第 57 卷 第 10 期 2008 年 10 月
1000-3290/2008/57(10)/6103-09

物 理 学 报
ACTA PHYSICA SINICA

Vol.57,No.10,October,2008

基于切延迟的椭圆反射腔的吸引子研究*

谭司庭† 何 毅 盛利元

(中南大学物理科学与技术学院,长沙 410083)

(2007 年 10 月 2 日收到;2008 年 2 月 26 日收到修改稿)

本文使用转移矩阵的方法,引入椭圆角转换函数,使椭圆问题得到简化,推导出十分简单的切延迟椭圆反射的迭代公式,这样非常有利于理论分析.切延迟椭圆反射腔映射系统(TD-ERCS)在切延迟 1 单位时存在吸引子,利用该公式,对其吸引子形成的原因及稳定性做了理论分析,发现圆的吸引子与椭圆不尽相同;同时发现椭圆有两个不动线,但只有一个是稳定的.本文还发现,随着椭圆压缩因子 μ 的减小,对于任意的切延迟因子 m,相邻两次迭代数据间的相关性增强,这说明将该系统用作密码系统,椭圆压缩因子 μ 不能太小,同时混沌系统本身要求 μ 不能太大,否则降低安全度.

关键词:混沌,切延迟,TD-ERCS,吸引子

PACC:0545

1. 引 言

由于信息技术的飞速发展,特别是互联网的普及,信息的安全性已显得越来越重要,同时也对信息安全提出了更高的要求.非线性混沌系统具有对初始条件敏感且使其迭代轨迹在一定程度上不可预测的特点,同时与初始条件存在着复杂的非线性关系.因此近年来,基于混沌系统的密码体系成为信息安全的一个研究热点[1—3].

基于切延迟的椭圆反射腔的物理系统,切延时因子 m 大于 1 时呈现各态遍历性、其全域混沌性和全域零相关性,是作为混沌加密系统的一个较为理想系统[4].因此对该系统的研究具有现实意义[5—7].

该系统在切延时因子 $m=1$ 时存在吸引子[4].如果能从理论上认识该吸引子,使我们对该系统有更加深刻的认识.对 $m>1$ 的系统状态研究,也有助于对该系统安全性的认识.

本文主要从理论和数值计算实验上研究 $m=1$ 时的吸引子,以及 $m>1$ 时在 μ 较小时状态聚集的情况.

2. 理论分析

2.1. 系统物理模型

为了方便起见,这里重写该物理模型.如图 1 所示,设一条射线 M_0M_1 入射到椭圆 M_1 点,在 M_1 点以 M_1 点的椭圆切线作为反射面,反射后达到 M_2 点,如此继续,系统演化成一个点序列

$$M = \{M_i, i = 0,1,2,3,\cdots\}.$$

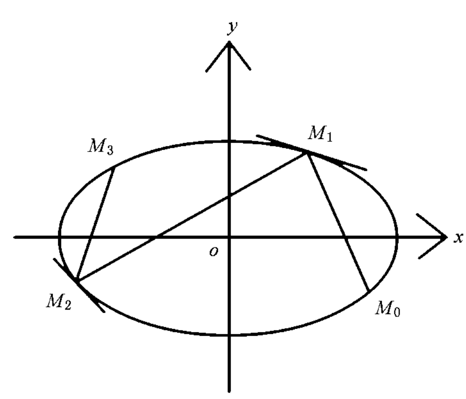

图 1 椭圆反射腔映射系统

* 国家自然科学基金(批准号:60672041)资助的课题.

† E-mail:tansting@mail.csu.edu.cn

如果入射线 $M_{n-1}M_n$ 在 M_n 点以 M_{n-m} 点的切线为反射面,这种操作称为延迟 m 个单位的切延时操作.经过切延时操作后的系统称为椭圆反射系统称为切延时椭圆反射腔系统(tangent-delay ellipse reflecting cavity map system,TD-ERCS).

设规一化标准椭圆参数方程为

$$x=\cos(\theta),\quad y=\mu\sin(\theta),\tag{1}$$

其中 $0<\mu\leqslant 1$ 为椭圆压缩因子.我们用参数角 θ_i 描述点 M_i,这样得到点序列

$$\theta=\{\theta_i,i=0,1,2,3,\cdots\}.$$

引进 M_iM_{i+1} 与 x 轴的夹角 α_i,也形成一个序列射线夹角序列

$$\alpha=\{\alpha_i,i=0,1,2,3,\cdots\}.$$

由于经过 M_i 点后,出射线在 α_i 和 $\alpha_i+\pi$ 两个方向上的直线都与椭圆交于 M_{i+1} 点.因此认为 α_i 和 $\alpha_i+\pi$ 代表同一个物理量,即不考虑射线方向.故 θ 和 α 的周期分别为 2π 和 π.为了方便,取 $\theta\in[-\pi,\pi]$,$\alpha\in\left[-\frac{\pi}{2},\frac{\pi}{2}\right]$.

对于有 m 个单位切延迟的系统,任意给出 θ 的初始值:

$$\begin{aligned}&\theta_0,\alpha_0, && m=0,\\ &\theta_0,\theta_1,\cdots,\theta_{m-1},\alpha_{m-1}, && m\geqslant 1,\end{aligned}\tag{2}$$

当然也可将 α_{m-1} 换成 θ_m,从而算出 α_{m-1}.这样就可以递推出后面所有序列.

