一类三次多项式混沌映射的判定及性能分析

臧鸿雁* 韦心元 袁 悦
(北京科技大学数理学院 北京 100083)

摘 要：该文给出了一般3次多项式映射与分段线性混沌映射拓扑共轭的充分条件，从而间接地给出了一般3次多项式成为混沌系统的充分条件。进一步对拓扑共轭的分段线性映射和多项式映射的均匀性、结构复杂性和随机性进行了分析，结果显示分段线性映射的均匀性优于多项式映射，多项式映射的随机性优于分段线性映射，在结构复杂性方面，二者没有显著差异，但量化方法对二者的结构复杂性影响显著。

关键词：混沌系统；多项式映射；拓扑共轭；复杂性；随机性
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2021)02-0454-07
DOI: 10.11999/JEIT190875

Determination and Properties Analysis of a Cubic Polynomial Chaotic Map

ZANG Hongyan WEI Xinyuan YUAN Yue
(*Mathematics and Physics School, University of Science and Technology Beijing, Beijing* 100083, *China*)

Abstract: This paper provides the sufficient conditions for topological conjugation between the general cubic polynomial maps and a piecewise linear chaotic map, then provides indirectly the sufficient conditions that make the cubic polynomial maps be chaotic. This paper analyzes further the uniformity, structural complexity and randomness of the piecewise linear map and cubic polynomial maps of topological conjugation. The results show that the uniformity of the piecewise linear map is better than the polynomial maps while the randomness of the polynomial maps is superior to the piecewise linear map. As for the structural complexity, there is no significant difference between the two kinds of systems, but it should be noted that the quantitative method makes a significant impact on the structure complexity of the systems.

Key words: Chaotic system; Polynomial maps; Topological conjugation; Complexity; Randomness

1 引言

混沌作为一门新兴的学科，一直是学者的重要研究对象。1975年，数学家李天岩和其导师约克(Yorke)建立了“周期三意味着混沌”的判别定理(Li-Yorke混沌判别定理)[1]，为研究1维离散混沌系统提供了理论依据[2]。

由于混沌系统具有初值敏感性、遍历性、类随机性等诸多基本特性，混沌系统和密码学之间存在许多相似之处，这也促使不少学者致力于研究基于混沌的密码算法[3,4]。目前，基于混沌系统生成统计性能良好的混沌伪随机数已经是混沌密码学中的热门研究之一。其中，伪随机序列的均匀性[5]、随机性[6]、复杂度[7]等性能是衡量序列优劣的重要指标。

众所周知，除了Tent映射具有好的均匀性外，其他大部分映射的均匀性并不理想[8]。而2次多项式映射和Tent映射在某些条件下是拓扑共轭的，文献[9]给出了一般2次多项式在满足$b^2-4ac-2b=8$的条件下与Tent映射拓扑共轭的结论。针对这类2次多项式映射，在保证其与Tent映射拓扑共轭的前提下，只要找到二者之间的桥函数，就能获得2次多项式混沌系统的概率密度函数，从而利用一个变换，将不均匀的混沌序列变为均匀的混沌序列[10]，或者依赖2次多项式混沌系统概率密度函数的形式，获取使得混沌系统产生的值以等概率落入不等分区间的区间分点表达式，从而设计出产生独立同分布的混沌密钥流的量化方法[11,12]。可见，利用2次多项式映射和Tent映射的拓扑共轭关系，学者已经取得了丰硕的研究成果。

然而，除了Chebyshev映射外，关于3次多项式映射拓扑共轭的研究却鲜有报道[13,14]。本文首先

收稿日期：2019-11-04；改回日期：2020-03-12；网络出版：2020-12-11
*通信作者： 臧鸿雁 zhylixiang@126.com
基金项目：中央高校基本科研业务费专项资金(06108236)
Foundation Item: The Fundamental Research Funds for the Central Universities of Ministry of Education of China (06108236)

引入一个具有均匀分布特性的分段线性混沌映射，给出了这个映射与一般3次多项式映射拓扑共轭的充分条件。并进一步对分段线性映射和多项式映射的均匀性、结构复杂性、随机性进行了对比分析。

