

级联混沌及其动力学特性研究*

王光义[†] 袁方

(杭州电子科技大学电子信息学院, 杭州 310018)

(2012年7月21日收到; 2012年8月18日收到修改稿)

初值敏感性是混沌的本质, 混沌的随机性来源于其对初始条件的高度敏感性, 而 Lyapunov 指数又是这种初值敏感性的一种度量. 本文的研究发现, 混沌系统的级联可明显提高级联混沌的 Lyapunov 指数, 改善其动力学特性. 因此, 本文研究了混沌系统的级联和级联混沌对动力学特性的影响, 提出了混沌系统级联的定义及条件, 从理论上证明了级联混沌的 Lyapunov 指数为各个级联子系统 Lyapunov 指数之和; 适当的级联可增加系统参数、扩展混沌映射和满映射的参数区间, 由此可提高混沌映射的初值敏感性和混沌伪随机序列的安全性. 以 Logistic 映射、Cubic 映射和 Tent 映射为例, 研究了 Logistic-Logistic 级联、Logistic-Cubic 级联和 Logistic-Tent 级联的动力学特性, 验证了级联混沌动力学性能的改善. 级联混沌可作为伪随机数发生器的随机信号源, 用以产生初值敏感性更高、安全性更好的伪随机序列.

关键词: 混沌, 级联, 离散映射, Lyapunov 指数

PACS: 05.45.-a, 05.45.Ac, 05.45.Xt

DOI: 10.7498/aps.62.020506

1 引言

伪随机序列在数字通信、密码系统、计算机仿真等领域有着广泛的应用. 一个伪随机序列发生器包括随机信号源(种)和一系列的量化及其实现技术, 其中良好的随机信号源是伪随机序列设计的关键问题. 混沌与传统密码学之间存在着一种自然的联系, 混沌动力学特性基本对应着高强度密码系统的某些安全特征, 以混沌作为随机信号源为伪随机序列发生器的设计提供了一种新的途径.

一般而言, 对混沌伪随机序列或混沌系统的要求是随机性好、安全性高. 混沌信号的随机性依赖于混沌的初值敏感性, 这是混沌的本质^[1]. 虽然目前文献中未对混沌初值敏感性的度量做出明显的说明, 但根据 Lyapunov 指数的定义我们完全有理由说 Lyapunov 指数就是初值敏感性的一种度量, 或可直接说 Lyapunov 指数越大, 表明系统对初值越敏感. 因此, 提高混沌系统的 Lyapunov 指数是改善其伪随机序列随机性的一种直接方法. 而混沌序

列的安全性则主要依赖于由系统初值和系统参数构成的密钥空间的大小, 即保证出现混沌时的初值范围和参数范围的大小.

利用连续和离散混沌系统进行伪随机序列发生器的设计已有不少研究^[2-5]. 连续混沌的数学模型为多变量耦合的微分方程组, 其系统参数和初始条件较多, 产生伪随机序列的密钥空间较大, 但由于其算法复杂导致运算速率较慢, 产生的序列码率较低. 而离散混沌由于算法简单使其运算速率快、序列码率高, 且其序列的复杂度好^[6], 因此目前混沌应用中首选离散混沌产生伪随机序列^[7-10], 应用最多的是 Logistic 映射、Tent 映射(分段线性映射)及其他的改进形式, 并且目前对此类离散映射仍做持续的研究^[11-19]. 但离散系统缺点是 Lyapunov 指数小、初值条件和系统参数较少, 其密钥空间较小从而导致序列的安全性降低.

为了提高离散混沌的随机性和安全性, 即提高混沌系统的 Lyapunov 指数和混沌映射参数区间, 本文提出了离散混沌的一种级联方案. 在定义混沌级联之后给出了级联混沌可提高其 Lyapunov 指

* 国家自然科学基金(批准号: 60971046)资助的课题.

[†] 通讯作者. E-mail: wanggyi@163.com

数的理论证明;以最常用的 Logistic 映射、Cubic 映射和 Tent 映射为例构成 Logistic-Logistic (L-L) 级联、Logistic-Cubic (L-C) 级联和 Logistic-Tent (L-T) 级联混沌系统,详细研究了级联对动力学性能改善. 本文的研究结果表明,利用级联混沌的良好动力学特性可产生性能更为优良的伪随机序列而应用于混沌保密通信或信息加密之中.

2 离散混沌系统的级联

2.1 离散混沌级联

定义 对于两个不同的离散混沌子系统 $f_1(x_n)$ 和 $f_2(x_n)$, $x \in D$, $f_1(x) \in D_1$, $f_2(x) \in D_2$, $n = 0, 1, 2, 3, \dots$. 如果满足 $D_1 = D_2 = D$, 即两个混沌映射的值域相同, 两个子系统 1、2 可构成一个新的级联系统

$$x_{n+1} = f_s(x_n) = f_2(f_1(x_n)). \quad (1)$$

级联的本质是, 一定的初值经系统 1 迭代后的输出作为系统 2 的迭代输入, 而经系统 2 迭代后的输出又作为系统 1 的迭代输入, 从而形成一个在两子系统之间的循环迭代, 如图 1 所示. 把两个或多个混沌系统级联之后形成的混沌称之为级联混沌.

