

离散动力系统无退化-配置 N 个正Lyapunov指数

赵耿^{①②} 李红^{*①②} 马英杰^② 秦晓宏^②

^①(西安电子科技大学 西安 710071)

^②(北京电子科技学院 北京 100070)

摘要: 针对离散时间混沌动力学系统, 该文提出一种基于矩阵特征值以及特征向量配置Lyapunov指数为正的新算法。计算离散受控矩阵的特征值以及特征向量, 设计一类具有正Lyapunov指数的通用控制器, 理论证明系统轨道的有界性和Lyapunov指数的有限性。对线性反馈算子以及微扰反馈算子进行数值仿真分析, 验证了算法的正确性、通用性和有效性。性能评估表明, 与Chen-Lai算法相比, 该方法可以构建较低计算复杂度的混沌系统, 并且运行时间较短, 其输出序列也具有更强的随机性, 实现了无退化、无兼并的离散混沌系统。

关键词: 混沌系统; 无退化; Lyapunov指数; 矩阵特征值; 线性反馈算子; 微扰反馈算子

中图分类号: TP309.7

文献标识码: A

文章编号: 1009-5896(2019)09-2280-07

DOI: [10.11999/JEIT180925](https://doi.org/10.11999/JEIT180925)

Discrete Dynamic System without Degradation -configure N Positive Lyapunov Exponents

ZHAO Geng^{①②} LI Hong^{①②} MA Yingjie^② QIN Xiaohong^②

^①(Xidian University, Xi'an 710071, China)

^②(Beijing Electronic Science and Technology Institute, Beijing 100070, China)

Abstract: Considering discrete-time chaotic dynamics systems, a new algorithm is proposed which is based on matrix eigenvalues and eigenvectors to configure Lyapunov exponents to be positive. The eigenvalues and eigenvectors of the discrete controlled matrix are calculated to design a general controller with positive Lyapunov exponents. The theory proves the boundedness of the system orbit and the finiteness of the Lyapunov exponents. The numerical simulation analysis of the linear feedback operator and the perturbation feedback operator verifies the correctness, versatility and effectiveness of the algorithm. Performance evaluations show that, compared with Chen-Lai methods, the proposed method can construct chaotic system with lower computation complexity and the running time is shorter and the outputs demonstrate strong randomness. Thus, a discrete chaotic system with no degradation and no merger is realized.

Key words: Chaotic system; No-degenerate; Lyapunov exponent; Matrix eigenvalue; Linear feedback operator; Perturbation feedback operator

1 引言

从一开始人们对混沌的陌生, 到慢慢对混沌进行深入了解以及在生活中应用的需要, 人们渐渐领悟到系统混沌运动的重要性, 并开始重视如何把混沌运动变为周期运动的问题。考虑到混沌的研究价值, 人们应该试图产生该混沌行为, 并使之混沌效应增强, 真正把混沌性能发挥到极致。而这种手段就被称为混沌的反控制, 所谓反控制就是利用

逆向思维, 增强行为运动效应, 使得混沌性能得以增强, 使系统完全处于混沌的状态。混沌反控制^[1-3]也是一个重要的和富有创新性的研究方向, 陈关荣等人^[1-3]首先给出了一般性方法和严格的数学理论, 为离散系统及其混沌控制与反控制领域提供了奠基性和开创性的基础。

李雅普诺夫(Lyapunov)指数是一个数值特征, 表示在维数不定的空间内, 相邻运动轨道之间的平均指数的一种发散强度, 它对于确定系统是否具有混沌行为起着关键性的作用。非混沌系统固定点吸引子具有非正的Lyapunov指数, 而非混沌周期或极限环吸引子Lyapunov指数为正值, 因此混沌系统至少具有一个Lyapunov指数是正值。

收稿日期: 2018-09-30; 改回日期: 2019-02-21; 网络出版: 2019-03-15

*通信作者: 李红 1940571437@qq.com

基金项目: 国家自然科学基金(61772047)

Foundation Item: The National Natural Science Foundation of China(61772047)

对于离散系统反馈混沌化的问题, 目前具有鲜明成果, 并大量被研究者引用的是由陈关荣和赖德健提出的Chen-Lai算法^[3], 以及汪小帆和陈关荣提出的Wang-Chen算法^[4], 这两个方法在一定程度上解决了离散系统反馈混沌化问题, 同时也为离散系统开辟了一个新的天地。目前对混沌研究的主要方向就是抑制其行为的退化, 在数字域中的退化问题^[5-7]首先表现在正李氏指数在系统发生行为改变时会发生简并的情况, 产生的结果是正李氏指数在随着运动轨迹的汇聚转化为负的李氏指数, 对于动力系统进行的反控制, 可以从Lyapunov指数兼并的角度进行研究混沌无退化的问题, 该方法能从根本上增强混沌的行为效应以及混沌性能。其核心的方法, 都是通过添加到受控系统中某种控制变量来改变受控系统的本身的雅可比矩阵, 从而达到改变李氏指数数值的目的, 算法的主要区别在于受控系统的初始形态和该系统的最终状态是不一样的。本质上采用混沌控制与反控制的方法能够将一个普通系统转化为具有混沌行为的系统, 把一个超混沌系统转化为简单的混沌系统, 以及把简单的混沌系统转化成超混沌, 把简单混沌系统转化成具有稳定不动点或者稳定周期态的系统等^[8-10]。

