

一类具有 Markov 性质的混沌系统的构造*

刘泉^{1)2)†} 李佩玥¹⁾ 章明朝¹⁾ 隋永新¹⁾ 杨怀江¹⁾

1) (中国科学院长春光学精密机械与物理研究所, 应用光学国家重点实验室, 长春 130033)

2) (中国科学院大学, 北京 100049)

(2013 年 4 月 3 日收到; 2013 年 5 月 21 日收到修改稿)

本文构造了一类具有 Markov 性质的分段扩张线性映射, 计算表明其具有正的李雅普诺夫指数. 通过理论分析, 证明了其极限分布是均匀分布, 并给出了其最小周期的计算公式. 通过分析符号熵测度应用于此系统时的具体涵义, 指出该系统的复杂度与系统的最小周期之间存在着矛盾关系, 说明了此系统具有可控的复杂度并给出了其复杂度随系统参数变化时的理论极限公式. 通过统计测试和复杂度测试表明, 此系统产生的混沌序列服从均匀分布, 而通过参数的调整该系统的符号熵可以接近其理论极限, 而与 Logistic 映射和斜帐篷映射的基于近似熵和符号熵的对比实验可知, 本文所提系统具有更高的复杂度, 并有更长的最小周期. 这表明此系统比较适合用于构造保密通信系统.

关键词: 混沌, Markov 性质, 复杂度, 均匀分布

PACS: 05.45.-a, 05.45.Ac, 05.45.Tp, 02.50.Ga

DOI: 10.7498/aps.62.170505

1 引言

混沌系统具有初值敏感的特性, 利用混沌系统设计的密码算法有着良好的混乱和扩散特性, 而自 Matthews 提出混沌加密思想以来^[1], 基于混沌的密码算法得到了广泛的研究, 文献 [2—6] 是基于 Logistic 映射和帐篷映射设计的通用加密算法, 文献 [7, 8] 是基于猫脸映射设计图像加密算法, 文献 [9] 基于广义混沌映射切换设计了一种单向 Hash 函数. 基于混沌的密码算法均受到了不同程度的攻击, 于是对保密通信系统好坏的评价也有越来越多的研究, 一般认为复杂度越高的系统越难破译, 近年来关于混沌系统复杂度的研究也吸引了越来越多的关注.

混沌伪随机序列的复杂度指的是它与随机序列的相似程度, 它可以衡量利用部分序列恢复出整体序列的难易程度^[10–12]. 复杂度的研究可分为两类: 一类是针对常规伪随机序列提出的线性复杂度^[13,14]和 K 错线性复杂度^[15,16], 它不太适合于混沌序列的精确测度; 另一类是针对混沌系统提

出的指标, 如基于近似熵 (ApEn) 的复杂度测度方法^[17,18]和基于符号熵的复杂度测度方法^[19,20]等.

本文首先构造了一类具有 Markov 性质的分段扩张线性映射, 然后分析了它基本的混沌特性, 证明了其极限分布是均匀分布, 给出了其最小周期的计算公式, 其次分析了符号熵测度应用于此系统时的具体涵义, 指出系统的复杂度与系统的最小周期之间存在的矛盾关系, 给出了随参数变化时系统复杂度的理论极限, 最后通过数值计算来实际测试系统的均匀性和复杂度, 并与常见的一维混沌系统做了比较, 验证了通过参数的调整可以提高系统的复杂度, 并增加其最小周期.

2 系统构造方法

2.1 基本定义

对一个分段线性映射来说, 若它具有 Markov 性质其符合下述定义.

定义1(Markov 性质^[21]) 设 $\{I_1, I_2, \dots, I_N\}$ 是实直线上的有限个内部不相交的闭区间集, 即

* 国家重点基础研究发展计划 (973 计划) (批准号: 2007CB311201) 和吉林省科技发展计划 (批准号: 20130522120JH) 资助的课题.

† 通讯作者. E-mail: lovefirespread@gmail.com

$\text{int}(I_i) \cap \text{int}(I_j) = \emptyset, i \neq j$, 存在一个定义在区间的并 $\cup_{j=1}^N I_j$ 上的仅有有限个不连续点的函数 f , 说函数 f 具有 Markov 的性质, 如果满足只要 $f(\text{int}(I_j)) \cap \text{int}(I_i) \neq \emptyset$, 则 $\overline{f(I_j)} \supseteq I_i$, 且称 $\{I_1, I_2, \dots, I_N\}$ 是 f 的一个 Markov 分割.