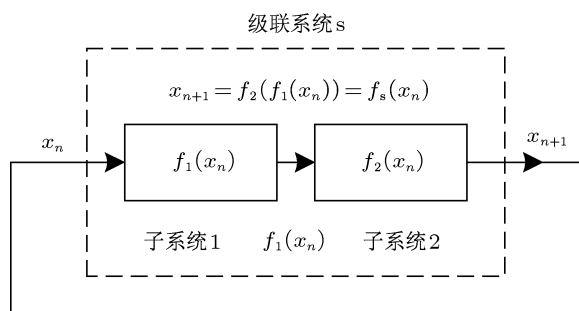


图 1 两个混沌系统级联原理图

如果 k 个混沌系统的迭代值域相同, 可由两个系统的级联推广到 k 个系统的级联

$$x_{n+1} = f_s(x_n) = f_k(f_{k-1}(\dots f_1(x_n))), \quad (2)$$

其中 $f_1(x_n), f_2(x_n), \dots, f_k(x_n)$ 为 k 个子系统, $x \in D$, $f_1(x) \in D_1, f_2(x) \in D_2, \dots, f_k(x) \in D_k$, 且 $D_1 = D_2 = \dots = D_k = D$. 也可扩展到一个系统自身的 m 次级联

$$x_{n+1} = f(f(\dots f(x_n))) = f^m(x_n). \quad (3)$$

定理 1 只有各个子系统的迭代值域 (或定义域) 相同才能进行级联.

如果各个子系统的迭代值域相同, 则它们在各自允许的值域内进行迭代; 如果各个子系统中只要一个系统其迭代值域不同, 则其迭代值会超出其他子系统的定义域, 或其他子系统的迭代值超出该子系统的定义域, 使得迭代无法进行.

2.2 级联混沌系统对动力学特性的改善

定理 2 假定子系统 $f_1(x_n), f_2(x_n), \dots, f_k(x_n)$ 可构成一个级联系统 $f_k(f_{k-1}(\dots f_1(x_n)))$, 如果各个子系统均是混沌的, 则它们的级联系统一定是混沌的, 且级联系统的 Lyapunov 指数等于各个子系统 Lyapunov 指数之和.

证明 级联系统 $f_k(f_{k-1}(\dots f_1(x_n)))$ 的 Lyapunov 指数为

$$\begin{aligned} LE_s &= \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |[f_k(f_{k-1}(\dots f_1(x_i)))]'| \\ &= \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f_1'(x_i) \cdot f_2'(f_1(x_i)) \dots f_k'(f_{k-1}(\dots f_1(x_i)))| \\ &= \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} (\ln |f_1'(x_i)| + \ln |f_2'(f_1(x_i))| \dots + \ln |f_k'(f_{k-1}(\dots f_1(x_i)))|) \\ &= \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f_1'(x_i)| + \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f_2'(f_1(x_i))| \\ &\quad + \dots + \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f_k'(f_{k-1}(\dots f_1(x_i)))| \\ &= LE_1 + \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f_2'(x_{2i})| \\ &\quad + \dots + \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f_k'(x_{ki})|, \end{aligned} \quad (4)$$

LE_1 为子系统 $f_1(x_n)$ 的 Lyapunov 指数, 式中其他量为

$$x_2 = f_1(x_1), \dots, x_{k-1} = f_{k-2}(\dots f_1(x_1)),$$

$$x_k = f_{k-1}(\dots f_1(x_1)), \quad (5)$$

$$f_2'(x_2) = \frac{df_2}{dx_2}, \dots, f_{k-1}' = \frac{df_{k-1}}{dx_{k-1}},$$

$$f_k' = \frac{df_k}{dx_k}. \quad (6)$$

对于一维离散混沌映射 $f_1(x_n), f_2(x_n), \dots, f_k(x_n)$, 当 $f_1(x), f_2(x) \dots f_k(x) \in D, x \in D$, 其 Lyapunov

Lyapunov 指数满足

$$\begin{aligned} LE_1 &= \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'_1(x_i)| > 0, \\ LE_2 &= \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'_2(x_i)| > 0, \\ &\dots\dots \\ LE_k &= \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'_k(x_i)| > 0. \end{aligned} \tag{7}$$

由于级联系统中同样满足 $f_1(x_i), f_2(f_1(x_i)), \dots, f_{k-1}(\dots f_1(x_i)) \in D$, 与 (7) 式中的 x_i 处于同一迭代值域, $i = 1, 2, 3, \dots, n$. 因此 (4) 式中各项必满足

$$\begin{aligned} &\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'_2(f_1(x_i))| \\ &= \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'_2(x_{2i})| = LE_2 > 0 \\ &\dots\dots \\ &\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'_k(f_{k-1}(\dots f_1(x_i)))| \\ &= \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'_k(x_{ki})| = LE_k > 0. \end{aligned} \tag{8}$$

根据 (4), (7) 和 (8) 式, (4) 式中 Lyapunov 指数各相加项均大于零, 且

$$LE_s = LE_1 + LE_2 + \dots + LE_k, \tag{9}$$

因此级联系统不仅是混沌的, 其 Lyapunov 指数远大于任意子系统的 Lyapunov 指数, 且等于各子系统 Lyapunov 指数之和.

混沌的本质是其对初始条件的高度敏感性^[1]. 在实际中由于受到测量精度的限制其初始条件无法绝对精确确定, 因而带来混沌状态长时间演化后的随机性和不可预测性, 而 Lyapunov 指数正是定量描述混沌初值敏感性的一个重要参数. 根据定理 2, 混沌系统的级联可以提高 Lyapunov 指数, 因此系统的级联是一种提高混沌系统初值敏感性, 即改善系统随机性或复杂性的一种简单有用的方法.

3 L-L 级联

把两个 Logistic 映射的级联称之为 L-L 级联. 著名的 Logistic 映射为

$$x_{n+1} = \mu x_n(1 - x_n), \tag{10}$$

$\mu \in [0, 4], x \in [0, 1]$. 由于其结构简单、行为复杂而得到了广泛的研究和应用. 但 Logistic 系统混沌映射范围小, 只有 $\mu = 4$ 时才是单位区间 $[0, 1]$ 上的

满映射且表现出较强的混沌特性, 如图 2(a) 所示. 映射范围较小的混沌映射在数字系统中量化时各迭代值之间更加相近, 更容易出现短周期和动力学退化. 为了改善 Logistic 映射的动力学特性, 对其进行级联并观察动力学性能的改善情况.