文献^[3]给出了一种算法——Chen-Lai算法, 由陈关荣和赖德健提出, 该算法通过在受控系统的基础上加入控制矩阵, 改变该受控系统的雅可比矩阵, 该算法实现的目标就是使受控系统的Lyapunov指数数值全部大于一个给定的正常数 C , 并且可以产生Devaney意义下的混沌以及Li-Yorke^[9]意义下的混沌。文献^[4]给出了汪小帆和陈关荣提出的Wang-Chen算法, 该算法主要是引入线性反馈控制, 为了使得系统在相空间内有界, 对整个系统采用取模的方法, 同样也能达到Chen-Lai算法一样的目标, 通过加入一个微小的控制变量就可以使得混沌效应得到显著的增强。本文主要从配置离散系统的Lyapunov指数的角度出发, 在Chen-Lai算法的启示下, 提出了一种新的Lyapunov指数配置方法, 方法的核心理论是通过引入反馈矩阵, 改变受控系统雅可比矩阵的子矩阵, 通过每个子矩阵的特征值与相对应的特征向量来改变李氏指数大小, 使得正Lyapunov指数的个数达到 $L = n$, 根据混沌吸引子与李氏指数的关系, 即具有混沌吸引子的系统, 其Lyapunov指数一定包含1个或多个正的Lyapunov指数, 从而达到系统无退化的目的, 即配置所有Lyapunov指数, 使其每个数值都可以大于给定的任意常数 $C_i (i = 1, 2, \dots, n)$ 。

以下是本文工作的几个方面贡献:

- (1) 基于受控系统矩阵特征值的配置原理, 提出配置Lyapunov指数全部为正的算法;
- (2) 理论证明系统运行轨迹的有界性和Lyapunov指数的有限性;
- (3) 对于线性反馈算子以及微扰反馈算子进行数值仿真分析, 并与Chen-Lai算法进行比较, 验证了算法的正确性、通用性和有效性;
- (4) 进行性能的分析。

2 基于矩阵特征值配置Lyapunov指数为正

2.1 受控系统矩阵特征值配置原理

考虑 k 维非线性离散时间系统

$$x_{k+1} = \mathbf{A}x_k \quad (1)$$

式中, $x_k \in R^n$ 为系统的状态, $\mathbf{A}$ 为 k 维的控制矩阵。混沌反控制的核心思想是: 设计控制器 u_k 使得控制系统具有混沌性能, 即受控系统为全局有界并且具有正的Lyapunov指数, 并且满足常用的混沌定义(Devaney混沌定义或者Li-Yorke混沌定义)^[11-13]。

考虑简单的线性状态反馈

$$u_k = \mathbf{B}x_k \quad (2)$$

其中, $\mathbf{B} \in R^{k \times k}$ 为待定矩阵, 则受控系统为

$$x_{k+1} = \mathbf{A}x_k + \mathbf{B}x_k \quad (3)$$

受控系统式(3)的Jacobi矩阵为

$$\mathbf{J}_j(z) = \mathbf{A} + \mathbf{B} = \mathbf{J} \quad (4)$$

记

$$\begin{aligned} \mathbf{T}_k &= \mathbf{T}_k(x_0, x_1, \dots, x_k) \\ &= \mathbf{J}_k(x_k) \mathbf{J}_{k-1}(x_{k-1}) \cdots \mathbf{J}_1(x_1) \mathbf{J}_0(x_0) = \mathbf{J}^k \end{aligned} \quad (5)$$

并记

$$\sigma_i^j = u_i | \mathbf{T}_j^T \mathbf{T}_j | \quad (6)$$

为第 j 个乘积矩阵 $\mathbf{T}_j^T \mathbf{T}_j$ 的第 i 个特征值^[3], 亦即矩阵 $\mathbf{T}_j$ 的第 i 个奇异值的平方。

根据Lyapunov指数的定义^[3], 系统式(3)的第 i 个Lyapunov指数为

$$\text{LE}_i = \lim_{k \rightarrow \infty} \frac{1}{2k} \ln |u_i | \mathbf{T}_j^T \mathbf{T}_j |, \quad i = 1, 2, \dots, n \quad (7)$$