定义2(输出熵) 对一个时齐 Markov 链 $\{X_n, n = 0, 1, 2, \dots\}$, 其状态空间记为 $S_t = \{1, 2, \dots, K\}$, 其状态转移图记为 G , 定义关于 G 的输出熵为

$$\text{GraphOutEn}(G) = - \sum_{\forall i, j \in S_t, \text{且 } i \rightarrow j} P_{ij} \times \ln(P_{ij}), \quad (1)$$

$i \rightarrow j$ 表示 i 可达 j , 而

$$P_{ij} \triangleq P\{X_n = i, X_{n+1} = j\} \\ = P\{X_{n+1} = j | X_n = i\} \times P\{X_n = i\}.$$

定义3(符号熵^[22]) 给定一个由 t 个符号组成的符号集 $\{s_0, s_1, \dots, s_{t-1}\}$ 和一个 $t+1$ 个临界点组成的集合 $\{C_0, C_1, \dots, C_t\}$, 可以用以下分割规则将时间序列 $\{u_0, u_1, u_3, \dots\}$ 转换为一个符号序列 $\{s(1), s(2), s(3), \dots\}$, 若 $C_k < u_j \leq C_{k+1}$, 则 $s(j) = s_k$. 将所得符号序列 $\{s(1), s(2), s(3), \dots\}$ 分割成为长度为 m 的窗口向量. 这些窗口向量可以通过下式来标记和辨别:

$$l_x(m, i) = \sum_{p=1}^m t^{m-p} S(p+i), \quad (2)$$

其中 t 是符号集 $\{s_0, s_1, \dots, s_t\}$ 中不同符号的个数, m 表示窗口向量的长度, i 表示窗口向量沿着符号序列 $\{s(1), s(2), s(3), \dots\}$ 从第 i 个符号开始. 为了方便, 通过将符号 s_k 用相应的整数 k 来代替, 则每一个窗口向量都可以方便地用整数集 $\{0, 1, 2, \dots, t^m - 1\}$ 的一个整数唯一地标记和辨别. 用 P_{l_x} 表示特定窗口向量 l_x 出现的概率,

这个概率可以采用窗口向量 l_x 在混沌符号序列 $\{s(1), s(2), s(3), \dots\}$ 中出现的次数除以所有窗口向量的总数计算. 包含在符号序列中的信息量可以用以下符号熵定量表示:

$$\text{SymbEn}(m, t, N) = - \frac{1}{m} \sum_{l_x} P_{l_x} \ln P_{l_x}. \quad (3)$$

定义4(近似熵 ApEn^[22]) 对于一个长度为 N 的序列样本空间 $[u(1), u(2), \dots, u(N)]$, 首先定义 m 维向量组 $x(1), x(2), \dots, x(i), \dots, x(N-m+1) \in R^m$, 其中

$$x(i) = [u(i), u(i+1), \dots, u(i+m-1)], \\ 1 \leq i \leq N-m+1,$$

m 维向量 $x(i)$ 和 $x(j)$ 的最大距离定义为

$$d[x(i), x(j)] = \max_{k=1, 2, \dots, m} (|u(i+k-1) - u(j+k-1)|),$$

满足与第 i 个向量的距离小于 r 的向量数为

$$C_i^{m,N}(r) = N_i(jr) / (N-m+1),$$

其中 $N_i(jr)$ 是满足 $d[x(i), x(j)] \leq r$ 的 j 的个数. 根据 $C_i^{m,N}(r)$ 定义

$$\Phi^{m,N}(r) = (N-m+1)^{-1} \sum_{i=1}^{N-m+1} \ln C_i^{m,N}(r).$$

那么 ApEn 可以被定义为

$$\text{ApEn}(m, r, N) = \Phi^{m,N}(r) - \Phi^{m+1,N}(r).$$

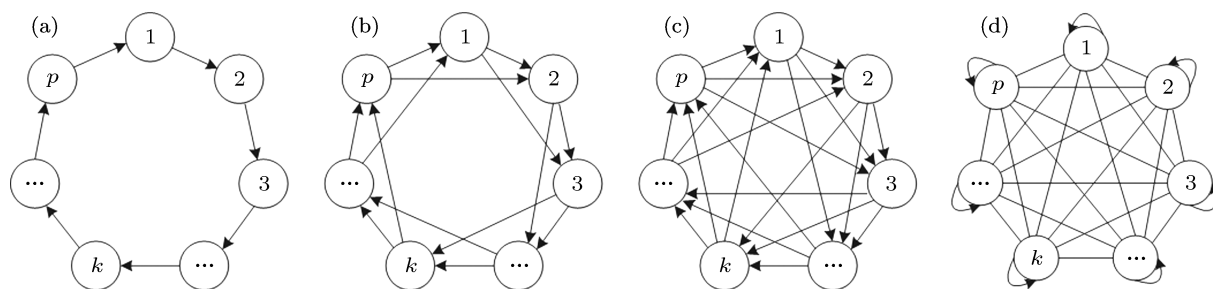
2.2 系统结构

选取参数 $p(p \geq 7)$, p 是素数, 将 $[0, 1]$ 区间 p 等分, 构造映射 $T(x, p, \sigma)$ 如下, 其中 $\sigma \in Z^+$ 且 $2 \leq \sigma \leq p-1$,

$$T(x, p, \sigma) = \begin{cases} \sigma x + \frac{(i+1) - i\sigma}{p} \bmod 1, & x \in \left[\frac{i}{p}, \frac{i+1}{p}\right), \quad i = 0, 1, \dots, p-2, \\ \sigma x + \frac{p - (p-1)\sigma}{p} \bmod 1, & x \in \left[\frac{p-1}{p}, 1\right]. \end{cases} \quad (4)$$