两个参数分别为 μ_1 和 μ_2 的 Logistic 映射的级联可表示为

$$x_{n+1} = \mu_1 [\mu_2 x_n(1 - x_n)] \{1 - [\mu_2 x_n(1 - x_n)]\}, \tag{11}$$

式中 $\mu_1, \mu_2 \in [0, 4], x \in [0, 1]$. 为扩展满映射区间和增强混沌特性, 令 $\mu_1 = 4, \mu_2$ 作为分岔参数, L-L 级联系统的分岔图和 Lyapunov 指数谱如图 2(b), (c) 所示. 以下分析说明级联系统明显改善了其动力学特性.

1) 混沌映射参数范围扩大: 比较图 2(a), (b) 看出, L-L 级联系统混沌映射参数范围大约扩展为 $[1.53, 4]$, 除去其间的三个明显的周期窗口后, 混沌映射参数范围约为 2.17, 约占整个参数范围 $\mu \in [0, 4]$ 的 54%, 是 Logistic 混沌映射参数范围 0.37 的 5.86 倍. 如果利用 L-L 级联系统产生伪随机序列对信息进行加密, 必使其工作于混沌映射状态, 较大的混沌映射参数范围提供了较大的密钥空间 (以初值和系统参数作为密钥), 可增强破译的难度从而提高安全性, 因此级联系统在混沌应用中有重要意义.

2) 混沌满映射参数范围扩大: Logistic 映射只在单一参数点 $\mu = 4$ 时才是满映射, 见图 2(a), 而 L-L 级联映射的满映射范围约为 1.7, 见图 2(b). 与非满映射相比, 满映射对应着较强的混沌强度, 其迭代值区间大, 利用数字系统对其处理时占据的数字空间相对较大, 后面的迭代值不易近似到前面的迭代值上, 因而可扩展混沌数字序列的周期, 改善混沌序列的动力学退化, 这在混沌应用中也有重要的意义.

3) Lyapunov 指数成倍提高: 根据定理 2, 级联系统能够增大 Lyapunov 指数. 由图 2(c) 看出, 在混沌区 L-L 级联系统的 Lyapunov 指数普遍大于 Logistic 系统, 其中前者的最大 Lyapunov 指数为 1.3863, 是后者最大 Lyapunov 指数 0.6930 的 2 倍, 这也验证了定理 2 的正确性. Lyapunov 指数的提高将会增强其初值敏感性, 从本质上改善其动力学特性, 这对混沌应用具有重要意义.

为便于比较, L-L 级联系统和子系统的主要动力学特性在表 1 中列出.

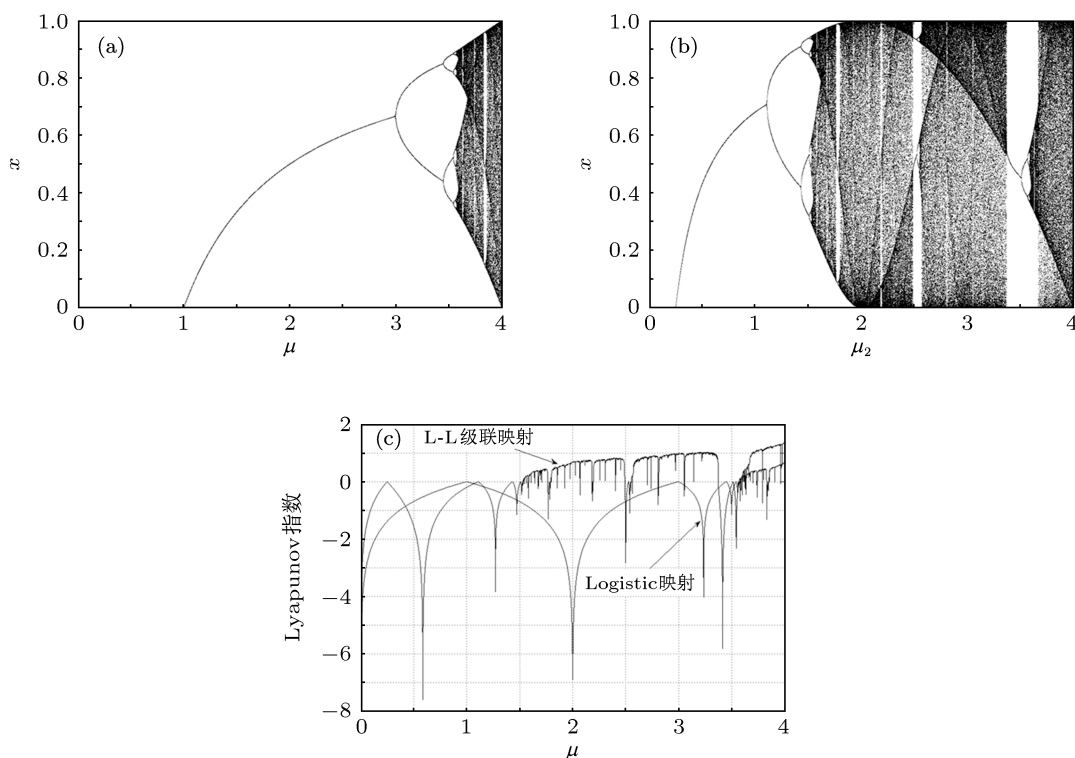


图2 Logistic映射和L-L级联映射的分岔图和Lyapunov指数谱 (a) Logistic映射分岔图; (b) L-L级联映射分岔图 ($\mu_1 = 4$); (c) L-L级联映射的Lyapunov指数谱 ($\mu_1 = 4$)