2.2.系统的转移矩阵描述

使用转移矩阵的方法,很容易得到系统的递推公式

$$\begin{pmatrix}\sin(\theta_n)\\ \cos(\theta_n)\end{pmatrix}=\begin{pmatrix}K_0 & -K_1\\ -K_1 & K_0\end{pmatrix}\begin{pmatrix}\sin(\theta_{n-1})\\ \cos(\theta_{n-1})\end{pmatrix},\tag{3}$$

$$\begin{pmatrix}\sin(\alpha_n)\\ \cos(\alpha_n)\end{pmatrix}=\begin{pmatrix}T_0 & -T_1\\ -T_1 & -T_0\end{pmatrix}\begin{pmatrix}\sin(\alpha_{n-1})\\ \cos(\alpha_{n-1})\end{pmatrix},\tag{4}$$

其中

$$K_0=\frac{\mu^2\cos^2(\alpha_{n-1})-\sin^2(\alpha_{n-1})}{\mu^2\cos^2(\alpha_{n-1})+\sin^2(\alpha_{n-1})},$$

$$K_1=\frac{2\mu\sin(\alpha_{n-1})\cos(\alpha_{n-1})}{\mu^2\cos^2(\alpha_{n-1})+\sin^2(\alpha_{n-1})},$$

$$T_0=\frac{\mu^2\cos^2(\theta_{n-m})-\sin^2(\theta_{n-m})}{\mu^2\cos^2(\theta_{n-m})+\sin^2(\theta_{n-m})},$$

$$T_1=\frac{2\mu\sin(\theta_{n-m})\cos(\theta_{n-m})}{\mu^2\cos^2(\theta_{n-m})+\sin^2(\theta_{n-m})},$$

$$n=m+1,m+2,\cdots.$$

2.3. 椭圆角转换函数

如图 2(a)所示,椭圆上的点 M 与原点的连线与 x 轴的夹角 $\angle AOM=\varphi$,对应的参数角 $\angle AOP=\theta$,则有 $\theta=f_\mu(\varphi)$,称为椭圆角转换函数.其定义为

$$f_\mu(\varphi)=\arctan\left(\frac{1}{\mu}\tan(\varphi)\right)+k\pi,\tag{5}$$

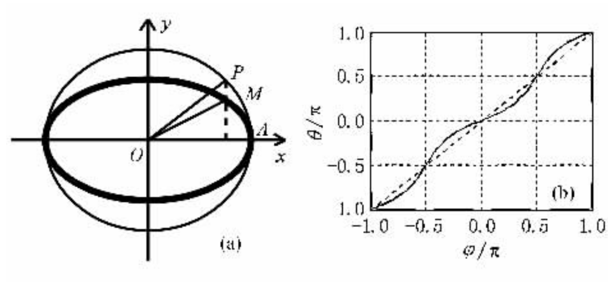

图 2 椭圆角转换函数 $\theta=f_\mu(\varphi)$

其中 $-\frac{\pi}{2}+k\pi\leqslant\varphi\leqslant\frac{\pi}{2}+k\pi$,$k$ 为整数,其函数如图 2(b)所示.

函数 $f_\mu(\varphi)$ 具有如下性质:

1)奇对称性:$f_\mu(-\varphi)=-f_\mu(\varphi)$.

2)周期点线性性:

$$f_\mu(\varphi+k\pi)=f_\mu(\varphi)+k\pi.$$

$$f_\mu(k\varphi/2)=k\pi/2.$$

3)其导数

$$\begin{aligned}\frac{\mathrm{d}\theta}{\mathrm{d}\varphi}&=f'_\mu(\varphi)\\ &=\frac{\mu}{\mu^2\cos^2\varphi+\sin^2\varphi}\\ &=\frac{\cos^2\theta+\mu^2\sin^2\theta}{\mu}.\end{aligned}\tag{6}$$

$$f'_\mu(0)=\frac{1}{\mu},f'_\mu\left(\frac{\pi}{2}\right)=\mu.$$

令

$$\begin{aligned}&\varphi_1=\mathrm{arctg}(\sqrt{\mu}),\\ &\varphi_2=\mathrm{arctg}\sqrt{\frac{\mu(2-\mu)}{1-2\mu}}\ \text{且}\ \mu<\frac{1}{2},\end{aligned}\tag{7}$$

则有 $f'_\mu(\varphi_1)=1$,$f'_\mu(\varphi_2)=\frac{1}{2}$.

2.4. 转移矩阵的物理意义

引进椭圆角转换函数后,转移矩阵 $\boldsymbol{K}$,$\boldsymbol{T}$ 可以写成

$$\boldsymbol{K}=\begin{pmatrix} K_0 & -K_1 \\ -K_1 & -K_0 \end{pmatrix} =\begin{pmatrix} \cos(2f_\mu(\alpha_{n-1})) & -\sin(2f_\mu(\alpha_{n-1})) \\ -\sin(2f_\mu(\alpha_{n-1})) & -\cos(2f_\mu(\alpha_{n-1})) \end{pmatrix},$$

$$\boldsymbol{T}=\begin{pmatrix} T_0 & -T_1 \\ -T_1 & -T_0 \end{pmatrix} =\begin{pmatrix} \cos(2f_\mu(\theta_{n-m})) & -\sin(2f_\mu(\theta_{n-m})) \\ -\sin(2f_\mu(\theta_{n-m})) & -\cos(2f_\mu(\theta_{n-m})) \end{pmatrix},$$

则(3)和(4)式可以简单的写成

$$\theta_n=\pi-\theta_{n-1}+2f_\mu(\alpha_{n-1})\bmod 2\pi, \tag{8}$$

$$\alpha_n=\pi-\theta_{n-1}+2f_\mu(\theta_{n-m})\bmod\pi. \tag{9}$$

(8)式代表的物理意义如图3(a)所示：在M_{n-1}点，出射线为α_{n-1}，则下一个序列点为M_n. α_{n-1}代表未经转换的射线$M_{n-1}M_n$，$f_\mu(\alpha_{n-1})$代表转换后的射线$M'_{n-1}M'_n$. 由于θ_n和θ_{n-1}都是参数角，即转换后的角，θ_n和θ_{n-1}的角平分线OM与转换后的射线$M'_{n-1}M'_n$垂直.