2　多项式混沌映射

首先，介绍Li-Yorke混沌判别定理，该定理的表述如下。

引理1[1]　设J是一个闭区间，且设$f:J\to J$是连续的，假设存在一点$a\in J$，使得$b=f(a)$，$c=f(b)$，$d=f(c)$满足$d\le a<b<c$（或$d\ge a>b>c$），则f是Li-Yorke意义下的混沌映射。

2.1　分段线性混沌映射

文献[9–12]中，在研究2次多项式映射和Tent映射的拓扑共轭关系时，所用的Tent映射及其分布密度表达式为

$$T_2(x)=\begin{cases}2x, & 0\le x\le 0.5\\ 2(1-x), & 0.5<x\le 1\end{cases},\ \rho_{T_2}(x)=1, x\in[0,1] \tag{1}$$

为研究3次多项式映射的混沌判定，本文首先引入式(2)所示的分段线性映射T_3。容易验证，映射T_3满足引理1，即T_3是Li-Yorke意义的混沌映射。

$$T_3(x)=\begin{cases}3x, & 0\le x\le 0.5\\ 3(1-x), & 0.5<x\le 1\\ 3(x-1), & 1<x\le 1.5\end{cases} \tag{2}$$

图1(a)和图1(b)分别为映射T_3的函数图像和样本概率密度拟合图。其Lyapunov指数为$\lambda=\ln 3$。与Tent映射类似，映射T_3服从$[0,3/2]$上的均匀分布。

2.2　3次多项式映射的混沌判

为了研究3次多项式系统与映射T_3的拓扑共轭关系，先给出拓扑共轭定义。

定义1[15]　设$f:X\to X$和$g:Y\to Y$是两个映射，若存在同胚$h:X\to Y$，满足$h\circ f=g\circ h$，则称f和g关于h拓扑共轭。

映射T_3和3次多项式的拓扑共轭关系由以下定理描述。

定理1　对于一般3次多项式$f(x)=ax^3+bx^2+cx+d$和映射T_3。若满足条件

$$\left.\begin{aligned}&a>0\\ &3ac-b^2+9a=0\\ &2b^3+9ab(1-c)+27a^2d=0\end{aligned}\right\} \tag{3}$$

则f和T_3关于同胚$h(x)=\dfrac{2}{\sqrt{a}}\cos(2\pi x/3)-\dfrac{b}{3a}$，$x\in[0,3/2]$拓扑共轭，从而$f$在Li-Yorke意义下是混沌的。

证明　记$m=\dfrac{2\pi}{3}$，令$h(x)=\dfrac{2}{\sqrt{a}}\cos(mx)-\dfrac{b}{3a}$$(a>0)$，且

$$\begin{aligned}h\circ T_3&=h(3x)=\frac{2}{\sqrt{a}}\cos(3mx)-\frac{b}{3a}\\ &=\frac{8}{\sqrt{a}}\cos^3(mx)-\frac{6}{\sqrt{a}}\cos(mx)-\frac{b}{3a},\end{aligned}$$

$$\begin{aligned}f\circ h=&\frac{8}{\sqrt{a}}\cos^3(mx)+\frac{2(3ac-b^2)}{3a^{3/2}}\cos(mx)\\ &+\frac{2b^3-9abc+27a^2d}{27a^2}.\end{aligned}$$

若$h\circ T_3=f\circ h$，则有

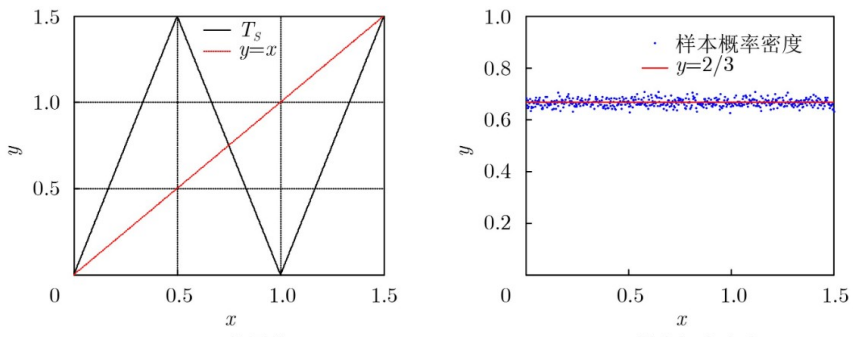
$$\left.\begin{aligned}&-\frac{6}{\sqrt{a}}=\frac{2(3ac-b^2)}{3a^{3/2}}\\ &-\frac{b}{3a}=\frac{2b^3-9abc+27a^2d}{27a^2}\end{aligned}\right\}$$
$$\Leftrightarrow\ \left.\begin{aligned}&3ac-b^2+9a=0\\ &2b^3+9ab(1-c)+27a^2d=0\end{aligned}\right\} \tag{4}$$

