when $h(x) = 2\cos(\pi x)/a - b/(2a),\ x \in [0,1]$, $h\left(g(x)\right) = f\left(h(x)\right)$. Therefore, $f(x)$ and $g(x)$ are topological conjugacy via $h(x)$.

III. PDF and Homogenization of the QPSM

A. PDF of the QPSM

Lemma 3.1 [21]: *If the maps $f(x)$ and $g(x)$ are topological conjugate via $h(x)$ and $\rho_g(x)$ is the PDF of $g(x)$, then the PDF of $f(x)$ is*

$$\rho_f(x) = \rho_g\left(h^{-1}(x)\right)\left|\frac{dh^{-1}(x)}{dx}\right|$$

Theorem 3.2: *The PDF of $f(x) = ax^2+bx+c(a,b)$ is*

$$\frac{|a|}{\pi}\frac{16}{\sqrt{-4a^2x^2-4abx-b^2+16}}$$

Proof: The PDF of the tent map is

$$\rho_T(x) = 1,\ x \in (0,1)$$

According to Lemma 3.1, we can obtain

$$h^{-1}(x) = \frac{1}{\pi}\arccos\left[\frac{a}{2}x+\frac{b}{4}\right]$$

and

$$\begin{aligned} \rho_f(x) &= \rho_T\left(h^{-1}(x)\right)\left|\frac{dh^{-1}(x)}{dx}\right| \\ &= 1 \times \left|\frac{d\left(\frac{1}{\pi}\arccos\left(\frac{a}{2}x+\frac{b}{4}\right)\right)}{dx}\right| \\ &= \frac{|a|}{\pi}\frac{16}{\sqrt{-4a^2x^2-4abx-b^2+16}} \end{aligned}$$

Therefore, $16|a|/\left(\pi\sqrt{-4a^2x^2-4abx-b^2+16}\right)$ is the PDF of $f(x) = ax^2+bx+c(a,b)$. Obviously, the distribution of the sequence produced by Eq. (3) is non-uniform.

B. Homogenization of the QPSM

Theorem 3.3: *If the PDF of a random variable X is*

$$\rho_X(x)=\begin{cases}\frac{-a}{\pi}\frac{16}{\sqrt{-4a^2x^2-4abx-b^2+16}}, \\ \frac{4-b}{2a}\le x\le\frac{-4-b}{2a} \\ 0, \text{otherwise}\end{cases}$$

then the random variable

$$Z=\frac{1}{\pi}\arcsin\left(-\frac{a}{2}X-\frac{b}{4}\right) \quad (8)$$

follows a uniform distribution in the interval $[-0.5,0.5]$.

Proof: The PDF of the random variable Z is

$$\begin{aligned}F_Z(z)&=P(Z\le z)\\&=P\left(\frac{1}{\pi}\arcsin\left(-\frac{a}{2}X-\frac{b}{4}\right)\le z\right)\\&=P\left(-\frac{a}{2}X-\frac{b}{4}\le\sin(\pi z)\right) \quad (9)\\&=P\left(X\le-\frac{2}{a}\sin(\pi z)-\frac{b}{2a}\right)\\&=\int_{-\infty}^{-\frac{2}{a}\sin(\pi z)-\frac{b}{2a}}\rho_X(x)dx\end{aligned}$$

If the derivation operation is applied to both sides of Eq. (9), then we can get the PDF of Z :

$$\rho_Z(z)=\begin{cases}\frac{32}{\pi}\frac{\cos(\pi z)}{\sqrt{-4a^2\left(-\frac{2}{a}\sin(\pi z)-\frac{b}{2a}\right)^2-4ab\left(-\frac{2}{a}\sin(\pi z)-\frac{b}{2a}\right)-b^2+16}}, \\ \frac{4-b}{2a}\le-\frac{2}{a}\sin(\pi z)-\frac{b}{2a}\le\frac{-4-b}{2a} \\ 0,\ \text{otherwise}\end{cases}$$

$$=\begin{cases}\sqrt{\cos^2(\pi z)}\sec(\pi z), -1\le\sin(\pi z)\le1 \\ 0, \text{otherwise}\end{cases}$$

$$=\begin{cases}1, -\frac{1}{2}\le z\le\frac{1}{2} \\ 0, \text{otherwise}\end{cases}$$

Therefore, the random variable $Z=\frac{1}{\pi}\arcsin\left(-\frac{a}{2}x-\frac{b}{4}\right)$ is uniformly distributed in $[-0.5,0.5]$.