那么该分段扩张线性映射具有一个 Markov 分割 $I_1, I_2, I_3, \dots, I_p$, 其中 $I_k = \left[\frac{k-1}{p}, \frac{k}{p}\right], k = 1, \dots, p$, 证明见结论 3. 将映射 T 按上述分割划分后, 它的状态

转移图如下所示, 事实上它构成了一个时齐 Markov 链, 其中图 1(a) 表示 $\sigma = 1$ 时的转移图, 其中图 1(d) 表示 $\sigma = p$ 时的转移图.


 图 1 系统状态转移图随斜率 (或出度) 变化 (a) $\sigma = 1$; (b) $\sigma = 2$; (c) $\sigma = 3$; (d) $\sigma = p$

3 理论分析

3.1 混沌系统的基本性质分析

结论1 T 具有对初始值的敏感依赖性.

该映射的李雅普诺夫指数记为 $L(x, f)$ 令 A 表示 $T(x, p, \sigma)$ 在固定 p 和 σ 时所有第一类断点的集合, 即 $A = \{x : \lim_{x \rightarrow x^-} T(x, p, \sigma) \neq \lim_{x \rightarrow x^+} T(x, p, \sigma), T(x, p, \sigma) \text{ 在 } x \text{ 的左右极限都存在}\}$, 当 $x \notin A$ 时, $|T'(x)| = \sigma$, 所以只要 $x^j = f^j(x_0) \notin A$, 就有 $L(x, f) = \ln(\sigma) \geq \ln(2) > 0$.

结论2 T 的最小周期为 $\left\lceil \frac{p}{\sigma} \right\rceil + 1$.

将 $[0, 1]$ 区间等分为 p 份, 用 p 个符号标记为 $\{s_1, s_2, s_3, \dots, s_p\}$, T 的状态转移图如图 1 所示. 若一条轨道依次通过区间 $I_{a_1}, I_{a_2}, I_{a_3}, \dots, I_{a_l}$, 而 $I_{a_k} \in \{I_j : j = 1, \dots, p\}$, $k = 1, \dots, l$, 那么它对应的符号序列记为 $s_{a_1}, s_{a_2}, s_{a_3}, \dots, s_{a_l}$. 若一个轨道是周期轨道, 那么它的符号序列一定是周期的, 这就说明了此混沌映射轨道的周期不会小于容许符号串

的最小周期. 由上述 $T(x, p, \sigma)$ 及其转移图可知, 其各状态等效, 以状态 1 为例, 最快返回 1 的符号序列的一个符号序列为 $\{s_1, s_{1+\sigma}, s_{1+2\sigma}, \dots, s_{1+t\sigma}, s_1\}$, 其中 $t = \left\lceil \frac{p}{\sigma} \right\rceil$, 而 $[x]$ 为高斯取整函数, 该序列长度为 $t + 1$. 于是, 此映射可以产生的最小周期的符号串的长度为 $\left\lceil \frac{p}{\sigma} \right\rceil + 1$.

结论3 $I_1, I_2, I_3, \dots, I_p$ 是 T 的一个的 Markov 分割.

由图 1 可知, $I_1, I_2, I_3, \dots, I_p$ 是内部不相交的闭区间集, 对任意 i 有 $f(I_i) = \cup_{j=1}^{\sigma} I_{i+j}$, $i = 1, \dots, p$, 其中 $I_{i+j} = I_{(i+j) \bmod \sigma}$, 若 $(i+j) \bmod \sigma = 0$, 则 $I_{i+j} = I_p$, 经验证其满足条件只要 $f(\text{int}(I_j)) \cap \text{int}(I_i) \neq \emptyset$, 则 $f(I_j) \supseteq I_i$. 于是 $I_1, I_2, I_3, \dots, I_p$ 是 T 的一个 Markov 分割.

结论4 T 的极限分布是均匀分布.

由 Lasota-Yorke 定理^[21,23,24] 及推论可知, 计算上述分段线性函数 T 的极限分布可通过求其转移矩阵的特征值为 1 对应的特征向量来完成, 其转移矩阵为 $M = (a_{ij})_{p,p}$, 满足 $\sum_{j=1}^p a_{ij} = 1$, 记 M 为

$$M = \begin{bmatrix} 0 & 1/\sigma & 1/\sigma & 0 & \dots & 0 \\ 0 & 0 & 1/\sigma & 1/\sigma & \ddots & 0 \\ \dots & \dots & \ddots & \ddots & \dots & \dots \\ 0 & 0 & \ddots & \ddots & 1/\sigma & 1/\sigma \\ 1/\sigma & 0 & \ddots & \ddots & \ddots & 1/\sigma \\ 1/\sigma & 1/\sigma & 0 & \dots & \dots & 0 \end{bmatrix}_{p \times p}, \quad (5)$$