证毕

定理1给出了一般3次多项式映射和映射T_3拓扑共轭的充分条件。因此，当条件式(3)成立时，3次多项式在Li-Yorke意义下是混沌的。容易验证，众所周知的3阶Chebyshev多项式映射$f(x)=4x^3-3x$满足本文定理1所提出的条件式(3)，也就是说，3阶Chebyshev多项式映射属于定理1所描述的这类混沌系统。

2.3　3次多项式映射的概率密度

由3次多项式映射与映射T_3的拓扑共轭关系，



(a) 函数图像　　(b) 样本概率密度

图 1 映射T_3拟合图

容易得到3次多项式映射的概率密度函数，见定理2。下面，先给出以下引理2。

引理2[15] 如果映射f, g和h满足$h\circ g=f\circ h$，即f和g关于h拓扑共轭，且$\rho_g(x)$是映射g的概率密度函数，则映射f的概率密度函数为

$$\rho_f(x)=\rho_g\left(h^{-1}(x)\right)\left|\frac{\mathrm{d}h^{-1}(x)}{\mathrm{d}x}\right| \tag{5}$$

定理2 对于一般3次多项式$f(x)=ax^3+bx^2+cx+d$，若满足条件式(3)，则f的概率密度为

$$\rho_f(x)=\begin{cases}\dfrac{\sqrt{a}}{\pi\sqrt{4-a\left(x+\dfrac{b}{3a}\right)^2}}, \\ \qquad x\in\left[-\dfrac{2}{\sqrt{a}}-\dfrac{b}{3a},\dfrac{2}{\sqrt{a}}-\dfrac{b}{3a}\right] \\ 0, \quad \text{其他}\end{cases} \tag{6}$$

证明 T_3服从$[0,3/2]$上的均匀分布，其概率密度为

$$\rho_{T_3}(x)=2/3, x\in[0,3/2] \tag{7}$$

由定理1可知，f和T_3关于h拓扑共轭，且

$$h^{-1}(x)=\frac{3}{2\pi}\arccos\left[\frac{\sqrt{a}}{2}\left(x+\frac{b}{3a}\right)\right], \quad x\in\left[-\frac{2}{\sqrt{a}}-\frac{b}{3a},\frac{2}{\sqrt{a}}-\frac{b}{3a}\right] \tag{8}$$

则根据引理2，f的概率密度为

$$\begin{aligned}\rho_f(x)&=\rho_{T_3}(h^{-1}(x))\left|\frac{\mathrm{d}h^{-1}(x)}{\mathrm{d}x}\right| \\ &=\frac{\sqrt{a}}{\pi\sqrt{4-a\left(x+\dfrac{b}{3a}\right)^2}}, \\ &\quad x\in\left[-\frac{2}{\sqrt{a}}-\frac{b}{3a},\frac{2}{\sqrt{a}}-\frac{b}{3a}\right]\end{aligned} \tag{9}$$

证毕

在式(6)中，当$a=4$, $b=0$时，$\rho_f(x)=\dfrac{1}{\pi\sqrt{1-x^2}}$，这正是3阶Chebyshev多项式映射的概率密度。而Chebyshev多项式映射的概率密度的形式已是众所周知的。