IV. THE CHAOTIC CHARACTERISTICS OF THE QPSM

In this section, we analyse the statistical properties and entropy of the QPSM from the perspectives of the statistical histogram, information entropy, and discrete entropy. First, several definitions of entropy are introduced.

A. Definitions of Entropy

Definition 4.1 (Information Entropy): Let $S=\{s_1,s_2,\cdots,s_n\}$ be an information source and p_i be the probability of s_i showing up in S. The information entropy of S is then defined as

$$H(S)=-\sum_{i=1}^{n}p_i\log p_i$$

When $p_i=1/n$ for all $i\in\{1,\cdots,n\}$, $H(S)$ achieves the maximum $\log_2 n$. In other words, the maximum entropy probability distribution is the uniform distribution.

Definition 4.2 [22] (Kolmogorov Entropy). Consider the trajectory $X(t)=[x_1(t),\cdots,x_d(t)]$ of a dynamical system on a strange attractor and suppose that the d -dimensional phase space is partitioned into boxes of size l_d. The state of the system is now measured at intervals of time τ. Let $P_{i_0\cdots i_n}$ be the joint probability that $X(t=0)$ is in box i_0, $X(t=\tau)$ be the joint probability that it is in box $i_1,\cdots,$, and $X(t+n\tau)$ be the joint probability that it is in box i_n. The K -entropy is defined as

$$K=-\lim_{\tau\to0}\lim_{l\to0}\lim_{N\to\infty}\frac{1}{N\tau}\sum_{i_0\cdots,i_{N-1}}P_{i_0\cdots i_{N-1}}\log P_{i_0\cdots i_{N-1}}$$

For one-dimensional maps, K is simply the positive Lyapunov exponent.

Definition 4 [23] (Discrete Entropy): Let $A=\{a_1,\cdots,a_L\}$ be a finite set endowed with a linear ordering $\le$, $F:A\to A$ be a bijection, and $\pi\in S_n$ be a permutation on $\{0,1,\cdots,n-1\}$ with $2\le n\le L$. The following is defined:

$$Q_\pi(n)=\left\{a\in A:F^{\pi_0}(a)<\cdots<F^{\pi_{n-1}}(a)\right\}$$

and

$$q_\pi(n)=\frac{|Q_\pi(n)|}{\sum_{\tau\in S_n}|Q_\tau(n)|}$$

Then, the discrete entropy of F with the order $n\ge2$ is defined as

$$h_\delta^{(n)}(F)=-\frac{1}{n-1}\sum_{\pi\in S_n}q_\pi\log q_\pi \quad (10)$$

The best way to encapsulate the information contained in $h_\delta^{(2)}(F),\ldots,h_\delta^{(n_{\max})}(F),n_{\max}=\max\left\{n:h_\delta^{(n)}(F)\ne0\right\}$ into a single number is by taking its arithmetic mean. We call

$$h_\delta(F)=\frac{1}{n_{\max}-1}\sum_{n=2}^{n_{\max}}h^{(n)}(F) \quad (11)$$

the discrete entropy of F.

B. Bifurcation Diagrams and Statistical Properties of a Quadratic Polynomial Map

Based on Eq. (12), suppose that $a=-1.8,b=2.8$. Then, $c=0.8$, and we can obtain a specific quadratic polynomial map:

$$f(x) = ax^2 + bx + c = -1.8x^2 + 2.8x + 0.8,\ x \in \left[-\frac{1}{3}, \frac{17}{9}\right] \tag{13}$$

This map evolves chaotic motions through period-doubling bifurcation while the system parameters vary. Figs 1(a)–(c) show the bifurcation diagrams.