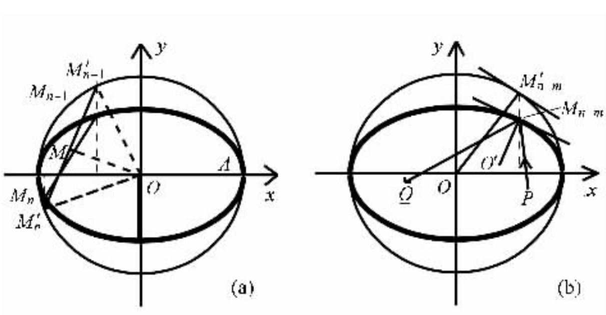

图3 递推公式(8)和(9)的物理意义

(9)式代表的物理意义如图3(b)所示：入射线P以α_{n-1}方向入射，以M_{n-m}点的切线为反射面，则出射线Q的方向为α_n. θ_{n-m}代表转换后的法线方向OM'_{n-m}，$f_\mu(\theta_{n-m})$代表转换之前的法线方向$O'M_{n-m}$，α_n和α_{n-1}是没有经过转换的角，α_n和α_{n-1}平分线必须与没有经过转换的法线$O'M_{n-m}$垂直或相等(有可能在反射线的反向延长线上，所以存在相等的情况)，反射定理才成立.

从这里可以看出，由于引进了椭圆角转换函数后，可以将椭圆问题变得非常简单.

2.5. 吸引子的理论分析

文献[4]中，通过实验的方法发现了在$m=1$时系统存在方形吸引子. 下面通过(8)和(9)式从理论上来分析吸引子产生的原因.

假设吸引子的存在函数依赖关系

$$\alpha_n=g(\theta_n)$$

代入(8)和(9)式，得

$$\theta_n=\pi+2f_\mu(g(\theta_{n-1}))-\theta_{n-1},$$

$$g(\theta_n)=\pi+2f_\mu(\theta_{n-1})-g(\theta_{n-1})\bmod 2\pi,$$

消去θ_n得

$$g(\pi+2f_\mu(g(\theta_{n-1}))-\theta_{n-1}) =\pi+2f_\mu(\theta_{n-1})-g(\theta_{n-1})\bmod 2\pi, \tag{10}$$

(10)式必须对所有的θ_{n-1}都成立，因此$g(x)$必须是线性函数，令$g(x)=ax+b$代入(10)式：

$$a(\pi+2f_\mu(a\theta_{n-1}+b)-\theta_{n-1})+b =\pi+2f_\mu(\theta_{n-1})-(a\theta_{n-1}+b),$$

化简得

$$a\pi+2b-\pi =-2(af(a\theta_{n-1}+b)-f(\theta_{n-1})). \tag{11}$$

下面分两种情况讨论：

1) $\mu=1$时

此时$f_\mu(\theta)=\theta$. (11)式变为

$$2(a^2-1)\theta_{n-1}+(a-1)\pi+2b(1+a)=0,$$

故$a=\pm1$. 当$a=1$时有，$b=0$；当$a=-1$时，b可以为任意数值. 所以吸引子表示为

$$\alpha_n+\theta_n=C(\text{常数})\text{ 或 }\alpha_n-\theta_n=0,$$

在后面的稳定性发现，$\alpha_n=\theta_n$是不稳定的. 所以看到的吸引子是

$$\alpha_n+\theta_n=C(\text{常数}). \tag{12}$$

2) $\mu<1$时

利用函数$f_\mu(\theta)$周期点线性性及角度的周期性，得到$a=\pm1$，$b=k\pi$.

由于射线没有方向性，α_n的周期为π. $b=k\pi$都对应同一条$b=0$的直线. 吸引子表示为

$$\alpha_n\pm\theta_n=0,$$

该吸引子是两条直线，$\alpha_n=\theta_n$或$\alpha_n=-\theta_n$. 如果采用文献[4]的坐标，即将$[-\pi,0]$的区域折射到$[0,\pi]$的区域，这两条直线都变为方形曲线. 在后面的稳定性分析可以知道，$\alpha_n=\theta_n$是不稳定的.

所以看到的吸引子是

$$\alpha_n+\theta_n=0. \tag{13}$$

从得到的吸引子可以看出，对于圆和椭圆的吸引子是不一样的. 对于椭圆而言，无论初值如何设置，最终都趋近于$\alpha_n+\theta_n=0$式的直线上. 但对于圆而言，初值不同，将吸引到不同的直线上，这样的直线上有无穷多个(因常数不同). 如果采用文献[4]的

坐标,这时的吸引子在纵轴上有一个平移,平移量的多少与初值有关.

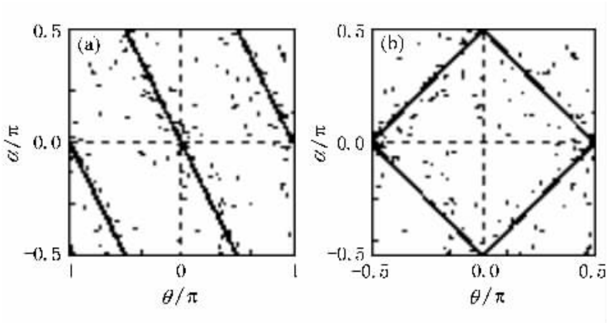

图 4 $m=1$ 时的吸引子.其中 $\mu=0.5$,$\theta_0=0.01$, $\alpha_0=0.011$

图 4 是实验结果.图 4(a)中的三条直线都是 $\alpha+\theta=0$ 直线,由于 α 的取值范围只有[$-\pi/2$,$\pi/2$],而 θ 的取值范围是[$-\pi$,π],$\alpha+\theta=0$ 直线的上半部分和下半部分平移就变成图 4(a)中的三条直线.如果再将图 4(a)中的左半部分,翻转到右半部分,使 θ 的取值范围为[0,π]就形成图 4(b),即方形吸引子,这是文献[4]的结果.

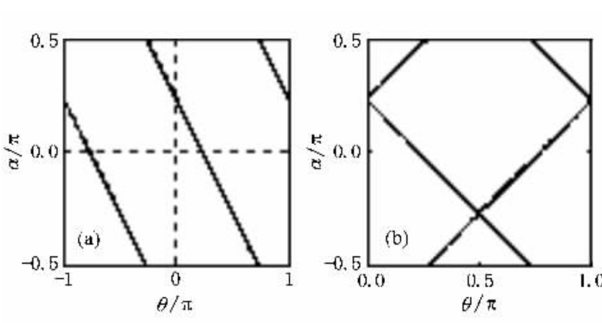

图 5 $m=1$ 时的吸引子.其中 $\mu=1$,$\theta_0=0.1$, $\alpha_0=0.4$

图 5 的实验结果显示了,在 $\mu=1$ 即圆时,吸引子对应的不再是固定的方形,而是在纵轴上有一个平移,平移量的多少与初值选取有关,这是圆的一个特殊情况.图 5(a)中直线正好对应(12)式.