这类3次多项式混沌映射的概率密度函数的形式，是进一步将3次多项式混沌映射均匀化或基于3次多项式混沌映射产生独立同分布的混沌密钥流[11,12]的理论基础。

2.4 分岔图和Lyapunov指数

定理1中，令$b=-6\sqrt{a}(a>0)$，化简并保留参数a，得到3次多项式混沌映射

$$f(x)=ax^3-6\sqrt{a}x^2+9x, x\in\left[0,4/\sqrt{a}\right] \tag{10}$$

在系统(10)中，固定$a\in[1,4]$，系统的分岔图和Lyapunov指数谱见图2。

3 性能分析

本节对分段线性混沌映射T_3和3次多项式混沌映射f的统计性质进行进一步的对比分析。

3.1 均匀性

信息熵是信息论中用于表征信源的不确定性程度。本文用信息熵度量混沌系统产生的混沌伪随机序列的不确定性程度。现在给出信息熵的定义。

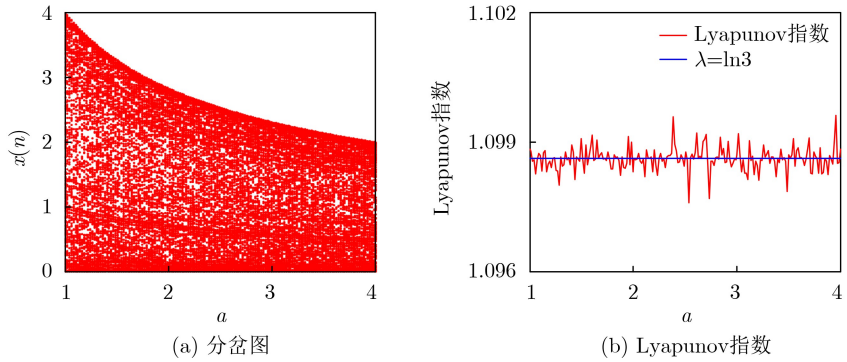
定义2 设$S=\{x_1,x_2,\cdots,x_n\}$是一种信息源，P为S的一个概率分布，记x_i的概率为p_i。则信源的信息熵定义为

$$H(S)=-\sum_{i=1}^{n}p_i\log_2 p_i \tag{11}$$

根据最大信息熵原理，当信源的概率分布为等概率分布，即$p_i=1/n$时，信息熵能取得最大值$\log_2 n$。

设混沌序列的长度为N，将序列的取值范围$[a,b]$划分为M个等分区间，并统计落在每个区间的序列值的个数，记为$n_i(i=1,2,\cdots,M)$。用频率$p_i=n_i/N$近似序列值落在每个区间上的概率，则有$\sum_{i=1}^{M}p_i=1$。

下面选定$N=10^6$, $M=2^8=256$，以T_3和系统



(a) 分岔图 (b) Lyapunov指数

图 2 系统(10)的分岔图和Lyapunov指数

式(10)为例，对拓扑共轭的这两类混沌系统进行信息熵分析，结果见图3。此处，序列的最大熵为8。

由图3可见，映射T_3的信息熵接近最大值8，从数值上验证了其均匀分布特性。

3.2 结构复杂性

3.2.1 谱熵算法和量化方法

在文献[16]中，谱熵(Spectral Entropy，SE)算法被用于分析混沌伪随机序列的结构复杂度，并得到了谱熵算法的计算速度快、实时性好以及可准确分析混沌伪随机序列的复杂度等结论。本文采用谱熵算法对分别基于拓扑共轭的映射T_3和3次多项式混沌映射的混沌伪随机序列的结构复杂度进行研究。具体的谱熵算法见文献[16]，下面仅给出谱熵的计算公式

$$\mathrm{se}=-\sum_{k=0}^{N/2-1}P_k\ln P_k,\ \mathrm{SE}=\frac{\mathrm{se}}{\ln(N/2)}\tag{12}$$

其中，P_k为相对功率谱密度，N是混沌序列的长度，se是信号的谱熵，SE是se归一化后的谱熵，其最大值是1。

根据香农熵的性质，序列功率谱分布越均衡，则序列频谱结构越复杂，信号没有明显的振荡规律，得到的SE测度值越大，即复杂度越大。下文直接用SE的值度量伪随机序列的结构复杂度，简称为SE复杂度。

本文主要考察二进制伪随机序列的SE复杂度，并采用如下量化方法将生成的混沌序列$\{z(n)\}$转换为二进制的混沌伪随机序列$\{y(n)\}$：

(1) 给定混沌系统的参数和初值，并进行n次迭代，得到混沌序列$\{z(n)\}$；

(2) 从序列$\{z(n)\}$截取长度为n_0的随机序列$\{x(n)\}_1^{n_0}$，其中$x(k)=z(k+1000)$；

(3) 按式(13)变换公式得到二进制伪随机序列$\{s(k)\}_1^{8n_0}$

$$\begin{aligned}&\mathrm{Tran}(x(k))=\begin{cases}\mathrm{mod}\left(\mathrm{round}\left(\dfrac{L(x(k)-\min(x))}{\max(x)-\min(x)}\right),256\right), & \min(x)\neq\max(x)\\ \mathrm{mod}\left(\mathrm{round}\left(\dfrac{Lx(k)}{\max(x)}\right),256\right), & \min(x)=\max(x)\end{cases}\\&s(k)=\mathrm{binary}(\mathrm{Tran}(x(k)))\end{aligned}\tag{13}$$

