湘潭大學

数字域上混沌系统动力学的网络分析

答辩人：　冯兵兵

学　号：　201510171812

导　师：　李澄清

选题背景

数字混沌系统动力学退化与抵抗

- 在数字设备上模拟混沌时，相应的动力学系统会在时间和空间两个方向上被离散化，数字化设备的有限字长恶化动力学系统的各项性能
- 抵抗动力学特性退化的各种策略：增大精度、扰动混沌状态、扰动控制参数、级联两个或多个混沌映射、转换多个混沌映射和反馈控制

选题背景

数字混沌系统动力学退化程度的刻画

- 2007年：Oteo等人给出64bit浮点运算下*Logistic*映射舍入误差随控制参数的变化规律
- 2011年：Takeru等人给出量化算法对*Logistic*映射拟混沌轨道的暂态分枝长度和循环长度的影响
- 2012年：Persohn等人给出32bit浮点运算下*Logistic*映射拟混沌轨道的暂态分枝和循环
- 2016年：Uehara等人给出控制参数对*Logistic*映射拟混沌轨道的暂态分枝长度和循环长度的影响
- 2017年：X.Liao等人理论推导出有限域$\mathbb{Z}_{3^n}$上*Logistic*映射拟混沌轨道的最长暂态分支

研究意义

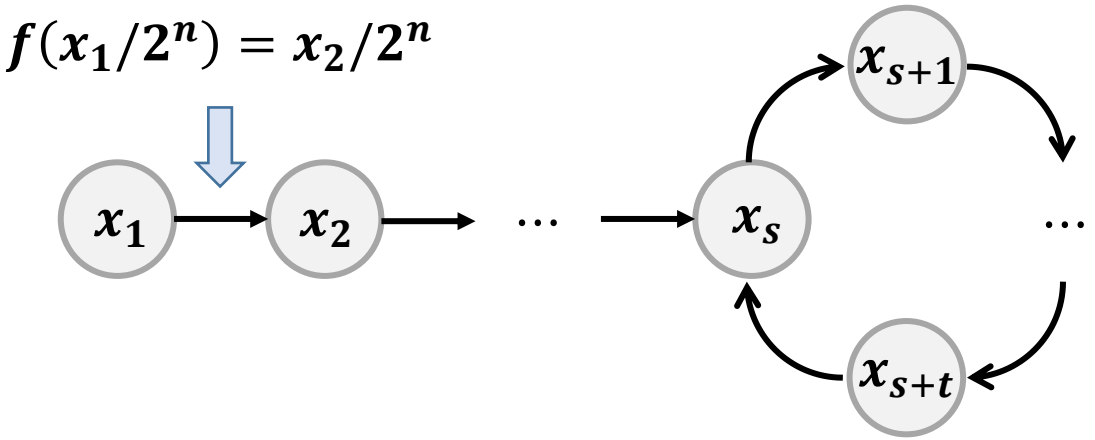
在任何数字世界的应用中各混沌系统的动力学性质因为有限精度效应必然在不同程度上退化。数字混沌动力学性质退化的“可知性”和“可控性”是攸关相关应用的基石

简单有效地从本质结构上检测基于混沌的伪随机数发生器的随机性缺陷

了解有限精度数字域中数字混沌系统的真实结构，从而促进数字混沌动力学退化的有效抵抗和准确评估

研究思路

以计算机中可表示的混沌状态值为点、以两点之间的映射关系（若存在）为边，建立混沌映射对应的状态映射网络(state-mapping network, SMN)。主要通过状态映射网络与实现精度之间的变化关系来研究对应混沌映射的退化过程。