表1 Logistic映射和L-L级联映射特性比较

映射类型	映射参数区间	混沌映射参数区间	混沌满映射参数区间	最大Lyapunov指数
Logistic映射	$\mu \in [0, 4]$	$\Delta\mu = 0.37$	$\Delta\mu = 0, \mu = 4$	0.6930
L-L级联映射	$\mu_1, \mu_2 \in [0, 4]$	$\Delta\mu_2 = 2.17$	$\Delta\mu_2 = 1.7$	1.3863

4 L-C 级联

4.1 改进的 Cubic 映射及其基本动力学特性

把 Logistic 映射与一个改进的 Cubic 映射级联称之为 L-C 级联. Cubic^[18] 映射为

$$x_{n+1} = ax_n^3 - bx_n, \quad (12)$$

$b \in [0, 3], x \in [-c, c], c$ 与 a, b 有关, 只有 $b = 3$ 时才为满映射, 这也是 Cubic 映射的缺陷之一. Logistic 映射的满映射区域为 $[0, 1]$, 为了使得 Cubic 映射与 Logistic 映射能够级联, 即两者具有相同的映射区间, 对 Cubic 映射改进为

$$x_{n+1} = |x_n^3/a^2 - bx_n|, \quad (13)$$

式中 $b \in [0, 3], x \in [0, 2a]$, 取 $a = 0.5$ 可使其迭代范围与 Logistic 相同; b 为分岔参数, 当 $b \in [2.43, 3]$ 时系统处于混沌状态; $b = 3$ 时为满映射, 满映射区间 $[0, 2a]$, 如图 3(b) 所示. 对改进的 Cubic 映射的基本动力学特性分析如下.

由不动点方程

$$x = |x^3/a^2 - bx|, \quad (14)$$

解得不动点: $x_a = a\sqrt{b+1}, x_b = a\sqrt{b-1}, x_0 = 0$, 如图 3(a) 所示, 图中画出了 $a = 0.5, b = 1, b = 1.5$ 和 $b = 3$ 时三条曲线对应的不动点分布情况.

1) 当 $0 < b < 1$ 时, x_b 不存在, 只有 x_a 和 x_0 两个不动点, 分别对应图 3(a) 中 A 点和 O 点. 由于

$$\begin{aligned} f'(0) &= |3x^2/a^2 - b|_{x=0} = b < 1, \\ f'(A) &= |3x^2/a^2 - b|_{x=1} = 12 - b > 1, \end{aligned} \quad (15)$$

故不动点 O 是稳定的, 而不动点 A 在 $b \in [0, 3]$ 范围内始终保持 $f'(A) > 1$, 因而始终是不稳定的.

2) 当 $b = 1$ 时, $f'(0) = 1$, 因而发生跨临界分岔.

3) 当 $1 < b < 2$ 时, 有三个不动点, 见图 3(a) 中 $b = 1.5$ 时的 O, A', B' 点.

O 点的 $f'(0) = b > 1$, 故它不稳定. 对于 A' 点,

由于

$$f'(a\sqrt{b+1}) = |3x^2/a^2 - b|_{x=a\sqrt{b+1}} = |2b+3| > 1, \quad (16)$$

故它也不稳定. 而对于 B' 点, 因为 $f'(a\sqrt{b-1}) = |3x^2/a^2 - b|_{x=a\sqrt{b-1}} = |2b-3| < 1$, 故它是稳定的. 因此由初值 x_0 出发的迭代过程, 总是离开不动点 O, A' 而趋近于不动点 B' , 产生周期 1 现象.

4) 当 $b = 2$ 时, O 点的 $f'(0) = b > 1$ 仍不稳定, B' 点 $f'(a\sqrt{b-1}) = |2b-3| = 1$, 故发生叉型分岔.

5) 当 $2 < b < 2.235$ 时, 对于 O, A' 点它们仍是不稳定的. 对于 B' 点 $f'(a\sqrt{b-1}) = |2b-3| > 1$, 则 B' 点由稳定变为不稳定. 例如 $b = 2.21$ 时, 系统出

现两个值 x_1^* 和 x_2^* 的交替状态, 即周期 2 现象:

$$\begin{aligned} x_1^* &= |x_2^2/a^2 - bx_2|, \\ x_2^* &= |x_1^2/a^2 - bx_1|. \end{aligned} \quad (17)$$

当 $a = 0.5, b = 2.2$ 时, x 趋向于在 1.3801 和 2.1738 两个值上跳动.

6) 如果继续增加 b 值, 周期 2 将不稳定, 各自产生一对新的不动点即产生周期 4 现象. 这样的过程继续下去, 不断地出现倍周期分岔, 即周期 2^{n-1} 不稳定时分岔出周期 2^n , 当 $b \in (2.4, 3]$ 时出现混沌现象.

7) 当 $b > 3$ 时, 平衡点为 O, A'' 和 B'' 三点, 且总有 $f'(a\sqrt{b+1}) = |2b \pm 3| > 1$, 故系统不稳定. $a = 0.5, b = 3$ 时的吸引子和平衡点如图 3(a) 所示.

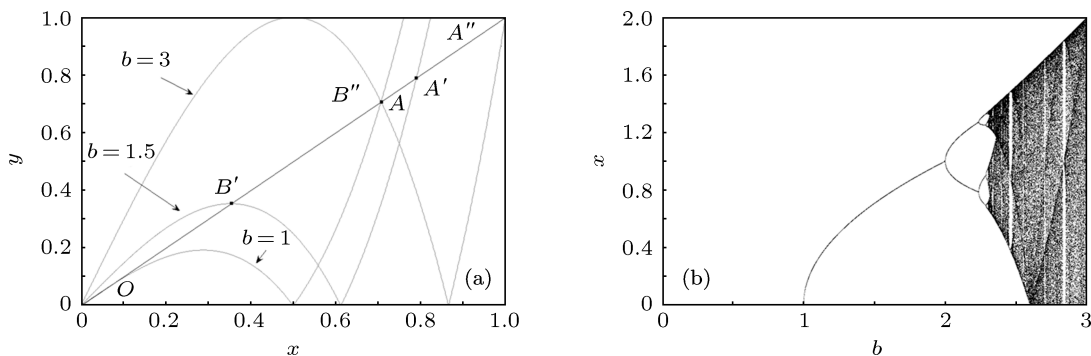


图 3 改进的 Cubic 映射不动点及分岔图 (a) 吸引子、不动点及随参数的变化; (b) 分岔图

4.2 L-C 级联

4.2.1 L-C 级联

虽然通过改进的 Cubic 映射可以将其映射范围限制在 $x \in [0, 2a]$, 但它和 Logistic 映射一样存在一些共性的缺陷:

1) 混沌映射分岔参数范围小: Logistic 映射约为 $\mu \in [3.57, 4]$, 即 μ 约在 0.43 的变化范围内出现混沌映射 (其中还包括周期 3 窗口), 改进的 Cubic 映射约 $b \in [2.41, 3]$, 即 b 约在 0.59 的变化范围内才出现混沌映射 (其中还包括一些小的周期窗口).

2) 只在一个参数点上出现满映射: Logistic 和改进的 Cubic 映射分别在 $\mu = 4$ 和 $b = 3$ 时才出现满映射.

3) Lyapunov 指数小: Logistic 和改进的 Cubic 映射最大 Lyapunov 指数分别为 0.6930 和 1.0984.

如果把两者级联, 上述缺陷会得到明显的改

善. 在改进的 Cubic 映射中取 $a = 0.5, b = 3$, 将其取值范围约束到与 Logistic 映射相同的取值范围 $x \in [0, 1]$ 且为满映射, 再把 Logistic 映射代入改进的 Cubic 映射之中, 就得到先进行 Logistic 迭代、后进行改进的 Cubic 迭代的级联系统:

$$\begin{aligned} x_{n+1} &= \left| \frac{[ux_n(1-x_n)]^3}{0.5^2} - 3 \times ux_n(1-x_n) \right| \\ &= \left| \frac{u^3 x_n^3 (1-x_n)^3}{0.25} - 3ux_n(1-x_n) \right|. \end{aligned} \quad (18)$$

4.2.2 L-C 级联系统的复杂动力学特性

与两个子系统相比级联系统有较复杂的动力学特性. 级联系统的映射函数为

$$y = \left| \frac{u^3 x^3 (1-x)^3}{0.25} - 3ux(1-x) \right|, \quad (19)$$

不动点随分岔参数 μ 的变化情况如图 4(a) 所示. 不动点为线段 OA 与各曲线的交点, 随着 μ 从

小到大的变化, 其不动点个数从 1 ($\mu = 0.5$) \rightarrow 2 ($\mu = 1.0, 2.0$) \rightarrow 3 ($\mu = 3.045$) \rightarrow 4 ($\mu = 3.6$) \rightarrow 5 ($\mu = 3.75$) \rightarrow 6 ($\mu = 4$), 其稳定性发生了非常复杂的变化并导致了非常复杂的分岔现象. 限于篇幅, 其稳定性的详细分析将另文研究.

级联系统的分岔图如图 4(b) 所示, 出现混沌的参数范围约为 [1.55, 4] (其间有几个小周期窗口), 比 Logistic 和改进 Cubic 映射的混沌参数区间 $\mu \in [3.57, 4]$, $b \in [2.41, 3]$ 大得多, 且满映射范围约为 [1.9, 4], 与两个子系统只在一个参数点满映射相比, 其动力性特性得到了显著的改善.

如图 4(c) 所示, 级联系统的 Lyapunov 指数明显大于 Logistic 子系统的指数. 计算表明, 级联系统的最大 Lyapunov 指数为 1.7011, 几乎是级联前两子系统 Lyapunov 指数 0.6930 和 1.0984 之和. 子系

统和级联系统性能的变化如表 2 所示.

5 L-T 级联

L-T 级联是指 Logistic 映射与 Tent 映射的级联. Tent 映射有多种形式 [4,8,19], 其一为

$$x_{n+1} = 1 - a|x_n - (1/a)|, \quad (20)$$

a 为参数, $a \in [0, 2]$. 图 5 示出了其分岔图、Lyapunov 指数谱和吸引子.

Tent 映射属于逐段线性混沌映射, 与 Logistic 映射相比它有均匀的不变分布, 但缺点是系统参数少, 映射区间小, 当且仅当 $a = 2$ 时才是一个单位区间 [0, 1] 上的满映射, 最大 Lyapunov 指数仅为 0.69265.

表 2 Logistic 映射、改进 Cubic 映射和 L-C 级联映射特性比较

映射类型	映射参数区间	混沌映射参数区间	混沌满映射参数区间	最大 Lyapunov 指数
Logistic 映射	$\mu \in [0, 4]$	$\Delta\mu = 0.37$	$\Delta\mu = 0, \mu = 4$	0.6930
改进 Cubic 映射	$b \in (0, 2]$	$\Delta b = 0.59$	$\Delta b = 0, b = 3$	1.0984
L-C 级联映射	$\mu \in [0, 4]$	$\Delta\mu = 2.45$	$\Delta\mu = 2.1$	1.7011