其中，$L=255\sqrt{2}\times10^8$。函数round(x)表示对x进行四舍五入运算得到整数，mod(x,n)表示对x进行模n运算。

(4) 从二进制伪随机序列$\{s(k)\}_1^{8n_0}$中截取长度为N的二进制伪随机序列$\{y(n)\}_1^N$，其中$y(k)=s(k)$。

在下文的SE复杂度分析中，若无特殊说明，则取序列长度$N=1000$。

3.2.2 SE复杂度分析

下面采用谱熵算法对映射T_3和系统式(10)产生的伪随机序列进行SE复杂度分析。

在系统式(10)中，取参数$a=1$，迭代初值$x_0=1.2$；两混沌系统的伪随机序列的SE复杂度随序列长度N变化的曲线见图4(a)。在系统式(10)中，固定参数$a\in[1,4]$，两混沌系统的伪随机序列的SE复杂度随参数a变化的曲线见图4(b)。图4(c)是当$a\in[2.004,2.124]$时，两混沌系统的伪随机序列的SE复杂度随参数a变化的曲线(图4(b)的局部放大)。

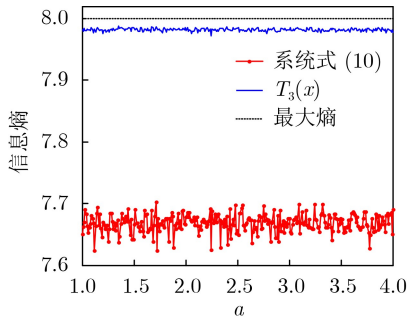
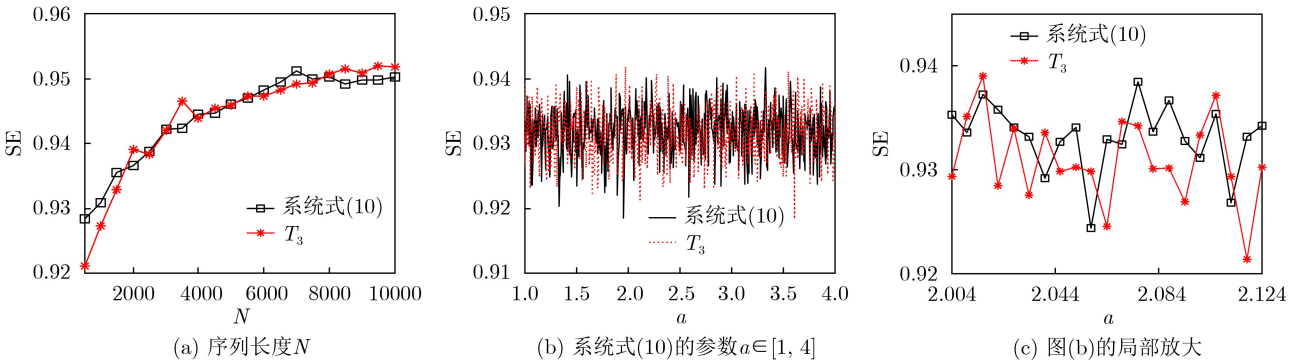


图 3 映射T_3和系统式(10)的信息熵



(a) 序列长度N　(b) 系统式(10)的参数$a\in[1,4]$　(c) 图(b)的局部放大

图 4 不同系统的伪随机序列的SE复杂度

由图4可知，两者的SE复杂度不存在明显的差异。本文将混沌序列量化成二进制伪随机序列的量化方法(记为M1)和文献[16]中的量化方法(记为M2)不同，以下进一步分析不同量化方法对于SE复杂度的影响。