其极限分布是一个均匀分布其特征值为 1 的特征向量标准化后为 $V_p = (\frac{1}{p}, \frac{1}{p}, \dots, \frac{1}{p})$, 于是其在 $[0, 1]$ 上的密度函数为

$$V_p = \left(\frac{1}{p} \times p, \frac{1}{p} \times p, \dots, \frac{1}{p} \times p \right),$$

也就是说其密度函数为

$$\rho(x) = \chi_{[0,1]}(x) = \begin{cases} 0, & x \in R/[0, 1], \\ 1, & x \in [0, 1]. \end{cases}$$

从而它的极限分布即为 $[0, 1]$ 上的均匀分布.

3.2 系统复杂度分析

3.2.1 基于符号熵的分析

对有 p 个元素的符号集 $S_{\text{sym}} = \{s_0, s_1, \dots, s_{p-1}\}$, 嵌入维数取 m , 它构成的 m 维离散空间 $K = \{(x_1, x_2, \dots, x_m) : x_i \in S_{\text{sym}}, i = 1, \dots, m\}$ 中点的个数为 p^m . 若该序列是理想的均匀随机序列, 则其在 m 维空间中点集上也是均匀分布的. 采样长度为 $S (S \gg p^m)$ 时均匀随机序列的符号熵为

$$\begin{aligned} \text{SymbEn}(m, p, S) &= -\frac{1}{m} \sum_{l_x} P_{l_x} \ln P_{l_x} = -\frac{1}{m} \sum_i^{p^m} \frac{1}{p^m} \ln \frac{1}{p^m} \\ &= \ln(p). \end{aligned} \quad (6)$$

这就说明了其符号熵在嵌入维数增加时不变, 而随符号个数增加时成对数增加.

以图论观点来看, 可将上述 m 维离散空间中的点表示为转移图中长度为 $m-1$ 的路径. 于是对映射 $T(x, p, \sigma)$ 来说, 它的转移图是不可约的有向连通图而且每个顶点的出度 (入度) 都相同为 $t (2 \leq t \leq p-1)$, 而顶点的出度 t 和映射斜率 σ 是一一对应的. 当采样长度为 $S (S \gg p^m)$ 时它的符号熵为

$$\begin{aligned} \text{SymbEn}(m, p, S) &= -\frac{1}{m} \sum_{l_x} P_{l_x} \ln P_{l_x} \\ &= -\frac{1}{m} \sum_i^{pt^{m-1}} \frac{1}{pt^{m-1}} \ln \left(\frac{1}{pt^{m-1}} \right) \\ &= \frac{1}{m} \times \ln(p \times t^{m-1}) \\ &= \frac{\ln(p) + (m-1)\ln(t)}{m} (t \leq p). \end{aligned} \quad (7)$$

当 $p = 29$, 嵌入维数取 2, 3 和 4 时, $T(x, p, \sigma)$ 的符号熵的理论值与 t (或 σ) 关系如图 2 所示, 当 t 增加时符号熵增大, 当嵌入维数增加时符号熵减小, 固定 p 时它们有一个共同的理论极限.

由上述理论分析可知, 当分割区间个数 p 趋于无穷大时, $T(x, p, \sigma)$ 的最小周期 (结论 2) 和复杂度 (公式 7) 均趋于无穷大. 固定嵌入维数 m 和分割区间个数 p 时, 随着系统参数 σ 增大时, 系统的复杂度变高, 直至达到最高值 $\ln(p)$, 系统的最小周期逐渐变短, 直至出现 $p-1$ 个不动点 ($p-1$ 不动点是因为有一个是不动点在边界处被 I_1 和 I_2 所共享), 此时满足 $\sigma = p$; 当 $\sigma = 1$ 时, $T(x, p, \sigma)$ 的运动是规

律的, 此时其最小周期最长, 复杂度最低.

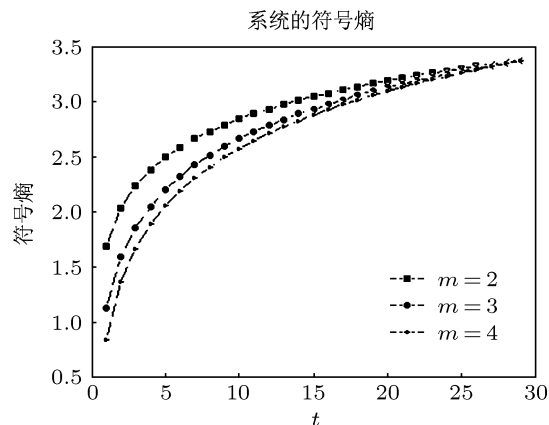


图 2 $T(x, p, \sigma)$ 的符号熵随参数的变化

3.2.2 符号熵与输出熵的关系

由上述输出熵定义可知, 当 $m = 2$ 时 $T = 2 \times \text{SymbEn}(2, p, S)$ 即为 $\text{GraphOutEn}(G)$ 的一个估计值. 这样一来, 当 $\text{GraphOutEn}(G)$ 达到最大值时 $\text{SymbEn}(2, p, S)$ 也能达到最大值. 当 $i \rightarrow j$ 对任意 i, j 都成立而且 $P_{ij} = \frac{1}{p^2}$ ($i, j = 1, \dots, p$) 时, $\text{GraphOutEn}(G)$ 取得最大值 $2\ln(p)$.