现在要提出的问题是:让椭圆压缩因子 μ 慢慢趋近 1,系统是如何从吸引子(13)式突变到吸引子(12)的呢.如果 μ 无限趋近 1 而不等于 1,吸引子永远停留在(13)式,只有等于 1 才到(12)式,所以从椭圆到圆的过程是一个质的飞跃,但这两个系统应该是无限接近的.这个问题将在稳定性讨论中得到回答.

2.6. 吸引子的稳定性讨论

将(8)和(9)式相加减,并利用 $m=1$ 的条件,容易得到

$$(\alpha_n \pm \theta_n)+(\alpha_{n-1} \pm \theta_{n-1}) = 2(f_\mu(\theta_{n-1}) \pm f_\mu(\alpha_{n-1})), \tag{14}$$

为方便起见,令

$$\delta_n = \alpha_n \pm \theta_n, \tag{15}$$

则(14)式变为

$$\delta_n + \delta_{n-1} = 2(f_\mu(\theta_{n-1}) - f_\mu(\theta_{n-1} \mp \delta_{n-1})). \tag{16}$$

从(15)式知,如果 $\delta_{n-1}=0$,则 $\delta_n=0$.因此在以后的每一级都满足 $\delta_{n+i}=0$.即 $\alpha_{n1} \pm \theta_n = 0$ 是不动线.

为了讨论其稳定性,假定 δ_{n-1}是一个微扰.

1)先讨论 $\theta_{n-1}-\alpha_{n-1}=0$ 的状态

(16)式变为

$$\delta_n + \delta_{n-1} = 2(f_\mu(\theta_{n-1}) - f_\mu(\theta_{n-1}+\delta_{n-1})),$$

利用拉格朗日中值定理得,存在 ξ_{n-1}使

$$\delta_n = -(2f'_\mu(\xi_{n-1})+1)\delta_{n-1},$$
$$\theta_{n-1} < \xi_{n-1} < \theta_{n-1}+\delta_{n-1}, \tag{17}$$

显然$|\delta_n| > |\delta_{n-1}|$.因此对于这种吸引子是不稳定的,所以它不能称为吸引子,而只能是不稳定不动线.

2)再讨论 $\alpha_{n-1}+\theta_{n-1}=0$ 的状态

使用同样的方法可以得出

$$\delta_n = (2f'_\mu(\xi_{n-1})-1)\delta_{n-1},$$
$$\theta_{n-1}-\delta_{n-1} < \xi_{n-1} < \theta_{n-1}, \tag{18}$$

重复利用(18)式得

$$\delta_n/\delta_0 = \prod_{i=0}^{n-1}(2f'_\mu(\xi_i)-1), \tag{19}$$

平均每一步的比值取对数

$$\lim_{n\to\infty}\ln\sqrt[n]{\delta_n/\delta_0} \approx \frac{1}{n}\sum_{i=0}^{n-1}\ln(2f'_\mu(\xi_i)-1). \tag{20}$$

下面再分两种情况讨论:

①$\mu=1$ 时

这时有 $f'_\mu=1$,(18)式变为

$$\delta_n = \delta_{n-1}.$$

所以,对圆来说,$\alpha_n+\theta_n$ 是不变的.对于任何 $\alpha_n+\theta_n$ 值都是不变线.这也是(12)式为何是常数的原因.

②$0<\mu<1$ 时

根据(7)式,当 $\mu>0.5$ 时,对任意的 δ_{n-1},

$$2f'_\mu(\xi_{n-1})-1>0;$$

而当 $\mu<0.5$ 时,$\xi_{n-1}\in[\varphi_2,\pi/2]\cup[-\pi/2,-\varphi_2]$ 时,

$$2f'_\mu(\xi_{n-1})-1<0.$$

当 $\xi_{n-1}\in[-\varphi_1,\varphi_1]$ 时，

$$1\leqslant 2f'_\mu(\xi_{n-1})-1\leqslant\frac{2}{\mu}-1,$$

此时有 $|\delta_n|\geqslant|\delta_{n-1}|$；当 $\xi_{n-1}\in[\varphi_1,\pi/2]\cup[-\pi/2,-\varphi_1]$ 时，$|2f'_\mu(\xi_{n-1})-1|\leqslant 1$，此时有 $|\delta_n|\leqslant|\delta_{n-1}|$. 因而，在 θ 较大时，状态向吸引子靠近的；而在 θ 较小时状态偏离吸引子.

在 $n\to\infty$ 时，(20) 式的求和可以近似地用积分代替，假定 θ 的分布是均匀的，这样

$$\frac{1}{n}\ln\frac{\delta_n}{\delta_0}\approx\frac{2}{\pi}\int_0^{\pi/2}\ln\left|\left(\frac{2\mu}{\mu^2\cos^2\alpha+\sin^2\alpha}-1\right)\right|\mathrm{d}\alpha,\quad(21)$$

利用数值积分，(21) 式 $\frac{1}{n}\ln\frac{\delta_n}{\delta_0}$ 随 μ 的理论变化规律如图 6(a) 所示.