在保持其他条件相同的情况下，采用文献[16]的量化方法得到二进制伪随机序列，并进行SE复杂度分析，结果见图5。

由图5可见，在SE复杂度方面，量化方法对系统的结构复杂性影响显著，与文献[16]中的量化方法比较，本文的量化方法对应的系统的SE复杂度更高。

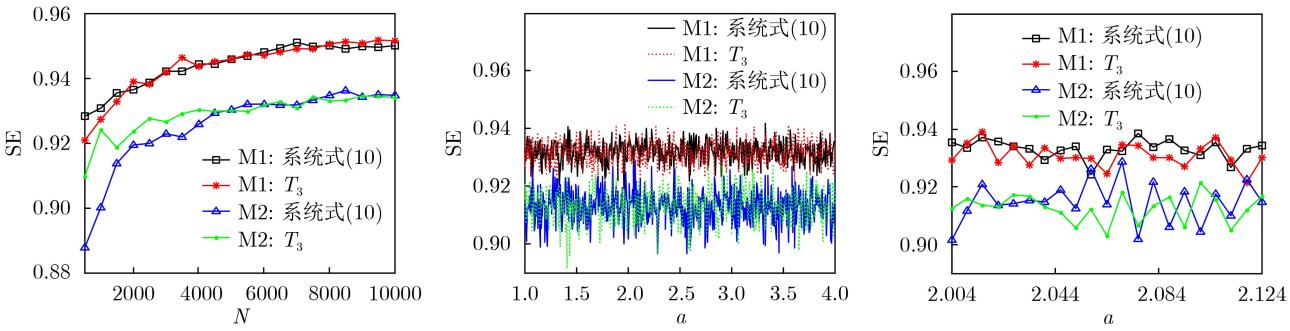
3.3 随机性分析

采用3.2.1节的量化方法，本节得到分别基于系统式(2)和系统式(10)的伪随机数发生器(Pseudo-Random Number Generator, PRNG)，并对比分析两系统的伪随机序列的随机性。

本节采用NIST提出的SP800-22检测标准[17]对混沌系统生成的二进制伪随机序列进行随机性检验。根据定理1，选取1000组不同的参数和初值，由PRNG生成1000组不同的二进制伪随机序列，并进行SP800-22随机性检测，结果见表1。

表1给出了检测序列的通过率和均匀性检验的P值(记为UP值)如果通过率位于区间$(1-\alpha)\pm 3\sqrt{\alpha(1-\alpha)/M}$且UP值大于$10^{-4}$，则认为该PRNG通过了检测。其中，$M$为进行该项测试的样本数，$\alpha$为显著性水平，此处取$\alpha=0.01$。

由表1可知，基于系统式(10)的PRNG通过了SP800-22随机性检验，而基于系统式(2)的PRNG不能全部通过SP800-22随机性检验。可见，拓扑共轭的两个混沌系统在使用本文的量化方法量化之后的随机性存在显著差异。3次多项式混沌映射与分段线性混沌映射T_3相比更适合用于设计PRNG。



(a) 序列长度N (b) 系统式(10)的参数$a\in[1, 4]$ (c) 图(b)的局部放大

图 5 不同量化方法下，不同系统的伪随机序列的SE复杂度

表 1 NIST SP800-22检测结果

序号	测试项	基于系统式(10)的PRNG			基于系统式(2)的PRNG		
		通过率	UP值	结果	通过率	UP值	结果
1	频率	0.9920	0.401199	通过	0.9880	0.890582	通过
2	块内频率	0.9880	0.275709	通过	**0.6940**	**$<10^{-4}$**	失败
3	累积和[1)]	0.9930	0.157251	通过	0.9860	0.358641	通过
4	游程	0.9900	0.010834	通过	0.9850	0.741918	通过
5	块内最长游程	0.9870	0.818343	通过	**0.0040**	**$<10^{-4}$**	失败
6	二元矩阵秩	0.9870	0.378705	通过	0.9880	0.520102	通过
7	离散傅里叶变换	0.9830	0.067300	通过	**0.8490**	**$<10^{-4}$**	失败
8	非重叠模块匹配[1)]	0.9810	0.759756	通过	**0.2950**	**$<10^{-4}$**	失败
9	重叠模块统计	0.9850	0.597620	通过	**0.0600**	**$<10^{-4}$**	失败
10	全局通用统计	0.9940	0.289667	通过	0.9910	**$<10^{-4}$**	失败
11	近似熵	0.9930	0.133404	通过	**0.0000**	**$<10^{-4}$**	失败
12	随机偏移[1)]	0.9875	0.482338	通过	0.9806	0.083979	通过
13	随机偏移变量[1)]	0.9860	0.196836	通过	0.9838	0.592833	通过
14	序列[1)]	0.9840	0.775337	通过	**0.0000**	**$<10^{-4}$**	失败
15	线性复杂度	0.9900	0.572847	通过	0.9910	0.811080	通过