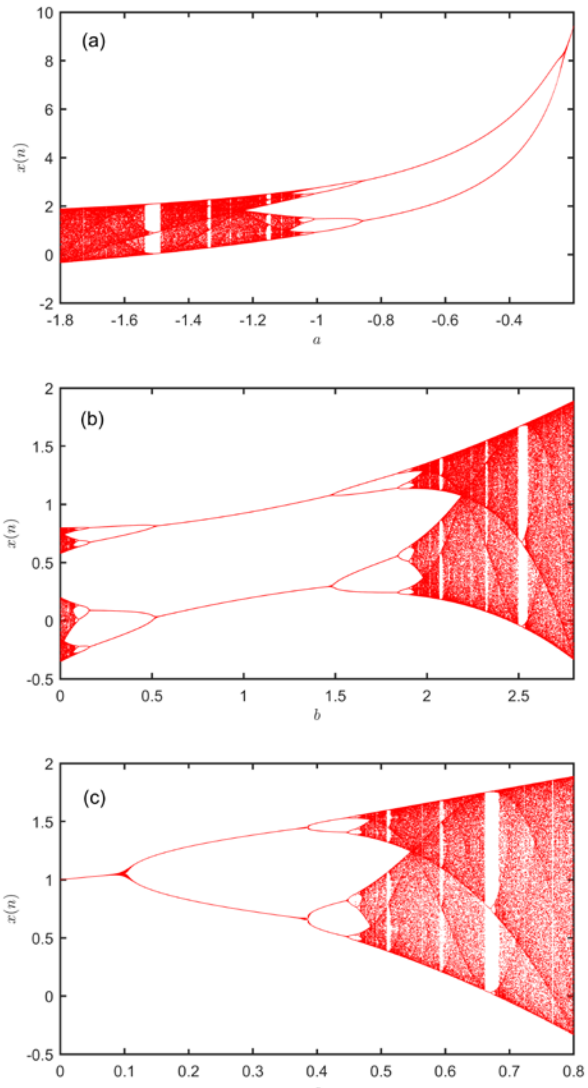


Fig. 1 bifurcation diagrams: (a) the bifurcation diagram of parameter a in system (12); (b) the bifurcation diagram of parameter b in system (12); (c) the bifurcation diagram of parameter c in system (12)

C. Statistical Histograms of the QPSM

The histograms of the sequences generated by both the original and homogenized maps are shown in Fig. 2 (a) and (b), respectively. The distribution of the homogenized chaotic sequence can clearly be observed to be approximately uniform.

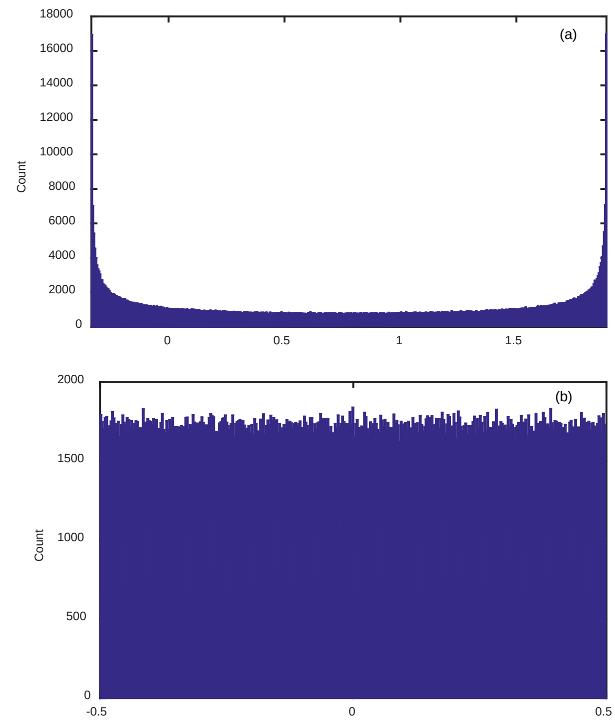


Fig. 2 histogram: (a) histogram of the sequence before uniformity; (b) histogram of the sequence after uniformity.

D. Entropy of the QPSM

In order to calculate the information entropy of an ergodic sequence with the length of N, we can divide the range of values into M equal intervals and count the number of samples that fall into each interval. This is denoted as $n_i\left(i = 1, 2, \cdots, M\right)$. Therefore, the probability of each interval can be considered as $p_i = n_i / N, \sum_{i=1}^{M} p_i = 1$. According to the maximum information entropy principle, the maximum information entropy is $\log_2 M$. Here, we let $N = 600000$ and calculate the information entropy of the original and homogenized sequences for the different M values. Table 1 lists the results.