即 $\{\mathbf{T}_k\}$ 奇异值序列的极限^[4]。

假设现在的受控系统矩阵的特征值为 $\lambda_1, \lambda_2, \dots, \lambda_k$, 那么式(7)对应的Lyapunov指数分别为: $\text{LE}_1 = \ln |\lambda_1|, \text{LE}_2 = \ln |\lambda_2|, \dots, \text{LE}_k = \ln |\lambda_k|$ 。

目前需要解决的主要问题就是, 如何设计反馈增益矩阵 $\mathbf{B}$, 使得受控系统的Lyapunov指数全部有限, 并且全部为正, 即

$$\left. \begin{aligned} \text{LE}_i(x_0) &< \infty, \forall i \in \{1, 2, \dots, k\} \\ \text{LE}_i(x_0) &> c, \forall i \in \{1, 2, \dots, k\} \end{aligned} \right\} \quad (8)$$

其中, $c > 0$ 为预先给定的常数。

系统矩阵 $\mathbf{A}$ 的全部特征值按照绝对值大小排列为 $|\lambda_1| \geq |\lambda_2| \geq \dots \geq |\lambda_k|$, 且令 $\mathbf{A}\mathbf{x} = \lambda\mathbf{x}$, 其中 $\mathbf{x} \neq 0$ 是相应于特征值 λ 的特征向量。取

$$\mathbf{B} = \mathbf{z}\mathbf{z}^T \quad (9)$$

其中, $\mathbf{z} \in R^n$ 满足 $\mathbf{x}^T \mathbf{z} = e^c + N > 0$, $N = \varepsilon + \lambda_i$, $\varepsilon > 0$, $i = (1, 2, \dots, k)$, λ_i 为第 i 个特征值, $N > 0$ 为给定常数, 在式(9)中只有 $\mathbf{z}$ 是未知量, 解此方程即得 $\mathbf{z}$ 。虽然 $\mathbf{z}$ 的解不是唯一的, 但是任意一个 $\mathbf{z}$ 的解都能满足 $LE_i = \lim_{k \rightarrow \infty} \frac{1}{k} \ln \sigma_i[\mathbf{J}^k] > \ln(e^c + N) > c$, ($i = 1, 2, \dots, n$)。本文中的 $\mathbf{z}$ 是利用 MATLAB 编程得到的。按式(9)选取 $\mathbf{B}$, 则系统的 Lyapunov 指数就会满足式(8), 将会在第3节中证明这一点。

要想系统成为混沌系统, 还要求控制增益矩阵一致有界, 即 $\sup_{0 \leq k < \infty} \|\mathbf{B}\| \leq M < \infty$, 其中 M 为一常数, $\|\cdot\|$ 为谱范数, 即矩阵最大奇异值。参考文献[1-3]已经证明了该式可以满足的, 因此控制增益矩阵 $\mathbf{B}$ 一致有界, 只要受控矩阵 $\mathbf{A}$ 一致有界, 即存在常数 N , 使得 $\sup_{0 \leq k < \infty} \|\mathbf{A}\| \leq N < \infty$, 就能达到整个系统的矩阵保持一致有界。

为了更好地证明新算法可以配置正的 Lyapunov 指数, 需要引入几个线性代数的性质以及定理, 如下所示:

性质1 令 $\mathbf{A} \in M_n$, $\mathbf{B} \in M_n$ 为 n 阶矩阵, 其特征值分别为 λ_i, λ_j , ($0 < i, j < n$), 如果 $\mathbf{A}, \mathbf{B}$ 的特征向量都是 ξ , 则 $\mathbf{A} + \mathbf{B}$ 的特征值为 $\lambda_k = \lambda_i + \lambda_j$, ($0 < k < n$)。

性质2 令 $\mathbf{A} \in M_n$ 为 n 阶矩阵, 其特征值为 λ_i ($1 \leq i \leq n$), 则 $\mathbf{A}^k$ 的特征值为 λ_i^k ($1 \leq i \leq n$)。性质2表明矩阵幂的特征值与特征值的幂的关系, 其证明是容易的。事实上该引理是线性算子谱映射定理的特例。

性质3 令 $\mathbf{x}, \mathbf{y} \in R^n$ 为 n 维列向量, $\mathbf{A} \in M_n$ 为 n 阶矩阵, 其全部特征值为 $\lambda_1, \lambda_2, \dots, \lambda_n$, 而 $\mathbf{x}$ 是 $\mathbf{A}$ 相应于特征值 λ_1 的特征向量。则 $\mathbf{A} + \mathbf{x}\mathbf{y}^H$ 的全部特征值为 $\lambda_1 + \mathbf{y}^H \mathbf{x}, \lambda_2, \dots, \lambda_n$, H 表示取共轭转置[14]。

从性质3上可以看出, 可以通过引入反馈来改变系统的某个特征值, 并能改变成任意的数值。

性质4 令 $\mathbf{A} \in M_n$ 为 n 阶矩阵, 其特征值 $|\lambda_1| \geq |\lambda_2| \geq \dots \geq |\lambda_n|$, 其奇异值为 $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_n$ 。则 $|\lambda_1 \lambda_2 \dots \lambda_j| \leq \sigma_1 \sigma_2 \dots \sigma_j, \forall 1 \leq j \leq n$ [15]。