转移图的输出熵在一定程度上可以代替符号熵来快速判断系统的复杂度. 当 $T(x, p, \sigma)$ 的参数 σ 增加 1 时, 其转移图的每个顶点的出度都增加 1, 相应的其符号熵按对数增加, 但是系统的最小周期变得更短了 (见结论 2).

3.2.3 基于近似熵的分析

Eckmann-Ruelle 提出的 KS 熵的计算方法就是 ApEn 算法 [25] 见 (8) 式, ApEn 是计算在已知 m 个样本的情况下, 产生第 $m+1$ 个样本的条件概率 [22].

$$\lim_{r \rightarrow 0} \lim_{m \rightarrow \infty} \lim_{N \rightarrow \infty} \text{ApEn}(m, r, N) = H_{\text{ER}}. \quad (8)$$

若是对 $T(x, p, \sigma)$ 产生的序列量化而产生 K 进制的序列, 那么该离散化的序列的近似熵的极限为 $\ln(K)$, 它的近似熵满足公式 [22] $0 \leq \lim_{n \rightarrow \infty} \text{ApEn}(m, N) \leq \ln(K)$, 当 $K = p$ 时, 上述极限等于符号熵的极限. 理论上来说, 序列越接近于均匀随机序列, 其近似熵就越大, 而 ER 熵也会越大. ER 熵是对 KS 熵的一个近似, 而 KS 熵衡量了一个系统运行时产生信息的速率. 对 $T(x, p, \sigma)$ 来说, 当 p 越大, 且 σ 越大时, 系统运行时产生的信息速率越大, 其 KS 熵相应的会越大, 于是 ApEn 也会越大.

3.3 系统不动点分析

对 $T(x, p, \sigma)$ 系统来说, 如果其出现不动点, 由区间的状态转移图 (如图 1(d)) 可知, 此点所在的区间将会转移到其自身, 其需要满足必要条件 $p = \sigma$, 这时可能产生至多 p 个不动点. 实际计算 $T(x, p, p)$ 的不动点时发现, 它的不动点只能出现在分割区间的边界处即 $\left\{\frac{1}{p}, \frac{2}{p}, \frac{3}{p}, \dots, 1\right\}$ 而 $T(x, p, p)$ 在这些点处都是间断的, 其取值正好避开了不动点, 这就是说系统没有不动点.

4 实证分析

4.1 均匀性测试

以系统 $T(x, 29, 3)$ 为例考察其均匀性, 初值 $x_0 = 1/23$, 选取迭代点数为 $N = 4096$. 实验结果如下图所述, 由图 3(a) 所示, 其经验分布函数是一个均匀分布, 而图 3(b) 的时序关系中亦无明显的规律

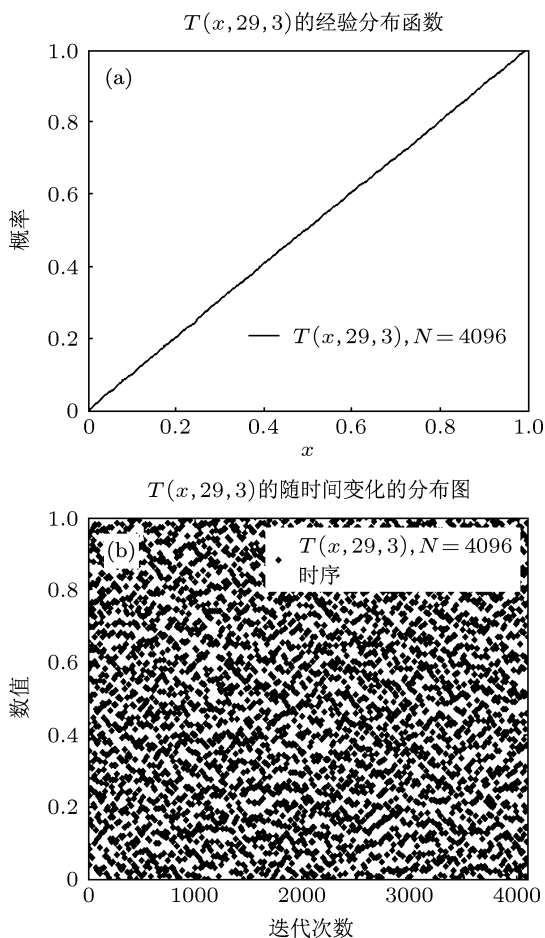


图3 (a) 系统的累积分布函数; (b) 系统的时序图

性. 另外, 通过 Kolmogorov-Smirnov 统计检验得 p 值为 $p_1\text{-KS} = 0.9590$, 通过 Chi-square 拟合优度检验得 p 值为 $p_1\text{-Chi2} = 0.9597$, 于是可以认为此系统产生的序列服从均匀分布.