Table. 1 Information and maximum entropies before and after uniformity

(N,M)	Before uniformity	After uniformity	Maximum information
(600000,100)	6.3508	6.6438	6.6439
(600000,200)	7.3342	7.6437	7.6439
(600000,300)	7.9124	8.2285	8.2288
(600000,600)	8.6412	8.9652	8.9658

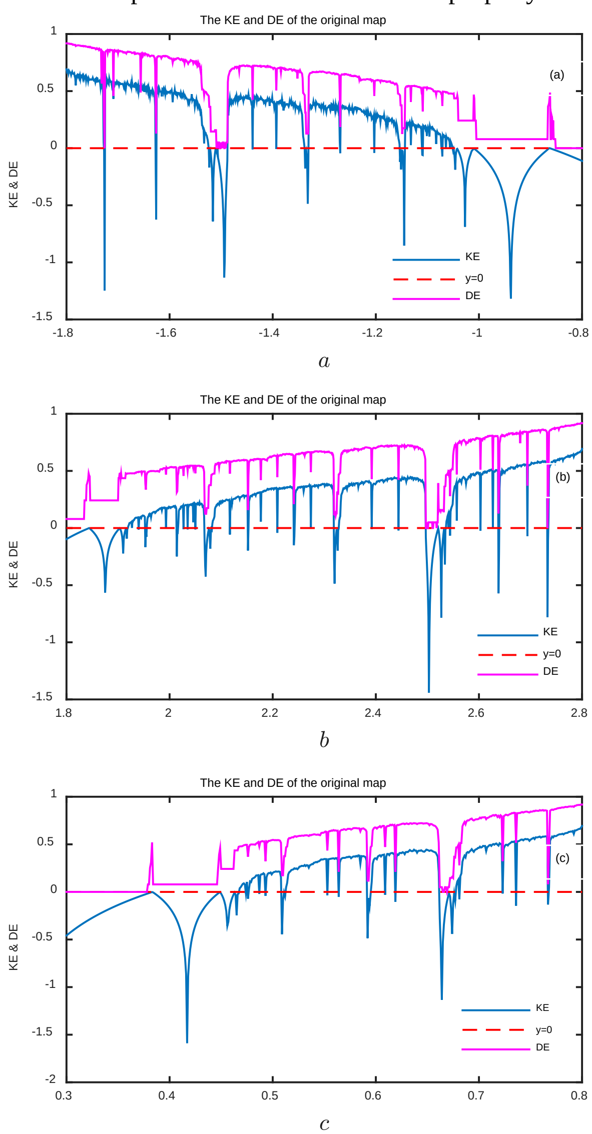
For all M values, the information entropy of the homogenized sequence is close to the maximum entropy $\log_2 M$, which suggests that the homogenization method is effective.

The concept of discrete entropy proposed by Kocarev in 2007 is used to measure the chaotic extent of a sequence by considering the permutations of successive $n\left(n \geq 2\right)$ points. In this paper, we let $n = 9$. Then, we can calculate the discrete entropies of the original and homogenized sequences with respect to the different coefficients, and compare then with the K entropy.

Let $a \in [-1.8, 0]$. The homogenized system can be written as

$$\begin{cases} x(n+1) = ax^2(x) + 2.8x(n) + 0.8 \\ z(n+1) = \dfrac{1}{\pi}\arcsin\left(-\dfrac{a}{2}x(n) - \dfrac{b}{4}\right) \end{cases} \tag{14}$$

The K entropies (i.e. positive Lyapunov exponent) and discrete entropies of the original and homogenized sequences are shown in Figs 3(a) and 3(d). Similarly, let $b \in [1.8, 2.8], c \in [0, 0.8]$. Fig. 3 shows the simulation results. As shown in Figs 3(a), (b), and (c), the discrete entropy of the original sequences approximated the K entropy with a constant offset. To some extent, the discrete entropy can be used to measure the chaotic extent of a system. As shown in Figs 3(d), (e), and (f), the discrete entropies of the original and homogenized systems are identical. The simulation results show that the uniformity of the distribution of the homogenized system was improved with the same chaotic property.