利用以上的性质, 能够得到定理1以及可以对其进行证明。

定理1 通过引入反馈变量, 并且严格指定某个变量反馈的形式如式(9), 则 n 维离散时间系统式(3)全部的 Lyapunov 指数满足

$$LE_i = \lim_{k \rightarrow \infty} \frac{1}{2k} \ln |u_i[\mathbf{T}_j^T \mathbf{T}_j]| > c, \quad k = 1, 2, \dots, n \quad (10)$$

证明 对于受控系统式(3), 根据式(9)选择反馈矩阵。根据 Lyapunov 指数的定义

$$\begin{aligned} LE_i &= \lim_{k \rightarrow \infty} \frac{1}{2k} \ln |u_i[\mathbf{T}_j^T \mathbf{T}_j]| \\ &= \lim_{k \rightarrow \infty} \frac{1}{2k} \ln |u_i[(\mathbf{J}^k)^T \mathbf{J}^k]| \\ &= \lim_{k \rightarrow \infty} \frac{1}{2k} \ln \sigma_i^2[\mathbf{J}^k] \\ &= \lim_{k \rightarrow \infty} \frac{1}{k} \ln \sigma_i[\mathbf{J}^k], \quad i = 1, 2, \dots, n \end{aligned}$$

根据性质3, 反馈矩阵 $\mathbf{B}$ 一定使得 $\lambda_i[\mathbf{J}] = e^c + N$, ($i = 1, 2, \dots, n$)。根据性质2, 可得 $\lambda_i[\mathbf{J}^k] = (e^c + N)^k$, ($i = 1, 2, \dots, n$)。根据性质4, $\sigma_i[\mathbf{J}^k] \geq |\lambda_i[\mathbf{J}^k]| = (e^c + N)^k$, 所以

$$LE_i = \lim_{k \rightarrow \infty} \frac{1}{k} \ln \sigma_i[\mathbf{J}^k] \geq \ln(e^c + N) > c, \quad i = 1, 2, \dots, n \quad (11)$$

证毕

定理2 (Gerschgorin 定理) [7] 设 $\mathbf{A} = (a_{ij})_{n \times n} \in C^{n \times n}$ 为 n 阶复数矩阵 (实数矩阵当然是复数矩阵的一个特例), 则 $\mathbf{A}$ 的特征值都落在复平面上的 n 个圆盘 $|z - a_{ii}| \leq R_i$, ($i = 1, 2, \dots, n$) 的并集内, 式中, R_i 称为圆盘的半径, 它等于第 i 行中除主对角线元素以外的其余各个元素的绝对值之和, 即

$$|z - a_{ii}| \leq R_i = \sum_{j \neq i}^n |a_{ij}| \quad (12)$$

定理2表明了对于 $\mathbf{A}$ 的任一特征值 λ_i , 总存在盖二圆 S_i , 使得 $\lambda_i \in S_i$ 。

2.2 配置 Lyapunov 指数为正的算法

上述的性质以及定理是新的混沌产生机理的基础, 并有重要的应用的价值, 也为配置 Lyapunov 指数的数值提供了理论支撑。有了以上的知识基础, 本文将对控制系统进行 Lyapunov 指数的配置。

对 $k = 0, 1, \dots, n$, 考虑控制系统

$$\mathbf{x}_{k+1} = \mathbf{A}\mathbf{x}_k + \mathbf{B}\mathbf{x}_k \quad (13)$$

现做如下计算:

步骤1 计算受控系统 $\mathbf{A}$ 的特征值以及特征向量;

步骤2 根据 $\mathbf{B} = \mathbf{z}\mathbf{z}^T, \mathbf{x}^T \mathbf{z} = e^c + N > 0, N =$

$\varepsilon + \lambda_i, \varepsilon > 0, i = (1, 2, \dots, n)$, 计算出其中一个 $\lambda_i (i = 1, 2, \dots, n)$ 所对应的 $z_i, B_i, C_i = B_i + A$;

步骤 3 计算步骤2得出的 C_i 的特征值以及特征向量;

步骤 4 同样按照步骤2, 求出其它 $\lambda_j (j \neq i)$ 所对应的 $z_j, B_j, C_j = B_j + C_i$;

步骤 5 直到配置完受控矩阵所有的特征值。

由以上步骤可知, 该算法主要是利用受控矩阵中子矩阵的特征值与特征向量, 因此不像Wang-Chen算法只适合受控系统本身是渐进稳定的、输入与输出都是有界的, 该算法不限制给定系统的具体形式, 对于低维系统而言, 控制器的形式简单, 易于理解, 更容易设计所需要的混沌系统模型, 在基于这种混沌系统的混沌密码系统和混沌保密通信中, 不存在非混沌状态的隐患。