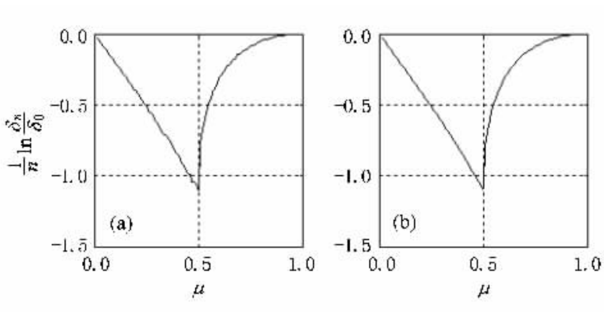

图 6　$(\ln(\delta_n/\delta_0))/n$ 在 $n\to\infty$ 时随 μ 的变化规律. (a) 为理论结果；(b) 为数值计算的实验结果，对于每一个 μ 迭代次数 $N=20000$

从图 6 可以看出，理论结果与实验结果完全吻合，这也从侧面说明了，$m=1$ 时，θ 的分布是均匀的. 从计算结果看，无论是 $\mu\geqslant0.5$ 还是 $\mu\leqslant0.5$，都有 $(\ln(\delta_n/\delta_0))/n\leqslant0$，即平均每一步的比值 $\sqrt[n]{\delta_n/\delta_0}\leqslant1$. 也就是说，就全局而言，无论是 $\mu\geqslant0.5$ 还是 $\mu\leqslant0.5$，状态向吸引子 $\alpha_{n-1}+\theta_{n-1}=0$ 靠近. 因此吸引子 $\alpha_{n-1}+\theta_{n-1}=0$ 是稳定的.

从这里可以看到，μ 趋近 1 过程中，随着 μ 的增大，$\frac{1}{n}\ln\frac{\delta_n}{\delta_0}$ 接近零，$\alpha_n+\theta_n$ 值变化越来越小，从而实现与 $\mu=1$ 的系统接近，这就回答了上节的问题.

图 7 是数值计算结果. 从图中可以看出，在初始条件时，θ_0 和 α_0 几乎相同，但随着迭代次数的增大，$\alpha-\theta$ 它们迅速偏离 0，根本无法走到 $\alpha=\theta$ 的直线上；刚开始，$\alpha+\theta$ 偏离 0，到 $n=80$ 左右，已达到最大 $\pi/2$. 随后才慢慢下降，最终，向 $\alpha+\theta=0$ 的吸引子靠近. 这完全证实了理论对 $m=1$ 时吸引子的猜想和分析.

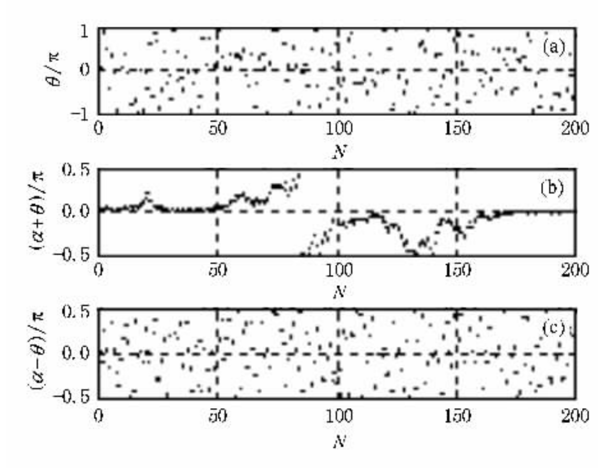

图 7　$\mu=0.8$，$\theta_0=0.01$，$\alpha_0=0.011$，$m=1$. (a)，(b)，(c) 分别是 θ，$\alpha+\theta$，$\alpha-\theta$ 随 N 的变化规律

2.7. Lyapunov 指数

从某种意义上说，(21) 式就是 Lyapunov 指数，它小于零正说明系统稳定的向吸引子 $\alpha_{n-1}+\theta_{n-1}=0$ 靠近. 但它不是整个系统的 Lyapunov 指数，事实上，尽管系统趋近于吸引子 $\alpha_{n-1}+\theta_{n-1}=0$，整个系统仍是混沌的，只是变化的维数从二维变为一维罢了. 为了证明这一点，我们计算整个系统的 Lyapunov 指数.

对于 (8) 和 (9) 式写成矢量形式

$$\boldsymbol{X}_n=\boldsymbol{F}(\boldsymbol{X}_{n-1}),\quad(22)$$

其中 $\boldsymbol{X}_n=\begin{pmatrix}\theta_n\\ \alpha_n\end{pmatrix}$，利用 $m=1$，其雅科比矩阵为

$$\boldsymbol{DF}_{n-1}=\begin{pmatrix}-1 & 2f'_\mu(\alpha_{n-1})\\ 2f'_\mu(\theta_{n-1}) & -1\end{pmatrix},\quad(23)$$

对于初值的偏离 $\mathrm{d}X_0=\begin{pmatrix}\mathrm{d}\theta_0\\ \mathrm{d}\alpha_0\end{pmatrix}$，可以得到

$$\mathrm{d}\boldsymbol{X}_n=\boldsymbol{DF}_{n-1}\cdot\boldsymbol{DF}_{n-2}\cdot\cdots\cdot\boldsymbol{DF}_0\cdot\mathrm{d}\boldsymbol{X}_0$$

令 $\boldsymbol{D}_{n-1}=\boldsymbol{DF}_{n-1}\cdot\boldsymbol{DF}_{n-2}\cdot\cdots\cdot\boldsymbol{DF}_0$，上式写成

$$\mathrm{d}\boldsymbol{X}_n=\boldsymbol{D}_{n-1}\mathrm{d}\boldsymbol{X}_{n-1},$$

则

$$\begin{aligned}\mathrm{d}\boldsymbol{X}_n^2&=(\mathrm{d}\theta_n)^2+(\mathrm{d}\alpha_n)^2\\&=\mathrm{d}\boldsymbol{X}_0^{\mathrm{T}}\boldsymbol{D}_{n-1}^{\mathrm{T}}\boldsymbol{D}_{n-1}\mathrm{d}\boldsymbol{X}_0,\end{aligned}$$

令 $\boldsymbol{H}_{n-1}=\boldsymbol{D}_{n-1}^{\mathrm{T}}\boldsymbol{D}_{n-1}$，它是对称矩阵，它的特征值都是正实数. 所以有

$$\mathrm{d}\boldsymbol{X}_n^2=\mathrm{d}\boldsymbol{X}_0^{\mathrm{T}}\boldsymbol{H}_{n-1}\mathrm{d}\boldsymbol{X}_0.\quad(24)$$

前面已经讨论了在 $n\to\infty$ 时，系统将趋近 $\alpha_{n-1}+\theta_{n-1}=0$. Lyapunov 指数是与初值无关的，故选择