测试项[1)]：该测试项包含几个子模块，此处列出了其中最差的结果。

黑体表示通过率或UP值不在接受范围内，即未通过检测。

4　4次多项式混沌映射和T_4的拓扑共轭

用同样的思路和方法可以得到的表达式为

$$T_4(x)=\begin{cases}4x, & 0\le x\le 0.5\\ 4(1-x), & 0.5<x\le 1.0\\ 4(x-1), & 1.0<x\le 1.5\\ 4(2-x), & 1.5<x\le 2.0\end{cases}\tag{14}$$

进一步可以得到，针对一般4次多项式$f(x)=ax^4+bx^3+cx^2+dx+e$和映射T_4，若满足条件

$$\left.\begin{array}{l}a>0\\ 32a^{4/3}+8ac-3b^2=0\\ 8a^2d-4abc+b^3=0\\ 256a^3e-512a^{8/3}+64a^2b(-d+1)\\ \quad+16ab^2c-3b^4=0\end{array}\right\}\tag{15}$$

则 f 和T_4 关 于 同 胚$h(x)=\dfrac{2}{a^{1/3}}\cos(\pi x/2)-\dfrac{b}{4a}$ $(x\in[0,2]\ )$拓扑共轭。

证明思路与定理1类似，证明过程略。

5　结论

本文基于一个分段线性混沌映射，分别给出了这个映射与3次多项式映射拓扑共轭的充分条件。从而间接地给出了一般3次多项式能成为混沌系统的充分条件。结合分段线性混沌映射的均匀分布特性，给出了这类3次多项式混沌映射的概率密度函数，这是进一步将3次多项式混沌映射均匀化或基于3次多项式混沌映射产生独立同分布的混沌密钥流的理论基础。对分段线性映射和多项式映射的均匀性、结构复杂性和随机性的分析结果显示，分段线性映射的均匀性优于多项式映射，而多项式映射的随机性优于分段线性映射，在结构复杂性方面，二者的结构复杂性并无显著差异，进一步给出了量化方法对二者的结构复杂性影响显著的结论。

参 考 文 献

[1] LI T Y and YORKE J A. Period three implies chaos[J]. *The American Mathematical Monthly*, 1975, 82(10): 985–992. doi: 10.2307/2318254.

[2] YANG Xiuping, MIN Lequan, and WANG Xue. A cubic map chaos criterion theorem with applications in generalized synchronization based pseudorandom number generator and image encryption[J]. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 2015, 25(5): 053104. doi: 10.1063/1.4917380.

[3] 王传福, 丁群. 基于混沌系统的SM4密钥扩展算法[J]. 物理学报, 2017, 66(2): 020504. doi: 10.7498/aps.66.020504.
WANG Chuanfu and DING Qun. SM4 key scheme algorithm based on chaotic system[J]. *Acta Physica Sinica*, 2017, 66(2): 020504. doi: 10.7498/aps.66.020504.

[4] LIN Zhuosheng, YU Simin, FENG Xiutao, *et al*. Cryptanalysis of a chaotic stream cipher and its improved scheme[J]. *International Journal of Bifurcation and Chaos*, 2018, 28(7): 1850086. doi: 10.1142/S0218127418500864.

[5] XU Zhengguang, TIAN Qing, and TIAN Li. Theorem to generate independently and uniformly distributed chaotic key stream via topologically conjugated maps of tent map[J]. *Mathematical Problems in Engineering*, 2012, 2012: 619257. doi: 10.1155/2012/619257.

[6] DASTGHEIB M A and FARHANG M. A digital pseudo-random number generator based on sawtooth chaotic map with a guaranteed enhanced period[J]. *Nonlinear Dynamics*, 2017, 89(4): 2957–2966. doi: 10.1007/s11071-017-3638-3.