2.3 系统轨道的全局有界性和Lyapunov指数的有限性

要想达到系统轨道全局有界的目标, 目前主要有2种方法, 第1种就是文献[2]中Chen-Lai算法提到的, 对整个系统采用取模运算的方式, 使得混沌行为在整个相空间下是有界的, 因而Chen-Lai算法可用于很大一类离散时间系统。第2种方法是文献[3]中Wang-Chen算法提到的对控制器取模, 不对控制系统进行相关界限的处理, 因此该算法只适用于系统本身渐进稳定、输入输出有界的、稳定的系统。鉴于第2种方法的局限性, 本算法使用第1种方法, 即

$$x_{k+1} = Ax_k + Bx_k \pmod{1} \quad (14)$$

文献[2]已证明该方法能使得系统轨道在有限的区域内产生混沌行为, 满足Devaney[8]意义下的混沌以及Li-Yorke[10]意义下的混沌。

下面进一步证明在该方法下Lyapunov指数不仅是正的, 而且是有界的, 即

$$c \leq LE_i(x_0) < \infty, i = 1, 2, \dots, n \quad (15)$$

事实上, 根据2-范数[9]的定义, 得

$$\begin{aligned} LE_i &= \lim_{k \rightarrow \infty} \frac{1}{2k} \ln |u_i[\mathbf{T}_j^T \mathbf{T}_j]| \\ &\leq \lim_{k \rightarrow \infty} \frac{1}{2k} \ln \left| \max_i \{u_i[\mathbf{T}_j^T \mathbf{T}_j]\} \right| \\ &= \lim_{k \rightarrow \infty} \frac{1}{2k} \ln \left| \max_i \left\{ \sqrt{u_i[\mathbf{T}_j^T \mathbf{T}_j]} \right\} \right|^2 \\ &= \lim_{k \rightarrow \infty} \frac{1}{k} \ln \|\mathbf{T}_i\|_2, i = 1, 2, \dots, n \end{aligned}$$

根据2-范数的定义[3], 得

$$\|\mathbf{T}_k\|_2 = \max_i \left\{ \sqrt{u_i(\mathbf{T}_i^T \mathbf{T}_i)} \right\} \leq (2N + e^c)^k \quad (16)$$

由式(15)可得

$$\begin{aligned} LE_i &= \lim_{k \rightarrow \infty} \frac{1}{2k} \ln |u_i[\mathbf{T}_j^T \mathbf{T}_j]| \\ &\leq \lim_{k \rightarrow \infty} \frac{1}{2k} \ln \left| \max_i \{u_i[\mathbf{T}_j^T \mathbf{T}_j]\} \right| \\ &= \lim_{k \rightarrow \infty} \frac{1}{k} \ln \|\mathbf{T}_i\|_2 \\ &= \lim_{k \rightarrow \infty} \frac{1}{k} \ln \left\{ \max_i \left\{ \sqrt{u_i(\mathbf{T}_i^T \mathbf{T}_i)} \right\} \right\} \\ &\leq \lim_{k \rightarrow \infty} \frac{1}{k} \ln (2N + \varepsilon)^k = \ln(2N + \varepsilon) \quad (17) \end{aligned}$$

根据前面的讨论, 只要受控系统一致有界, 即存在常数 N , 使得

$$\sup_{0 \leq k < \infty} \|\mathbf{A}\| \leq N < \infty$$

就一定能保证式(17)满足 $LE_i \leq \ln(2N + e^c) < \infty$, 又由定理1的理论证明, 得 $LE_i = \lim_{k \rightarrow \infty} \frac{1}{k} \ln \sigma_i[\mathbf{J}^k] \geq \ln(e^c + N) > c, (i = 1, 2, \dots, n)$, 因此, 所有的Lyapunov指数既为正又有界, 既满足

$$0 < c < \ln(e^c + N) \leq \ln_i \leq \ln(2N + \varepsilon) < \infty, i = 1, 2, \dots, n \quad (18)$$

3 线性反馈混沌化的算子

猫映射[10](Cat map)的离散系统为

$$\begin{bmatrix} x_{1,n+1} \\ x_{2,n+1} \end{bmatrix} = \mathbf{A} \begin{bmatrix} x_{1,n} \\ x_{2,n} \end{bmatrix} \pmod{1} \quad (19)$$

该系统的行为会随着 A 的不同取值而展现不同的状态, 因此, 取

$$\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

若对系统式(19)配置Lyapunov指数全部大于3, 即该系统Lyapunov指数达到无兼并状态。

A 对应的特征值以及特征向量分别为:

$$\lambda_1 = 0.3819, \lambda_2 = 2.6180, \mathbf{E}_1 = [-0.8507 \ 0.5257]^T, \mathbf{E}_2 = [0.5257 \ 0.8507]^T$$