数字化混沌系统的典型拟混沌轨道

主要贡献

Review

- 综述已有相关文献
- 迭代混沌映射的SMN与实现精度之间的一般性质

Logistic

- 定点运算模式下*Logistic*映射的SMN的无标度属性

Tent

- 定点运算模式下*Tent*映射的SMN的入度分布
- 浮点运算模式对该SMN的具体影响
- 这两种运算模式下混沌映射SMN之间的强相关关系

Cat

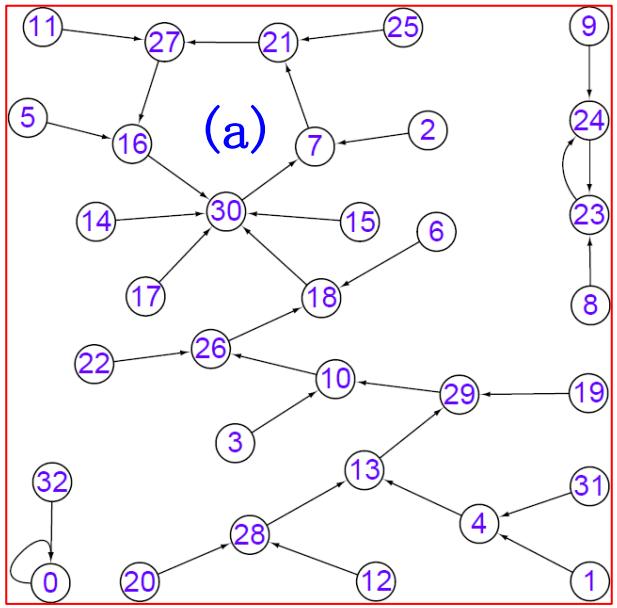
- 二维*Cat*映射的SMN随实现精度增大时的变化性质
- 二维*Cat*映射的周期分布与其SMN结构之间的具体关系

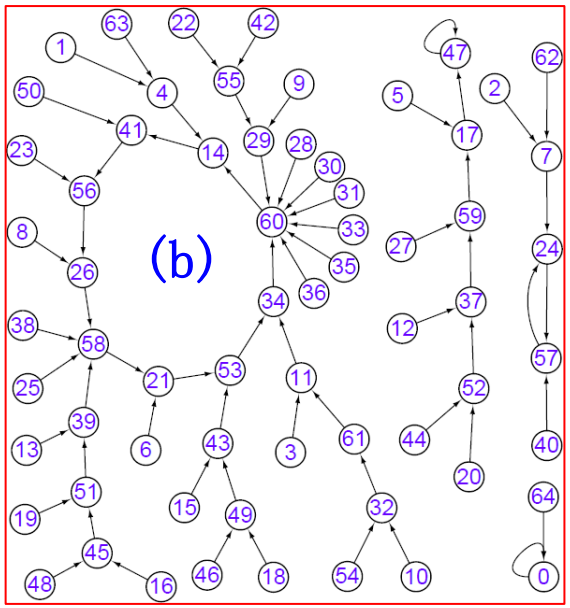
创新之处：

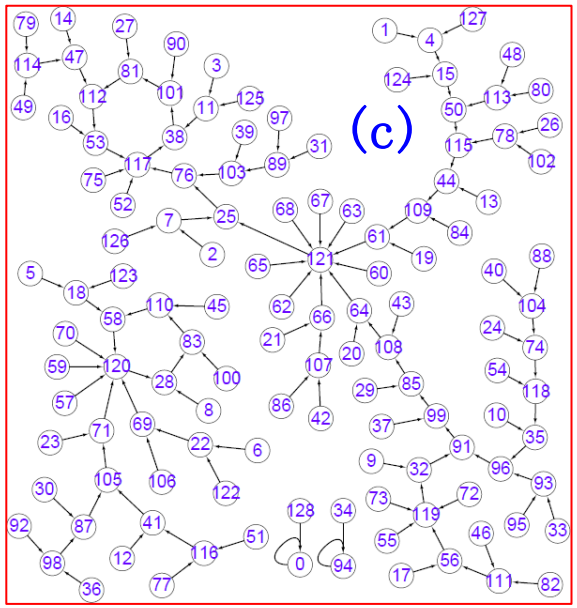
- 从网络空间域的角度来观察和控制混沌系统的动力学性质
- 对数字域中混沌退化生成的各种周期轨道有一个全局把握