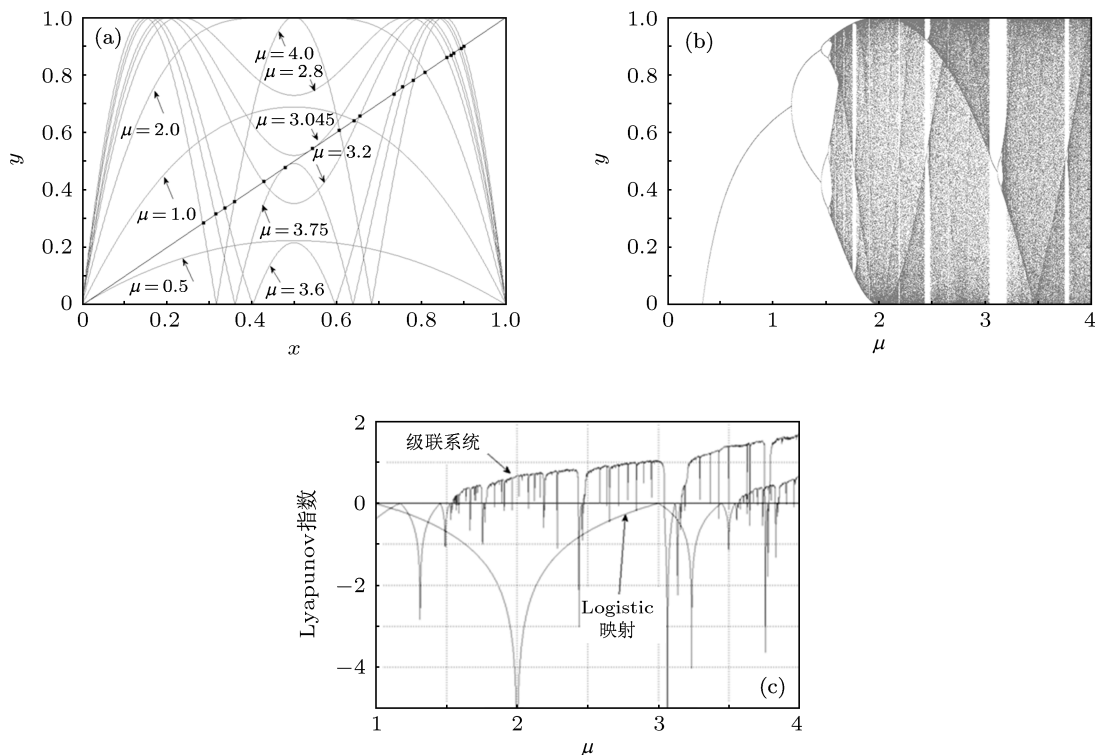


图 4 L-C 级联系统的吸引子、分岔图和 Lyapunov 指数谱 (a) L-C 级联系统的函数曲线及不动点; (b) L-C 级联系统分岔图; (c) Lyapunov 指数谱

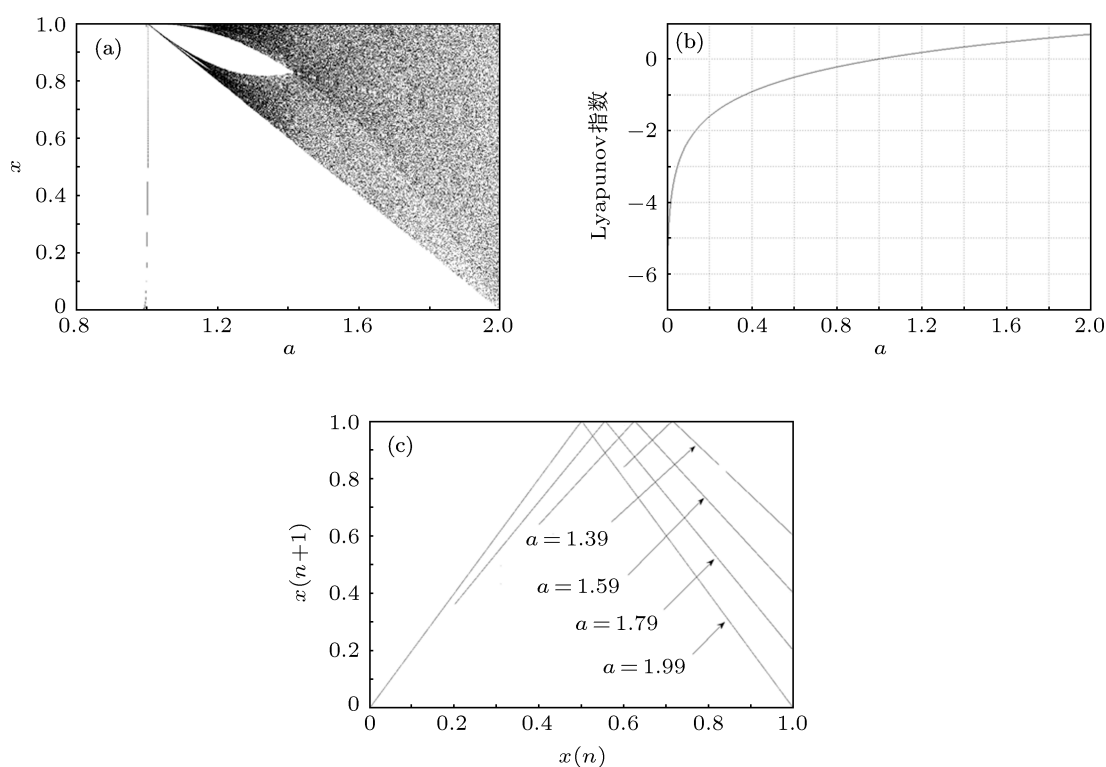


图5 Tent映射分岔图、Lyapunov指数谱和吸引子 (a)分岔图;(b)Lyapunov指数谱;(c)吸引子

把 Logistic 映射与 Tent 映射级联,得级联系统:

$$x_{n+1} = 1 - a|\mu x_n(1 - x_n) - (1/a)|. \quad (21)$$

该级联系统的吸引子、分岔图和 Lyapunov 指数谱如图 6 所示,由图 6 可获得级联前后各系统的相关动力学特性. L-T 级联映射的动力学特性有如下优势:

1) Logistic 映射和 Tent 映射分别在 $\mu = 4$ 和 $a = 2$ 时才是区间 $[0, 1]$ 上的满映射,从而具有足够强的混沌特性. 而 L-T 映射对参数 a 满映射区间约为 $a_1 + a_2 + a_3 \approx 0.45 + 0.29 + 0.2 = 0.94$ (图 6(a)), 即约在 $1/2$ 参数区间 ($a \in [0, 2]$) 上具有足够强的混沌特性; 参数 μ 满映射区间约为 $\mu_1 + \mu_2 + \mu_3 \approx 0.26 + 0.60 + 0.45 = 1.31$ (图 6(b)), 即

约在 $1/3$ 参数区间 ($\mu \in [0, 4]$) 上具有足够强的混沌特性,与 Logistic 和 Tent 映射相比优势明显.