取 $\varepsilon = 0.0001, c = 3$, 按照新算法步骤, 最终得到Lyapunov指数: $\lambda_1 = 3.0201; \lambda_2 = 3.0131$ 。

根据Chen-Lai算法, 计算系统的Lyapunov指数得 $\lambda_1' = 3.1392; \lambda_2' = 3.2317$ 。

本文算法的仿真结果如图1和图2所示(初值取 $(1/3, 1/3)$)。

由上面的结果可以看出, 首先该方法能够使得混沌系统的Lyapunov指数个数达到最大的可能

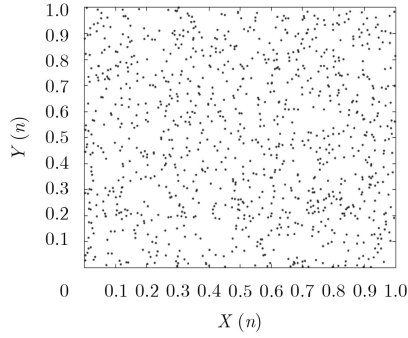
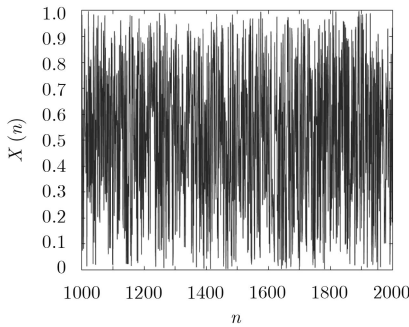


图1 2维混沌吸引子相图

图2 混沌轨道 $x(n)$ 的混沌轨道

性, 即 $L = n$, 而且方法的运算复杂度与文献[2]和文献[3]相比会低很多, 提高了相应的运算速率, 同样也提高了通信信息安全加密的效率, 该算法也与Chen-Lai算法达到的目标一致, 并且由数值的大小可以看出, 本文算法更能达到李氏指数预期的数值 $c = 3$, 这也是该算法的优势所在, 2种算法配置Lyapunov指数的比较如表1所示。总之, 在增强混沌强度方面, 本文算法有着一定的优势。

表1 两种算法配置Lyapunov指数效果比较

期望配置的李氏指数	Chen-Lai算法	本文算法
0.1	1.4112; 1.8741	0.1261; 0.1101
0.6	1.5732; 1.9542	0.6612; 0.6213
3.0	3.1392; 3.2317	3.0201; 3.0131

4 微扰反馈混沌化稳定系统的算子

考虑3阶Lü映射

$$\left. \begin{aligned} x &= a(y - x) \\ y &= cx - xz - y \\ z &= xy - bz \end{aligned} \right\} \quad (20)$$

令参数 $a = 36$, $b = 3$ 保持不变, c 作为变量, 使得系统处于混沌状态。

就其对Lü混沌系统的稳定性而言, 可以利用线性的方法, 求得在定点 $O(0, 0, 0)$ 处, 其线性方程的系数矩阵, 如式(21)

$$A = \begin{bmatrix} -36 & 36 & 0 \\ 0 & 20 & 0 \\ 0 & 0 & -3 \end{bmatrix} \quad (21)$$

其对应的特征值以及特征向量分别为:

$$\lambda_1 = -36, \lambda_2 = 20, \lambda_3 = -3, \mathbf{X}_1 = [1 \ 0 \ 0]^T,$$

$$\mathbf{X}_2 = [0.5408 \ 0.84120]^T, \mathbf{X}_3 = [0 \ 0 \ 1]^T$$

取 $\varepsilon = 0.0001$, $c = 3$, 最终得到Lyapunov指数: $\lambda_1 = 3.123$; $\lambda_2 = 3.0231$; $\lambda_3 = 3.0341$ 。

按照Chen-Lai算法达到的系统Lyapunov指数为 $\lambda_1' = 3.8224$; $\lambda_2' = 3.9449$; $\lambda_3' = 4.2495$ 。

本文算法的仿真结果如图3所示(初值取 $(1/3, 1/3, 1/3)$)。

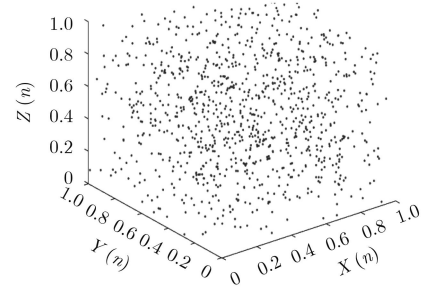


图3 3维混沌吸引子相图

5 性能分析

关于采用本文算法配置的离散混沌系统的性能, 主要从以下方面进行分析: (1)计算复杂度; (2)运行速度; (3)吸引子相图以及时间序列。

5.1 计算复杂度

从计算的角度来说, 本文算法与Chen-Lai算法配置离散混沌系统的计算复杂度相差不大, 其中涉及到的运算有: 特征值与特征向量运算、矩阵加、矩阵乘、雅克比矩阵运算、谱范数运算(矩阵乘)。主要的计算复杂度如下。