4.2 复杂度测试

4.2.1 基于近似熵的实验分析

本文将 $T(x, p, \sigma)$ 与斜帐篷 (Tent Map) 映射

$$f(x, p) = \begin{cases} \frac{x}{p}, & x \in [0, p], \\ \frac{1-x}{1-p}, & x \in [p, 1] \end{cases}$$

和 Logistic 映射 $x_n = rx_{n-1}(1-x_{n-1})$ 作比较来说明其在 ApEn 测度意义下的复杂度, 实验选取嵌入维数为 1 到 8, 分辨率参数为 0.3, 初值 $x_0 = 1/23$, 选取迭代点数为 $N = 4096$. 对 Logistic 来说, 选取参数 r 依次为 3.5, 3.6, 3.7, 3.8, 3.9, 4.0, 其复杂度如图 4(a) 所示, 在 $r = 4.0$ 时系统有最高的复杂度. 对 Tent Map 来说, 选取参数 p 依次为 0.31, 0.36, 0.41, 0.46, 0.51, 其复杂度如图 4(b) 所示, 系统的复杂度在 $p = 0.51$ 附近时能够达到最高, 理论上在选取 $p = 0.5$ 时系统极限分布是均匀分布, 其复杂度达到最高, 但在计算机实现时系统受有限精度影响有严重的退化效应, 因而实验中没有选择这个点. 对 $T(x, p, \sigma)$ 来说, 为避免系统受计算机精度影响而严重退化, 系统参数 p 一般选择大于 5 的素数, 本次实验选取参数 $p = 29$, $\sigma(k)$ 依次为 2, 3, 4, 5, 其复杂度如图 4(c) 所示, 复杂度随着映射斜率 $\sigma(k)$ (或图的出度 t) 增大而变高; 选取参数 $p = 89, 91, 97, 101$, $\sigma(k)$ 依次为 86, 88, 94, 98, 其复杂度如图 4(d) 所示, 从图中可以看出, $T(x, p, \sigma)$ 在选取合适的参数时复杂度可以超过上述两个一维系统. 在嵌入维数变大时, 其复杂度会降低, 甚至低于那些相对简单的系统, 这主要是因为随着维数变大时, 测试过程中需要的数据量迅速增加, 相对来说, 当数据量一定时, 较低的嵌入维数, 其复杂度测试更精确.

$T(x, p, \sigma)$ 可以在理论上保证其最小周期为 $\left\lceil \frac{p}{\sigma} \right\rceil + 1$, 通过参数的调整可以使其变长, 不会同 Tent Map 和 Logistic 映射一样出现不动点.