2) Logistic 映射出现混沌的 μ 参数范围约为 0.43, 而 L-T 级联系统出现混沌的 μ 参数区间约为 1.66, 后者约为前者的 3.86 倍; Tent 映射出现混沌的 a 参数范围约为 0.8, 而 L-T 级联系统出现混沌的 a 参数区间约为 1.1, 后者约为前者的 1.38 倍.

3) Logistic 映射和 Tent 映射的最大 Lyapunov 指数分别为 0.6930 和 0.6926, 而 L-T 级联系统分别随参数 μ 和 a 变化时的最大 Lyapunov 指数为 1.2522 和 1.2937, 后者分别是前者的 1.80 和 1.87 倍. 为便于比较,把 Logistic 映射、Tent 映射和 L-T 级联映射的相关动力学特性列入表 3.

表3 Logistic映射、Tent映射和L-T级联映射特性比较

映射类型	映射参数区间	混沌映射参数区间	混沌满映射参数区间	最大 Lyapunov 指数
Logistic 映射	$\mu \in [0, 4]$	$\Delta\mu = 0.37$	$\Delta\mu = 0, \mu = 4$	0.6930
Tent 映射	$a \in (0, 2]$	$\Delta a = 1.00$	$\Delta a = 0, a = 2$	0.6926
L-T 级联映射	$\mu \in [0, 4]$	$\Delta\mu = 1.66$	$\Delta\mu = 1.31$	1.2522
L-T 级联映射	$a \in (0, 2]$	$\Delta a = 1.1$	$\Delta a = 0.94$	1.2937

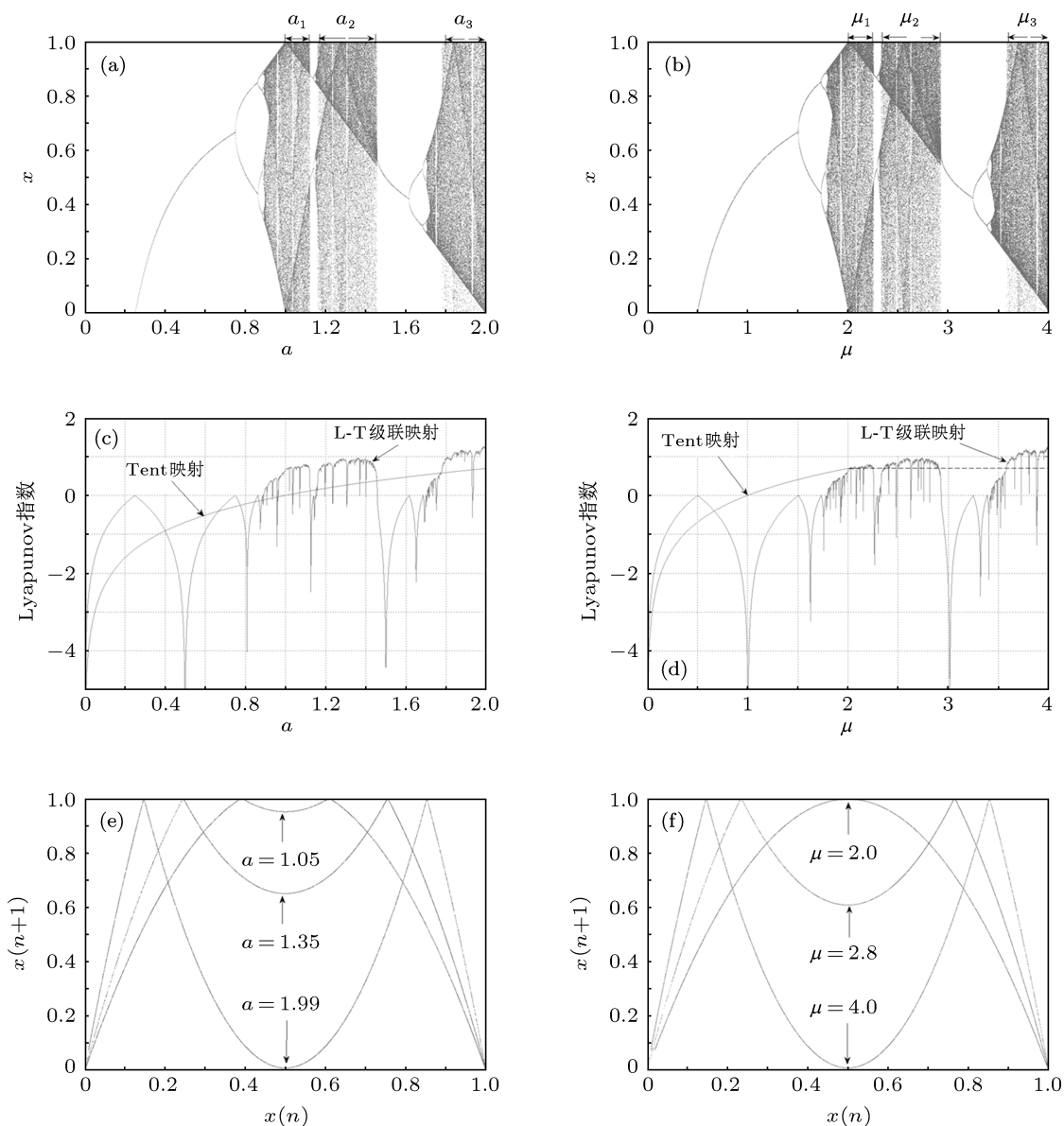


图6 L-T级联映射的分岔图、Lyapunov 指数谱和吸引子 (a) x 随 a 变化的分岔图; (b) x 随 μ 变化的分岔图; (c) 随 a 变化的 Lyapunov 指数谱; (d) 随 μ 变化的 Lyapunov 指数谱; (e) 随 a 变化的吸引子; (f) 随 μ 变化的吸引子