初值 $\alpha_0+\theta_0=0$,则以后恒有 $\alpha_n+\theta_n=0$.设

$$G=\begin{pmatrix}\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2}\\ -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2}\end{pmatrix},$$

则

$$G^{-1}\cdot DF_i\cdot G=\begin{pmatrix}-1-2f'_\mu(\alpha_i) & 0\\ 0 & -1+2f'_\mu(\alpha_i)\end{pmatrix},$$

因此

$$G^{-1}\cdot H_{n-1}\cdot G=\begin{pmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{pmatrix}, \tag{25}$$

其中

$$\lambda_1=\prod_{i=0}^{n-1}(1+2f'_\mu(\alpha_i))^2, \tag{26}$$

$$\lambda_2=\prod_{i=0}^{n-1}(1-2f'_\mu(\alpha_i))^2, \tag{27}$$

所以得到,最大和最小的 lyapunov 指数分别为

$$LE_{1\max}=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln(1+2f'_\mu(\alpha_i)), \tag{28}$$

$$LE_{2\min}=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln(|1-2f'_\mu(\alpha_i)|). \tag{29}$$

比较(29)和(20)式很容易看到,(20)式就是最小的 Lyapunov 指数.

利用 θ 的均匀性很容易得到 $m=1$ 时的最大的 Lyapunov 指数理论值.

$$LE_{1理大}=\frac{2}{\pi}\int_0^{\pi/2}\ln\left(1+\frac{4\mu^2}{(\mu^2\cos^2\theta+\sin^2\theta)^2}\right)\mathrm{d}\theta,$$

$$LE_{2理小}=\frac{2}{\pi}\int_0^{\pi/2}\ln\left(\left|1-\frac{4\mu^2}{(\mu^2\cos^2\theta+\sin^2\theta)^2}\right|\right)\mathrm{d}\theta,$$

最大,最小 Lyapunov 指数结果分别对应图 8 和图 6.

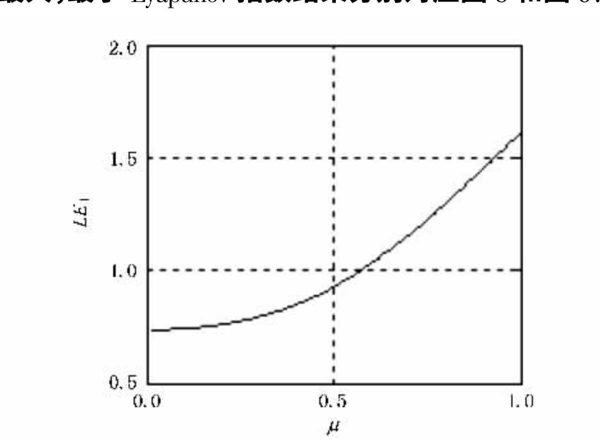

图 8 $m=1$ 时最大的 Lyapunov 指数理论值 LE_1

2.8. 任意延时因子 m 的情形

使用 2.4 节中 $m=1$ 的情况同样的方法讨论 $m>1$ 的情况,发现不可能存在吸引子.下面利用 Lyapunov 指数分析的方法来证明这一点.对于 $m>1$ 时,将有 $m+1$ 个 Lyapunov 指数.

利用(8)和(9)式我们可以将递推公式写成矢量形式:

$$X_n=\begin{pmatrix}\theta_{n-m+1}\\ \cdots\\ \theta_n\\ \alpha_n\end{pmatrix},\quad X_n=F(X_{n-1}),$$

具体表达式为

$$\begin{aligned}\theta_{n-m+1}&=\theta_{n-m+1},\\ &\cdots\\ \theta_{n-1}&=\theta_{n-1},\\ \theta_n&=\pi-\theta_{n-1}+2f(\alpha_{n-1}),\\ \alpha_n&=\pi-\alpha_{n-1}+2f(\theta_{n-m}),\end{aligned}$$

这样得到雅科比矩阵

$$DF_{n-1}=\begin{pmatrix}0 & 1 & 0 & \cdots & 0\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & \cdots & 0 & 1 & 0\\ 0 & \cdots & 0 & -1 & 2f'(\alpha_{n-1})\\ 2f'(\theta_{n-m}) & 0 & \cdots & 0 & -1\end{pmatrix}, \tag{30}$$

H_n 和 2.7 节中一样,不过求 H_n 特征值不容易.由于 H_n 是实对称矩阵,可以使用 Jacobi 方法求解[8,9],但必须避免数据溢出和小特征值被吃的问题,具体方法在这里不再说明.图 9 就是用该方法计算得到的三个 Lyapunov 指数.从计算结果看到它们几乎相同,而且都大于零,因此 $m=2$ 时不可能有吸引子存在.实际上 $m\geqslant2$ 时有类似的情况.

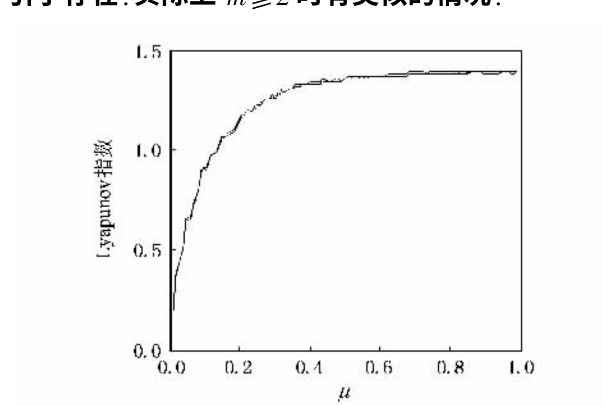

图 9 $m=2$ 时的 Lyapunov 指数

尽管在 $m>1$ 时不存在吸引子,但是当 μ 趋向 0 时,所有 α_{n-1} 转换后几乎都变成 $\pi/2$,即 $f_\mu(\alpha_{n-1})$