对于本文算法:

(1)特征值与特征向量运算: $k(n o(k) + o(k^2))$;

(2)矩阵乘法运算: $k(o(n) + o(n^2))$;

(3)矩阵加法运算: $k o(n)$

因此本文算法的计算复杂度:

$$\begin{aligned} O_{Pr} &= k(n o(k) + o(k^2)) + k(o(n) + o(n^2)) + k o(n) \\ &= k(n o(k) + o(k^2) + 2 o(n) + o(n^2)) \end{aligned}$$

对于Chen-Lai算法:

(1)雅克比矩阵运算: $2 o(n^2)$;

(2)谱范数(矩阵乘)运算: $2 k o(n^3)$;

(3)矩阵和运算: $o(n)$

因此Chen-Lai算法的计算复杂度: $O_{C-L} =$

$2o(n^2)+2ko(n^3)+o(n)$, 其中, k, n 分别代表矩阵的各个特征值不同的个数、矩阵维数。

由此可以看出, 当矩阵各个特征值不同的个数与矩阵维数相等时: $k = n$, 本文算法比Chen-Lai算法将近小1个数量级。

5.2 运行速度

在同一维数的条件下, 比较了本文算法与Chen-Lai算法的运行速度, 如表2所示。

表 2 2种算法运行速度的比较(s)

混沌系统的维数	Chen-Lai算法	本文算法
3	0.0517	0.0279
4	0.0579	0.0287
5	0.1025	0.0587
6	0.1534	0.6640

从表中可以看出, 2个算法的运算速度都很小, 但本文算法的运行时间总是比Chen-Lai算法的运行时间快, 这对基于这种混沌系统的混沌密码体系和混沌保密通信至关重要。

5.3 吸引子相图以及时间序列

混沌的特征可通过相空间中混沌吸引子的轨迹来表示, 在图1和图3混沌吸引子相图中, 整个相空间都充满了混沌轨迹; 在图2输出的时间序列中, 可以看出该混沌系统可以同时输出2个或3个不同的伪随机序列, 且随机性较强。由于雅克比矩阵与输出时间序列无关, 因此, n 维离散混沌系统对于所有的初始值, 都处于无退化的混沌状态, 在基于这种混沌系统的分组密码设计以及其他通信保密, 都不会存在非混沌状态或者混沌进入周期状态的隐患。

6 结束语

本文提出一种配置离散系统Lyapunov指数的新算法, 若所有Lyapunov指数大小都是预先确定的, 可以实现对离散混沌系统中每个Lyapunov指数的精确配置。通过引入指定形式的反馈和取模运算, 利用受控系统的特征值以及特征向量确定控制矩阵, 准确地配置正的Lyapunov指数, 可以有目的地产生或增强混沌效应, 从而使得系统成为无兼并、无退化的混沌系统, 也增强了混沌系统的混乱性与不规则性。本文算法完全吻合混沌的Lyapunov指数判据, 通过算例可以看出, 本文算法配置的Lyapunov指数更准确, 可以避免多变量非混沌状态。但是本文算法也存在一定的缺点, 对于高维的系统, 运算上有一定的困难, 这也是接下来的工作, 做更进一步改进, 使得算法更加灵活地运用在更高的混沌系统中。