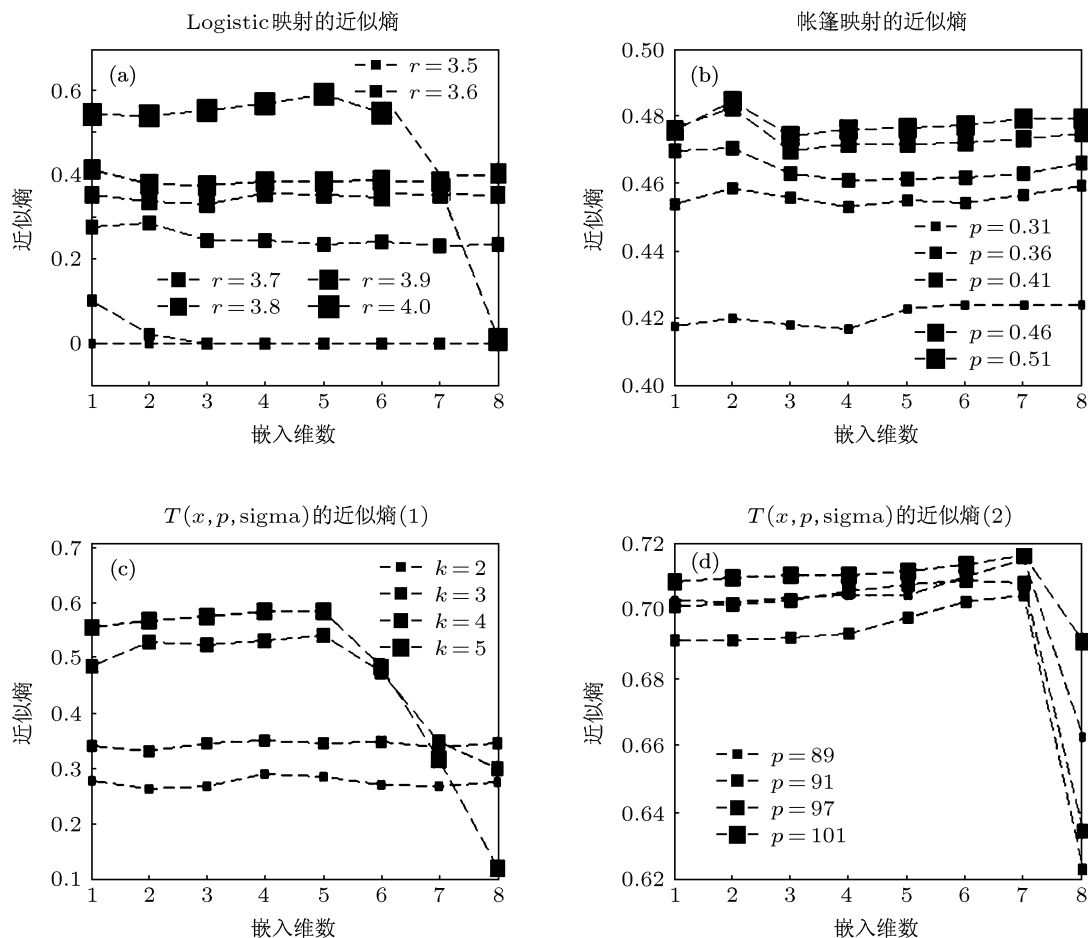


图4 各系统基于近似熵的复杂度的比较 (a) Logistic 映射参数取 3.5, 3.6, 3.7, 3.8, 3.9, 4.0; (b) 斜帐篷映射参数取 0.31, 0.36, 0.41, 0.47, 0.51; (c) $T(x, p, \sigma)$ 参数取 2, 3, 4, 5; (d) $T(x, p, \sigma)$ 参数取 89, 91, 97, 101

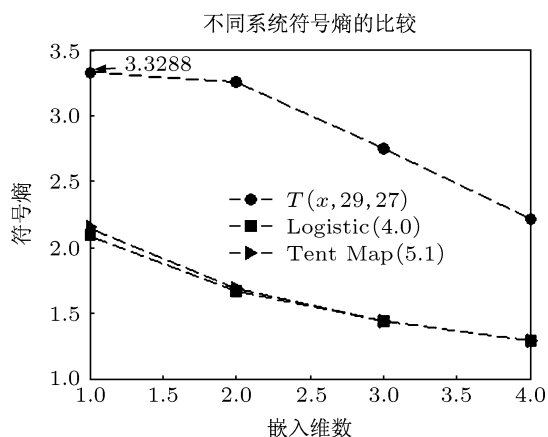


图5 Logistic 映射帐篷映射和 $T(x, p, \sigma)$ 关于符号熵的复杂度比较

4.2.2 基于符号熵的实验分析

本文对系统 $T(x, 29, 27)$ 和 $r = 4$ 的 Logistic 映射以及 $p = 0.51$ 的斜帐篷映射进行了比较, 说明其在符号熵意义下的复杂度的区别, 将 $[0, 1]$ 均匀分割为 29 份, 记符号集为 $\{s_0, s_1, \dots, s_{28}\}$. 实验选取嵌入维数为 2 到 5, 初值 $x_0 = 1/23$, 选取迭代次数为

$N = 65536$, 实验结果如图 5 所示, 系统 $T(x, 29, 27)$ 在嵌入维数为 2 时符号熵为 3.3288, 可以接近上述符号集的符号熵的极限 $\ln(29) = 3.3673 > 3.3288$. 而随嵌入维数增加符号熵变小, 这也符合上述的理论分析. 另外 $r = 4$ 的 Logistic 映射以及 $p = 0.51$ 的斜帐篷映射的符号熵均远小于 $T(x, 29, 27)$. 从符号熵的含义来看, 这说明上述两种系统在迭代过程中的符号变化的不确定性远低于系统 $T(x, 29, 27)$.

5 结论

本文提出了一种新的具有 Markov 性质的混沌系统 $T(x, p, \sigma)$, 分析了它基本的混沌特性, 从理论上证明了此系统的极限分布是 $[0, 1]$ 上的均匀分布, 其最小周期为 $\left\lceil \frac{p}{\sigma} \right\rceil + 1$, 其基于符号熵的复杂度是关于 p 和 σ 的一个函数, 通过对参数 p 和 σ 的控制可以实现对系统的复杂度和最小周期的控制. 实验结果显示, 此系统产生的序列服从均匀分布,

从时序图上看没有明显的规律性. 另外, 与常见的混沌系统 Logistic 映射和斜帐篷映射相比, 通过调整 $T(x, p, \sigma)$ 的参数, 无论是从近似熵还是从符号

熵的角度来看, $T(x, p, \sigma)$ 都将大于这两种系统的复杂度.