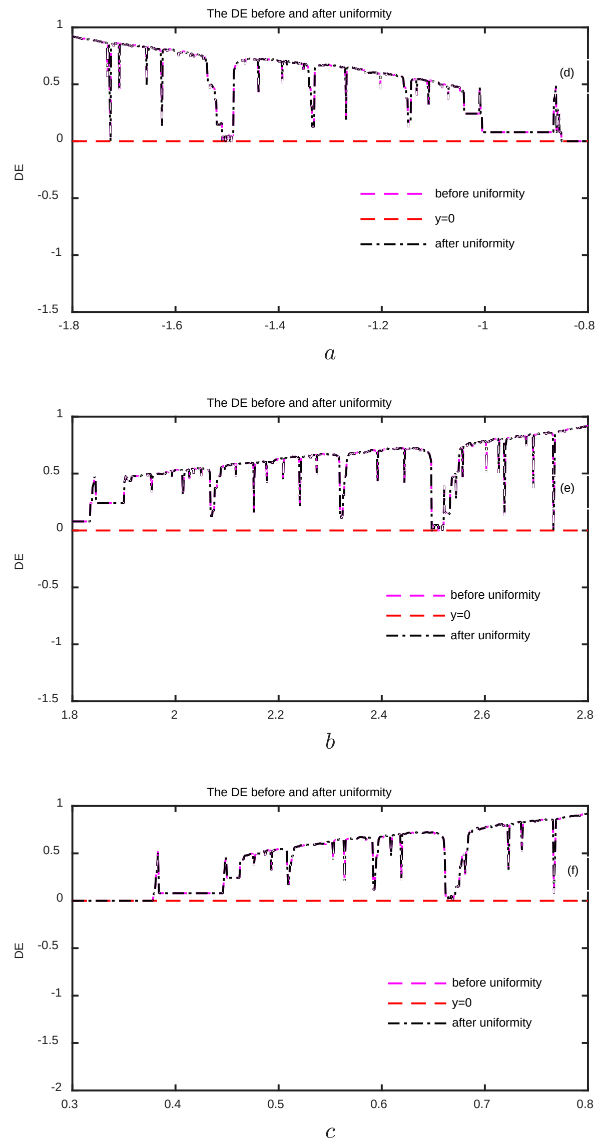


Fig. 3(a), (b), (c) K entropy and discrete entropy before uniformity; (d), (e), (f) discrete entropy of the before and after uniformity

V. CONCLUSION

In this paper, we propose a method for determining the coefficients of the QPSM and prove that the QPSM is topologically conjugate to the tent map. We then derive an analytical expression of the PDF of the QPSM and present an approach to homogenize the QPSM. The information entropy, K entropy, and discrete entropy of the QPSM were analysed and simulated. The theoretical results showed that the information entropy was highest for the sequence generated by the homogenized system, and the discrete entropy remained the same. The simulation results show that the discrete entropy is similar to the K entropy with a constant offset. In other words, homogenization improves the information entropy of the QPSM while maintaining the chaos properties unchanged.

The construction and optimization methods of chaotic system proposed in this paper can be used to generate noise-like sequences, which can be applied to communication and radar aeras.

REFERENCES

[1] A. L. Goldberger, "Non-linear dynamics for clinicians: chaos theory, fractals, and complexity at the bedside," *Lancet*, vol. 347, pp. 1312-1314, 1996.K. Aihara, "Chaos and Its Applications," *Procedia Iutam*, vol. 5, pp. 199–203, 2012.

[2] R. C. Hilborn, S. Coppersmith, A. J. Mallinckrodt, and S. Mckay, "Chaos and Nonlinear Dynamics: An Introduction for Scientists and Engineers," *The Quarterly Review of Biology*, vol. 62, pp. 235-235, 1995.

[3] E. Ott, "Chaos in Dynamical Systems - 2nd Edition," *Cambridge University Press*, 2002.

[4] T. Y. Li and J. A. Yorke, "Period Three Implies Chaos," *American Mathematical Monthly*, vol. 82, pp. 985-992, 1975.

[5] Q. Gan, S. Yu, C. Li, J. Lü, Z. Lin, and P. Chen, "Design and ARM‐embedded implementation of a chaotic map-based multicast scheme for multiuser speech wireless communication," *International Journal of Circuit Theory & Applications*, 2016..

[6] J. X. Chen, Z. L. Zhu, C. Fu, and H. Yu, "Optical image encryption scheme using 3-D chaotic map based joint image scrambling and random encoding in gyrator domains," *Optics Communications*, vol. 341, pp. 263-270, 2015.

[7] Flores, Benjamin C., and G. Thomas. "Chaotic signals for wideband radar imaging." Proceedings of SPIE - The International Society for Optical Engineering 4727(2002):100-111.

[8] N. Sircar, J. Sonnenschein, and W. Tangarife, "Extending the scope of holographic mutual information and chaotic behavior," *Journal of High Energy Physics*, vol. 2016, pp. 1-33, 2016.