参 考 文 献

- [1] 陈关荣. 控制非线性动力系统的混沌现象[J]. 控制理论与应用, 1997, 14(1): 1-6.
CHEN Guanrong. Controlling chaos in nonlinear dynamical systems[J]. *Control Theory and Applications*, 1997, 14(1): 1-6.
- [2] CHEN H K and LEE C I. Anti-control of chaos in rigid body motion[J]. *Chaos, Solitons & Fractals*, 2004, 21(4): 957-965. doi: [10.1016/j.chaos.2003.12.034](https://doi.org/10.1016/j.chaos.2003.12.034).
- [3] 陈关荣, 汪小帆. 动力系统的混沌化——理论、方法与应用[M]. 上海: 上海交通大学出版社, 2006.
CHEN Guanrong and WANG Xiaofan. Chaos of Power System - Theory, Method and Application[M]. Shanghai: Shanghai Jiao Tong University Press, 2006.
- [4] HUA Zhongyun, Yi Shuang, ZHOU Yicong, et al. Designing hyperchaotic cat maps with any desired number of positive Lyapunov exponents[J]. *IEEE Transactions on Cybernetics*, 2018, 48(2): 463-473. doi: [10.1109/TCYB.2016.2642166](https://doi.org/10.1109/TCYB.2016.2642166).
- [5] WANG Chuanfu, FAN Chunlei, and DING Qun. Constructing discrete chaotic systems with positive Lyapunov exponents[J]. *International Journal of Bifurcation and Chaos*, 2018, 28(7): 1850084. doi: [10.1142/S0218127418500840](https://doi.org/10.1142/S0218127418500840).
- [6] CHEN Shikun, YU Simin, LÜ Jinhua, et al. Design and FPGA-based realization of a chaotic secure video communication system[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2018, 28(9): 2359-2371. doi: [10.1109/TCSVT.2017.2703946](https://doi.org/10.1109/TCSVT.2017.2703946).
- [7] 张良, 唐驾时. 四维超混沌系统Hopf分岔分析与反控制[J]. 计算力学学报, 2018, 35(2): 188-194. doi: [10.7511/jslx20170313005](https://doi.org/10.7511/jslx20170313005).
ZHANG Liang and TANG Jiashi. Hopf bifurcation analysis and anti-control of bifurcation of a four-dimensional hyperchaotic systems[J]. *Chinese Journal of Computational Mechanics*, 2018, 35(2): 188-194. doi: [10.7511/jslx20170313005](https://doi.org/10.7511/jslx20170313005).
- [8] PHAM V T, VOLOS C, JAFARI S, et al. Constructing a novel no-equilibrium chaotic system[J]. *International Journal of Bifurcation and Chaos*, 2014, 24(5): 1450073. doi: [10.1142/S021812741450073](https://doi.org/10.1142/S021812741450073).
- [9] LIN Zhuosheng, YU Simin, LÜ Jinhua, et al. Design and ARM-embedded implementation of a chaotic map-based real-time secure video communication system[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2015, 25(7): 1203-1216. doi: [10.1109/TCSVT.2014.2369711](https://doi.org/10.1109/TCSVT.2014.2369711).
- [10] ZHENG Hanzhong, YU Simin, and LÜ Jinhua. Multi-images chaotic communication and FPGA implementation[C]. The 33rd Chinese Control Conference, Nanjing, China, 2014. doi: [10.1109/ChiCC.2014.6895876](https://doi.org/10.1109/ChiCC.2014.6895876).
- [11] SHEN Chaowen, YU Simin, LÜ Jinhua, et al. Designing hyperchaotic systems with any desired number of positive

- Lyapunov exponents via a simple model[J]. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2014, 61(8): 2380–2389. doi: [10.1109/TCSI.2014.2304655](https://doi.org/10.1109/TCSI.2014.2304655).
- [12] WU Yue, HUA Zhongyun, and ZHOU Yicong. N -dimensional discrete cat map generation using Laplace expansions[J]. *IEEE Transactions on Cybernetics*, 2016, 46(11): 2622–2633. doi: [10.1109/TCYB.2015.2483621](https://doi.org/10.1109/TCYB.2015.2483621).
- [13] 王贺元, 尹霞. 新超混沌系统的动力学行为及自适应控制与同步[J]. 动力学与控制学报, 2017, 15(4): 335–341. doi: [10.6052/1672-6553-2017-002](https://doi.org/10.6052/1672-6553-2017-002).
- WANG Heyuan and YIN Xia. Dynamical behaviors of a new hyperchaotic system and its adaptive control and synchronization[J]. *Journal of Dynamics and Control*, 2017, 15(4): 335–341. doi: [10.6052/1672-6553-2017-002](https://doi.org/10.6052/1672-6553-2017-002).
- [14] 杨昌烨, 陈艳峰, 张波, 等. 基于参数扰动的混沌控制方案在 Buck-Boost 变换器中的应用研究[J]. 电源学报, 2018, 16(2): 32–37. doi: [10.13234/j.issn.2095-2805.2018.2.32](https://doi.org/10.13234/j.issn.2095-2805.2018.2.32).
- YANG Changye, CHEN Yanfeng, ZHANG Bo, *et al.* Applications of chaotic control scheme based on parameter-perturbation in Buck-Boost converter[J]. *Journal of Power Supply*, 2018, 16(2): 32–37. doi: [10.13234/j.issn.2095-2805.2018.2.32](https://doi.org/10.13234/j.issn.2095-2805.2018.2.32).
- [15] MAMAT M, VAIDYANATHAN S, SAMBAS A, *et al.* A novel double-convection chaotic attractor, its adaptive control and circuit simulation[C]. IOP Conference Series: Materials Science and Engineering, Tangerang, Indonesia, 2018, 332: 012033. doi: [10.1088/1757-899X/332/1/012033](https://doi.org/10.1088/1757-899X/332/1/012033).
- 赵 耿: 男, 1964年生, 博士后, 研究方向为混沌密码理论及应用, 计算机信息安全与保密.
- 李 红: 女, 1991年生, 硕士生, 研究方向为混沌抗退化与无退化, 图像加密.
- 马英杰: 女, 1979年生, 副教授, 研究方向为混沌保密通信.
- 秦晓宏: 女, 1976年生, 讲师, 研究方向为信息安全、信息隐藏.