-
- [1] Matthews R 1989 *Cryptologia* **13** 29
 - [2] Baptista M S 1998 *Phys. Lett. A* **240** 50
 - [3] Xiao D, Liao X F, Deng S J 2008 *Phys. Lett. A* **372** 4682
 - [4] Li P Y, Gu L, Sui Y X, Yang H J 2010 *Optics and Precision Engineering* **18** 2102 (in Chinese) [李佩玥, 古力, 隋永新, 杨怀江 2010 光学精密工程 **18** 2102]
 - [5] Kanso A, Ghebleh M 2012 *Commun Nonlinear Sci Numer Simulat* **17** 2943
 - [6] Hu H P, Liu S H, Wang Z X, Wu X G 2004 *Chinese Journal of Computers* **27** 408 (in Chinese) [胡汉平, 刘双红, 王祖喜, 吴晓刚 2004 计算机学报 **27** 408]
 - [7] Ye R S 2011 *Optics Communications* **284** 5290
 - [8] Tong X J 2013 *Commun Nonlinear Sci. Numer Simulat* **18** 1725
 - [9] Wang X M, Zhang J S, Zhang W F 2003 *Acta Phys. Sin.* **52** 2737 (in Chinese) [王小敏, 张家树, 张文芳 2003 物理学报 **52** 2737]
 - [10] Li Z, Cai J P, Chen X J, Lu X F 2009 *Wireless Communications and Networking Conference 2009 IEEE* **4** p1
 - [11] Li Z, Cai J P, Lu X F, Si J B 2009 *Communications 2009 ICC 09. IEEE International Conference on* **6** p1
 - [12] Li Z, Cai J P, Chang Y L 2009 *IEEE Trans Commun* **57** 812
 - [13] Xiao G Z, Wei S M, Lam K Y, Imamura K 2000 *IEEE Trans Inform Theory* **46** 2203
 - [14] Kolokotronis N, Kalouptsidis N 2003 *IEEE Trans Inform Theory* **49** 3047
 - [15] Kurosawa K, Sato F, Sakata T, Kishimoto W 2000 *IEEE Trans Inform Theory* **46** 694
 - [16] Lauder A G B, Paterson K G 2003 *IEEE Trans Inform Theory* **49** 273
 - [17] Cai J P, Li Z, Song W T 2003 *Acta Phys. Sin.* **52** 1871 (in Chinese) [蔡觉平, 李赞, 宋文涛 2003 物理学报 **52** 1871]
 - [18] Pincus S M 1995 *Chaos* **5** 110
 - [19] Xiao F H, Yan G R, Han Y H 2004 *Acta Phys. Sin.* **53** 2877 (in Chinese) [肖方红, 阎桂荣, 韩宇航 2004 物理学报 **53** 2877]
 - [20] Azad R K, Rao J S, Ramaswamy R 2002 *Chaos Soliton & Fract.* **14** 633
 - [21] Robinson R C 2004 *An Introduction to Dynamical Systems: Continuous and Discrete* (Prentice Hall Press) p459–499
 - [22] Chen X J, Li Z, Bai B M, Cai J P 2011 *ACcta Phys. Sin.* **60** 064215 (in Chinese) [陈小军, 李赞, 白宝明, 蔡觉平 2011 物理学报 **60** 064215]
 - [23] Lasota A, Yorke J 1973 *Transactions Amer Math Soc.* **186** 481
 - [24] Li T Y, Yorke J 1978 *Transactions Amer Math Soc.* **235** 183
 - [25] Eckmann J P, Ruelle D 1985 *Rev. Mod. Phys.* **57** 617

Construction of a class of chaos systems with Markov properties*

Liu Quan^{1)2)†} Li Pei-Yue¹⁾ Zhang Ming-Chao¹⁾
Sui Yong-Xin¹⁾ Yang Huai-Jiang¹⁾

1) (State Key Laboratory of Applied Optics, Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun 130033, China)

2) (Graduate School of Chinese Academy of Sciences, Beijing 100049, China)

(Received 3 April 2013; revised manuscript received 21 May 2013)

Abstract

In this article, a kind of piecewise expanding linear system is constructed. It has a positive Lyapunov exponent as calculated. It is proved that the system has a uniform limit distribution. The formula of the least period of the system is also presented. It is indicated that there is a contradictory relationship between the complexity and the least period of the system when the symbol entropy is applied to the system. The theoretical limit of the complexity of the system with changing parameters is presented. Simulation of the system shows that the sequence generated by the chaos is uniformly distributed. It also tells that the system can have higher complexity but longer least-period than the logistic system and the Tent-Map system. Experiments show that the system is suitable for constructing the cipher.

Keywords: chaos, Markov property, complexity, uniform distribution

PACS: 05.45.-a, 05.45.Ac, 05.45.Tp, 02.50.Ga

DOI: 10.7498/aps.62.170505

* Project supported by the National Basic Research Program of China (Grant No. 2007CB311201), and the Project Development Plan of Science and Technology of Jilin Province (Grant No. 20130522120JH).

† Corresponding author. E-mail: lovefirespread@gmail.com