近似为一个阶跃函数，这样大量的数据将集中在$\pi/2$附近．从(8)式可以看出，这等价与大量的数据集中在 $\theta_n+\theta_{n-1}=0$ 的直线附近．即当 μ 较小时也存在一种吸引，而且这种吸引与 m 无关．下面我们定量来讨论一下．

定理　设任意函数 $y=f(x)$，如果 x 的态密度为$p_x(x)$，则 y 的态密度为

$$p_y(y)=p_x(f^{-1}(y))/f'(f^{-1}(y)).\qquad(31)$$

证明　在 x 处任给一微小的区间$(x,x+\mathrm{d}x)$，则在该区间的状态数为 $p_x(x)\mathrm{d}x$．在该区间对应的 y 的区间为$(y,y+\mathrm{d}y)$，其状态数为 $p_y(y)\mathrm{d}y$．他们是同样的状态，故

$$p_x(x)\mathrm{d}x=p_y(y)\mathrm{d}y,$$

$$p_y(y)=p_x(x)/(\mathrm{d}y/\mathrm{d}x)=p_x(f^{-1}(y))/f'(f^{-1}(y)).$$

证毕．

令 $\theta=\theta_n+\theta_{n-1}$，$\alpha=\alpha_{n-1}$，则(8)式变为

$$\theta=\pi+2f(\alpha).$$

设 α 的状态密度为$p_\alpha(\alpha)$，则根据上述定理，θ 的状态密度为

$$p_\theta(\theta)=p_\alpha(\alpha)/(2f'(\alpha)),$$

$$p_\theta(\theta)=p_\alpha(\alpha)\frac{\mu}{(1+\mu^2)-(1-\mu^2)\cos\theta},\qquad(32)$$

$p_\theta(\pi)=\mu p_\alpha(0)/2$；$p_\theta(0)=p_\alpha(\pi/2)/2\mu$．所以当 $\mu\to0$ 时，$p_\theta(\pi)\to0$，而 $p_\theta(0)\to\infty$．可见 θ 的态密度主要集中在$\theta=0$处，即 $\theta_n+\theta_{n-1}=0$ 处．显然这种集中与切延时因子 m 无关，它是椭圆压缩因子 μ 的直接结果．

假设 α 是均匀分布的，即在$[-\pi/2,\pi/2]$范围内，$p_\alpha(\alpha)=1/\pi$．则很容易画出 $p(\theta)$的函数，如图 10 所示．

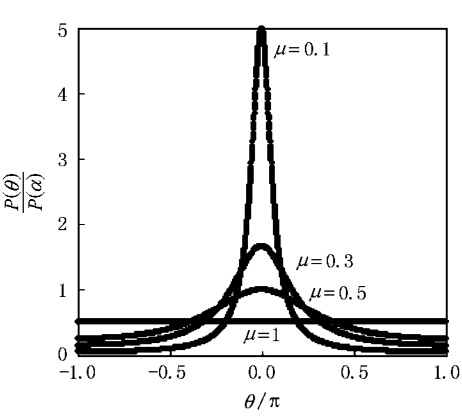

图 10　不同 μ 值，态密度的分布情况

从图 10 可以看出，随着 μ 的减少，在直线 $\theta_n+\theta_{n-1}=0$ 上态密度越来越大．由于态密度集中在直线 $\theta_n+\theta_{n-1}=0$ 上，因此相邻两位置 θ_n、θ_{n-1} 的相关性增强．这种现象对加密来说是极为不利的，相当于密码空间减少，使安全性降低．无论系统的延时因子 m 取何值，当 $\mu\to0$ 时，由于 $\theta_n+\theta_{n-1}\to0$，系统都变成了一维．因此在 μ 取值很小的情况下，企图利用增大延时因子 m 来提高加密强度的方法是不可取的．

相邻两位置的相关性计算可以使用线性相关公式．

令 $\boldsymbol{X}=(\theta_1,\theta_2,\cdots,\theta_n)$，$\boldsymbol{Y}=(\theta_2,\theta_2,\cdots,\theta_{n+1})$，

$$r_1=\left|\frac{\sum_{i=1}^{N}(X_i-\bar{X})(Y_i-\bar{Y})}{\sqrt{\sum_{i=1}^{N}(X_i-\bar{X})^2}\sqrt{\sum_{i=1}^{N}(Y_i-\bar{Y})^2}}\right|.$$

图 11 说明 $m=2$ 时，随着椭圆的压缩因子 μ 的减少，状态点越来越集中在 $\theta_n+\theta_{n-1}=0$ 的直线上，态密度也越来越尖锐．

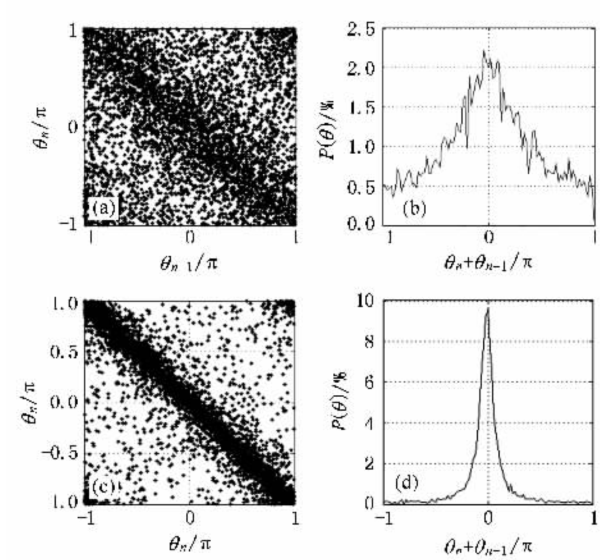

图 11　$m=2$，$\theta_0=0.01$，$\theta_1=0.467$，$\alpha_0=0.011$．(a)，(b)中 $\mu=0.5$；(c)，(d)中 $\mu=0.1$．(a)，(c)为 θ_n 与θ_{n-1}的关系；(b)，(d)为 $\theta_n+\theta_{n-1}$的态密度曲线