[9] J. P. Eckmann and D. Ruelle, "Ergodic theory of chaos and strange attractors," *Review of Modern Physics*, vol. 57, pp. 1115-1115, 1985.

[10] L. Billings and E. M. Bollt, "Probability density functions of some skew tent maps," *Chaos Solitons & Fractals*, vol. 12, pp. 365-376, 2001.

[11] H. O. Peitgen, H. Jürgens, and D. Saupe, *Chaos and Fractals: New Frontiers of Science*: Springer-Verlag, 2004.

[12] Z. He, "CHAOTIC MAP BINARY SEQUENCES WITH GOOD SECURITY," *Journal of Electronics & Information Technology*, vol. 21, pp. 641-651, 1999.

[13] L. I. Pei-Yue, J. X. Shi, J. L. Guo, X. Chen, and H. J. Yang, "Improvement of a Universal Algorithm for Uniformization of Chaotic Pseudo-Random Sequences," *Acta Electronica Sinica*, vol. 43, pp. 753-759, 2015.

[14] Z. G. Xu, Q. Tian, and L. Tian, "Theorem to Generate Independently and Uniformly Distributed Chaotic Key Stream via Topologically Conjugated Maps of Tent Map," *Mathematical Problems in Engineering*, vol. 2012, pp. 1695-1698, 2012.

[15] Z. Xu, "An Image Encryption Method Based on Independently and Uniformly Distributed Chaotic Key Stream," *Journal of Information & Computational Science*, vol. 10, pp. 5971-5980, 2013.

[16] P. Li, Z. Li, W. A. Halang, and G. Chen, "A multiple pseudorandom-bit generator based on a spatiotemporal chaotic map," *Physics Letters A*, vol. 349, pp. 467-473, 2006.

[17] N. S. Liu, "Pseudo-randomness and complexity of binary sequences generated by the chaotic system," *Communications in Nonlinear Science & Numerical Simulation*, vol. 16, pp. 761-768, 2011.

[18] M. François, T. Grosges, D. Barchiesi, and R. Erra, "Pseudo-random number generator based on mixing of three chaotic maps," *Communications in Nonlinear Science & Numerical Simulation*, vol. 19, pp. 887-895, 2014.

[19] H. L. Zhou and E. B. Song, "Discrimination of the 3-periodic points of a quadratic polynomial," *Journal of Sichuan University*, vol. 46, pp. 561-564, 2009.

[20] A. Lasota and M. C. Mackey, "Chaos, Fractals, and Noise," *Applied Mathematical Sciences*, 1994.

[21] B.-L. Hao, "Starting with parabolas: an introduction to chaotic dynamics," *Shanghai Scientific and Technological Education Publishing House*, pp. 10-12, 1993.

[22] P. L. Knight, "Deterministic Chaos: An Introduction," *Journal of Modern Optics*, vol. 35, pp. 1114-1114(1), 1988.

[23] J. M. Amigó, L. Kocarev, and I. Tomovski, "Discrete entropy," *Physica D Nonlinear Phenomena*, vol. 228, pp. 77-85, 2007.

Jun Tang received the B.S and M.S. degree in communication and information system form Lanzhou University of Technology and Xidian University, China, in 2000 and 2007 respectively. He is now pursuing Ph.D. degree in communication and information in Xiamen University. He has been in Xiamen University of Technology since 2007 and is currently an assistant professor with the School of Photoelectricity and Communication Engineering. His research interests include chaotic signal processing, radar signal processing and multimedia signal processing.

Jianghong Shi received the Ph.D. degree from Xiamen University, China, in 2002. He is currently a professor in the School of Information Science and Technology, Xiamen University. He is also the director of the West Straits Communications Engineering Center, Fujian, China. His research interests include wireless communication networks and satellite navigation.

Zhenmiao Deng received the B.S. degree in electronic engineering from the Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing, China, in 1999, and the Ph.D. degree in signal and information processing from the NUAA, Nanjing, China, in 2007. From 2007 to 2009, he was a post-doctor research fellow in the College of Automation Engineering, NUAA, Nanjing, China, working in the field of signal detection and parameter estimation. In 2010, he joined the College of Information Science and Technology, Xiamen University, where he is now a professor. His current research interests include signal detection, parameter estimation, array signal processing, multirate signal processing.