6 结论

本文研究了离散混沌系统的级联, 包括混沌系统级联的定义及其条件、级联混沌系统对动力学特性的改善. 理论分析和仿真验证表明, 级联混沌系统的 Lyapunov 指数为各子系统 Lyapunov 指数之和, 从而提高了混沌的初值敏感性, 改善了混沌信号的随机性; 两个子系统的适当级联可增加系统参

数、扩展混沌映射或满映射的参数区间, 从而增强混沌特性、提高混沌伪随机序列的密钥空间. 鉴于级联混沌系统所带来的动力学特性的改善, 可将其作为随机信号源应用于伪随机数发生器的设计之中, 以产生随机性好、安全性高的伪随机序列, 在混沌保密通信、信息加密等领域将有良好的应用潜力.

- [1] Lorenz E N 1993 *The Essence of Chaos* (Washington: The University of Washington Press) p25
- [2] Persohn K J, Povinelli R J 2012 *Chaos, Solitons & Fractals* **45** 238
- [3] Chen S L, Hwang T T, Lin W W 2010 *IEEE Trans. Circ. Syst.-II: Express Briefs* **57** 996
- [4] Jongsig Bae, Changha Hwang, Doobae Jun 2012 *Statistics and Probability Letters* **82** 1021
- [5] Maier M P S, Peacock-López E 2010 *Physics Letters A* **374** 1028
- [6] Sun K H, He S B, Yin L Z, A Di Li D L K 2012 *Acta Phys. Sin.* **61** 130507 (in Chinese) [孙克辉, 贺少波, 尹林子, 阿地力·多力坤 2012 物理学报 **61** 130507]
- [7] Narendra Singh, Aloka Sinha 2010 *Optics and Lasers in Engineering* **48** 398
- [8] Martínez-Ñonthe J A, Castañeda-Solís A, Díaz-Méndez A, Cruz-Irisson M, Vázquez-Medina R 2012 *Microelectronic Engineering* **90** 168
- [9] Jovic B, Unsworth C P 2010 *Electronics Letters* **46** 1
- [10] Feng C F, Xu X J, Wu Z X Wang Y H 2008 *Chinese Physics B* **17** 1674
- [11] Young R M B, Read P L 2008 *Physica D* **237** 2251
- [12] Thomas Curtright, Andrzej Veitia 2011 *Physics Letters A* **375** 276
- [13] Levinsohn E A, Mendoza S A, Peacock-López E 2012 *Chaos, Solitons & Fractals* **45** 426
- [14] Wang X Y, Wang M J 2008 *Acta Phys. Sin.* **57** 731 [王兴元, 王明军 2008 物理学报 **57** 731]
- [15] Meng J D, Bao B C, Xu Q 2011 *Acta Phys. Sin.* **60** 10504 [孟继德, 包伯成, 徐强 2011 物理学报 **60** 10504]
- [16] Wang G Y, Yu J B, Gu T X 2011 *Acta Phys. Sin.* **50** 2307 [王改云, 虞厥邦, 古天祥 2011 物理学报 **50** 2307]
- [17] Bao B C, Kang Z S, Xu J P 2009 *Acta Phys. Sin.* **58** 1420 [包伯成, 康祝圣, 许建平, 胡文 2009 物理学报 **58** 1420]
- [18] Wei Y, Nan J, Tang G 2011 *Czechoslovak Mathematical Journal* **61** 1023
- [19] Ben Futter, Viktor Avrutin, Michael Schanz 2012 *Chaos, Solitons & Fractals* **45** 465

Cascade chaos and its dynamic characteristics*

Wang Guang-Yi[†] Yuan Fang

(School of Electronics and Information, Hangzhou Dianzi University, Hangzhou 310018, China)

(Received 21 July 2012; revised manuscript received 18 August 2012)

Abstract

The dependence of sensitivity on initial conditions is the essence of chaos. And the randomness of chaos originates from the high sensitivity to initial values, which is measured by the Lyapunov exponents. It is found in this paper that the cascade of chaotic systems can considerably improve the Lyapunov exponents of cascade chaos and other dynamic properties. Therefore, in this paper, we study the cascade of chaotic systems and the influence on dynamic performances of the cascade chaos, and we present the definition and conditions of chaotic system cascade. It is proved in theory that the Lyapunov exponent of cascade chaos system is a sum of Lyapunov exponents of cascade subsystems. Appropriate cascade for chaotic systems can increase system parameters and expand parameter regions of chaos mapping and full mapping, thereby enhancing initial condition sensitivity of chaotic map and security of chaotic pseudo-random sequences. For logistic map, cubic map and tent map, the dynamic characteristics of logistic-logistic, logistic-cubic and logistic-tent cascade are investigated in detail, verifying the improvements on dynamic characteristics of cascade chaos systems. The proposed chaotic cascade system can be used to generate better pseudo-random sequences for initial condition sensitivity and security.

Keywords: chaos, cascade, discrete map, Lyapunov exponent

PACS: 05.45.-a, 05.45.Ac, 05.45.Xt

DOI: 10.7498/aps.62.020506

* Project supported by the National Natural Science Foundation of China (Grant No. 60971046).

[†] Corresponding author. E-mail: wanggyi@163.com