图 12 给出了不同的延时因子 m 下，相邻两次反射点的相关系数随 μ 的变化规律．可以看出，在 $m\geqslant2$ 时，他们的线性相关性，随 μ 的减少而增强．但对 $m=1$ 不存在这一规律，它在 $\mu=0.5$ 处取得最小值．这主要由于 $m=1$ 时存在吸引子，θ_n 和 θ_{n-1} 存在非线性关系，而且当 μ 变小时，曲线变得更弯曲，即非线性增强，线性相关性减弱，如图13所示，但

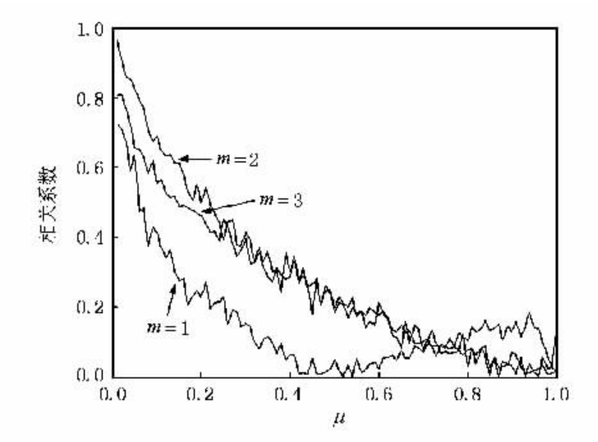

图 12 相邻两反射的相关系数与 μ 的关系

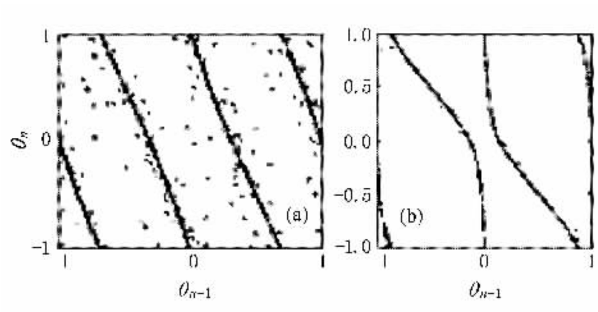

图 13 $m=1$ 时 θ_n 与 θ_{n-1} 的关系图 $\theta_0=0.01$，$\alpha_0=0.011$.(a) $\mu=0.8$；(b) $\mu=0.1$

中间部分的点数很稀少，两者共同作用使得 $m=1$ 时的相关系数呈现出如图 12 所示的曲线. 但无论如何只要 μ 很小，其线性相关性都很强.

3. 结　论

根据理论和数值实验，可以得出如下主要结论：

1. 本文提出了一种全新的研究方法 转移矩阵法，同时引进了椭圆角转换函数，推导出十分简单迭代公式，该公式特别适合理论分析.

2. 当切延时 1 个单位时，存在直线吸引子. 对椭圆和圆，它们的吸引子不相同. 椭圆的吸引子是 $\alpha_n+\theta_n=0$；而对于圆的吸引子是 $\alpha_n+\theta_n=C$（常数）.

3. 对任意的切延时因子 m，随着椭圆的压缩因子 μ 的减少，状态逐渐集中在 $\theta_n+\theta_{n-1}=0$ 的直线上，状态的线性相关性也增强，但对于 $m=1$ 的系统状态的线性相关性在 $\mu=0.5$ 时取得最小值. 因此如果使用该系统作为混沌加密，我们不能让 μ 取得太小. 当然，μ 也不能取得太大，否则混沌效果不好.

[1] Pecora L M，Carroll T L 1990 *Phys. Rev. Lett.* **64** 821

[2] Hayes S C，Grebogi C，Ott E 1993 *Phys. Rev. Lett.* **70** 3031

[3] Zhao G，Zheng D L 2002 *Acta Elec. Sin.* **30** 536 (in Chinese)［赵耿、郑德玲 2002 电子学报 **30** 536］

[4] Sheng L Y，Sun K H，Li C B 2004 *Acta Phys. Sin.* **53** 2871 (in Chinese)［盛利元、孙克辉、李传兵 2004 物理学报 **53** 2871］

[5] Sheng L Y，Cao L L，Sun K H，Wen J 2005 *Acta Phys. Sin.* **54** 4031 (in Chinese)［盛利元、曹利凌、孙克辉、闻　姜 2005 物理学报 **54** 4031］

[6] Sheng L Y，Jia W Y 2005 *Acta Phys. Sin.* **54** 5574 (in Chinese)［盛利元、贾伟尧 2005 物理学报 **54** 5574］

[7] Sheng L Y，Li G Q，Li Z W 2006 *Acta Phys. Sin.* **55** 5700 (in Chinese)［盛利元、李更强、李志炜 2006 物理学报 **55** 5700］

[8] Sano M，Sawada Y 1985 *Phys. Rev. Lett.* **55** 1082

[9] Eckmann J P，Ruelle D 1985 *Rev. Mod. Phys.* **57** 617

Study of attractor based on tangent-delay for elliptic reflecting cavity *

Tan Si-Ting† He Yi Sheng Li-Yuan

(*School of Physics Science and Technology*, *Central South University*, *Changsha* 410083, *China*)

(Received 2 October 2007; revised manuscript received 26 February 2008)

Abstract

By introducing the conversion function on ellipse angle, we use the method of shift matrix to achieve the simplification of ellipse problem. A very simple iterative formula is deduced on the tangent-delay for elliptic reflection, which is very useful for theoretical analysis. There exits a chaotic attractor when tangent delays one unit in TD-ERCS. The origin of the attractor and its stability are analyzed in theory. We find that the attractors in the circular and the elliptic cases are not entirely the same; the ellipse has two immobile lines, but only one of them is steady. We also find that, with the decrease of ellipse compression factor μ, the correlation of nearby iterative data is strengthened when the tangent-delay factor m is arbitrary. It means that in using the system for cryptography, the ellipse compression factor μ can not be too small, and the chaos system requires that it should not be too big, otherwise the degree of safety will be reduced.

Keywords: chaos, tangent-delay, TD-ERCS, attractor

PACC: 0545

---

* Project supported by the National Natural Science Foundation of China (Grant No. 60672041).

† E-mail: tansting@mail.csu.edu.cn