[7] 梁涤青, 陈志刚, 邓小鸿. 基于小波包能量熵的混沌序列复杂度分析[J]. 电子学报, 2015, 43(10): 1971–1977. doi: 10.3969/j.issn.0372-2112.2015.10.014.
LIANG Diqing, CHEN Zhigang, and DENG Xiaohong. Analysis of chaotic sequence complexity based on wavelet packet energy entropy[J]. *Acta Electronica Sinica*, 2015, 43(10): 1971–1977. doi: 10.3969/j.issn.0372-2112.2015.10.014.

[8] MURILLO-ESCOBAR M A, CRUZ-HERNÁNDEZ C, CARDOZA-AVENDAÑO L, *et al*. A novel pseudorandom number generator based on pseudorandomly enhanced logistic map[J]. *Nonlinear Dynamics*, 2017, 87: 407–425. doi: 10.1007/s11071-016-3051-3.

[9] 臧鸿雁, 黄慧芳, 柴宏玉. 一类2次多项式混沌系统的均匀化方法研究[J]. 电子与信息学报, 2019, 41(7): 1618–1624. doi: 10.11999/JEIT180735.
ZANG Hongyan, HUANG Huifang, and CHAI Hongyu. Homogenization method for the quadratic polynomial chaotic system[J]. *Journal of Electronics & Information Technology*, 2019, 41(7): 1618–1624. doi: 10.11999/JEIT180735.

[10] 臧鸿雁, 柴宏玉. 一个二次多项式混沌系统的均匀化及其熵分析[J]. 物理学报, 2016, 65(3): 030504. doi: 10.7498/aps.65.030504.
ZANG Hongyan and CHAI Hongyu. Homogenization and entropy analysis of a quadratic polynomial chaotic system[J]. *Acta Physica Sinica*, 2016, 65(3): 030504. doi: 10.7498/aps.65.030504.

[11] 徐正光, 田清, 田立. 一类可以产生独立同分布密钥流的混沌系统[J]. 物理学报, 2013, 62(13): 120501. doi: 10.7498/aps.62.120501.
XU Zhengguang, TIAN Qing, and TIAN Li. A class of topologically conjugated chaotic maps of tent map to generate independently and uniformly distributed chaotic key stream[J]. *Acta Physica Sinica*, 2013, 62(13): 120501. doi: 10.7498/aps.62.120501.

[12] LIU Lingfeng, MIAO Suoxia, HU Hanping, *et al*. N-phase

logistic chaotic sequence and its application for image encryption[J]. *IET Signal Processing*, 2016, 10(9): 1096–1104. doi: 10.1049/iet-spr.2015.0522.

[13] TONG Xiaojun, CUI Minggen, and WANG Zhu. A new feedback image encryption scheme based on perturbation with dynamical compound chaotic sequence cipher generator[J]. *Optics Communications*, 2009, 282(14): 2722–2728. doi: 10.1016/j.optcom.2009.03.075.

[14] TONG Xiaojun, ZHANG Miao, WANG Zhu, *et al*. A image encryption scheme based on dynamical perturbation and linear feedback shift register[J]. *Nonlinear Dynamics*, 2014, 78(3): 2277–2291. doi: 10.1007/s11071-014-1564-1.

[15] HAO Bolin. Starting with Parabola: An Introduction to Chaotic Dynamics[M]. 2nd ed. Beijing: Peking University Press, 2013: 114–118.

[16] 孙克辉, 贺少波, 何毅, 等. 混沌伪随机序列的谱熵复杂性分析[J]. 物理学报, 2013, 62(1): 010501. doi: 10.7498/aps.62.010501.

SUN Kehui, HE Shaobo, HE Yi, *et al*. Complexity analysis of chaotic pseudo-random sequences based on spectral entropy algorithm[J]. *Acta Physica Sinica*, 2013, 62(1): 010501. doi: 10.7498/aps.62.010501.

[17] RUKHIN A, SOTO J, NECHVATAL J, *et al*. Special Publication 800-22 A statistical test suite for random and pseudorandom number generators for cryptographic applications[S]. U. S. Department of Commerce: National Institute of Standards and Technology, 2010.

臧鸿雁：女，1973年生，副教授，研究方向为非线性系统同步理论与混沌密码学.

韦心元：男，1994年生，硕士生，研究方向为混沌系统理论与混沌密码学.

袁 悦：女，1996年生，硕士生，研究方向为混沌系统理论与混沌密码学.

责任编辑：陈 倩