研究结果

状态映射网络结构与定点运算精度之间的关系







(a) 定点运算精度5bit时32个状态构成的状态映射网络

(b) 精度增加到6bit时对应的状态映射网络

(c) 精度增加到7bit时对应的状态映射网络

研究结果

- 迭代混沌映射的SMN与实现精度之间的一般性质

性质1 SMN F_{n+1}中节点$(2i)$与SMN F_n中节点 i 满足关系

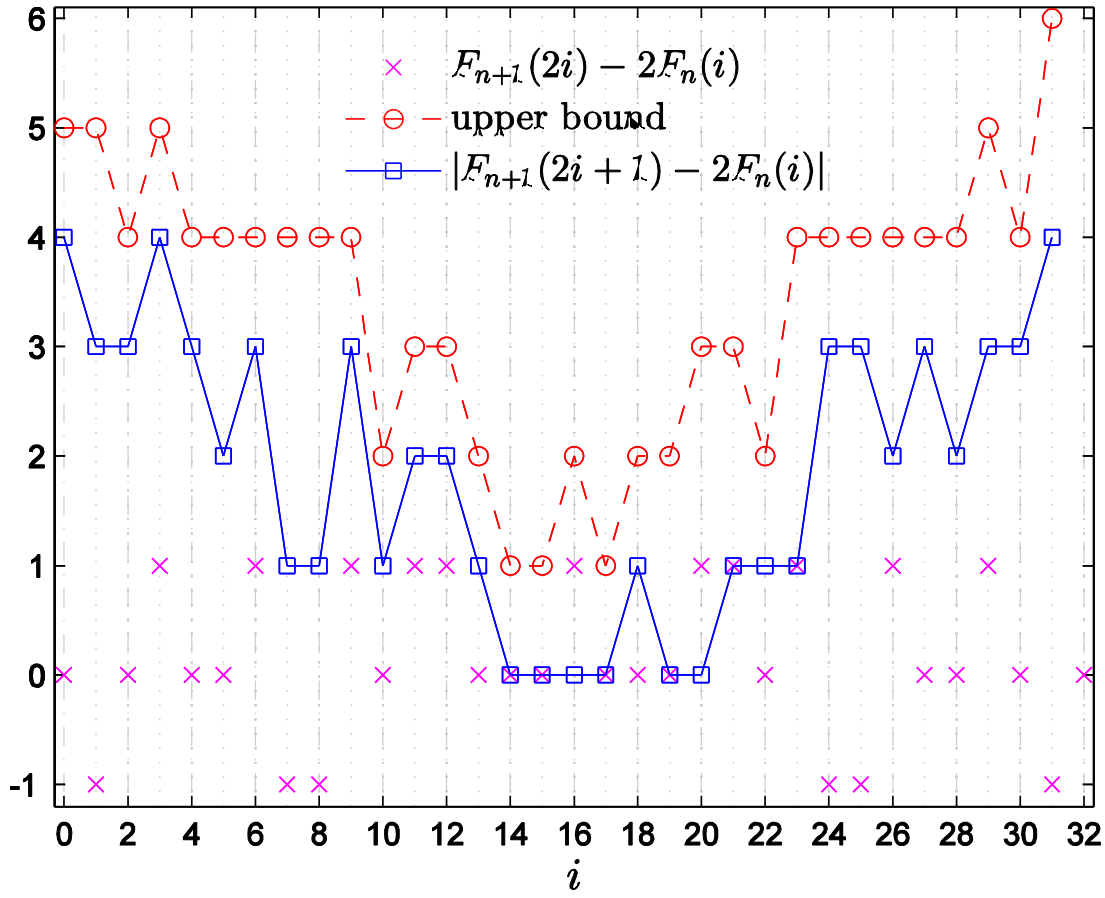
$$F_{n+1}(2i)-2F_n(i)=\begin{cases}1 & r_n\in[0.25,0.5);\\ -1 & r_n\in[0.5,0.75);\ r_n=\mathrm{frac}\left(f_n(i)\cdot 2^n\right).\\ 0 & \text{其他}.\end{cases}$$

性质2 SMN F_{n+1}中节点$(2i\pm 1)$与SMN F_n中节点 i 满足关系

$$\left|F_{n+1}(2i+1)-2F_n(i)\right|\le\left|\mathrm{R}\left(\left(f_{n+1}(2i+1)-f_{n+1}(2i)\right)\cdot 2^{n+1}\right)\right|+\begin{cases}2 & r_n\in[0.25,0.75);\\ 1 & \text{其他}.\end{cases}$$

$$\left|F_{n+1}(2i-1)-2F_n(i)\right|\le\left|\mathrm{R}\left(\left(f_{n+1}(2i-1)-f_{n+1}(2i)\right)\cdot 2^{n+1}\right)\right|+\begin{cases}2 & r_n\in[0.25,0.75);\\ 1 & \text{其他}.\end{cases}$$

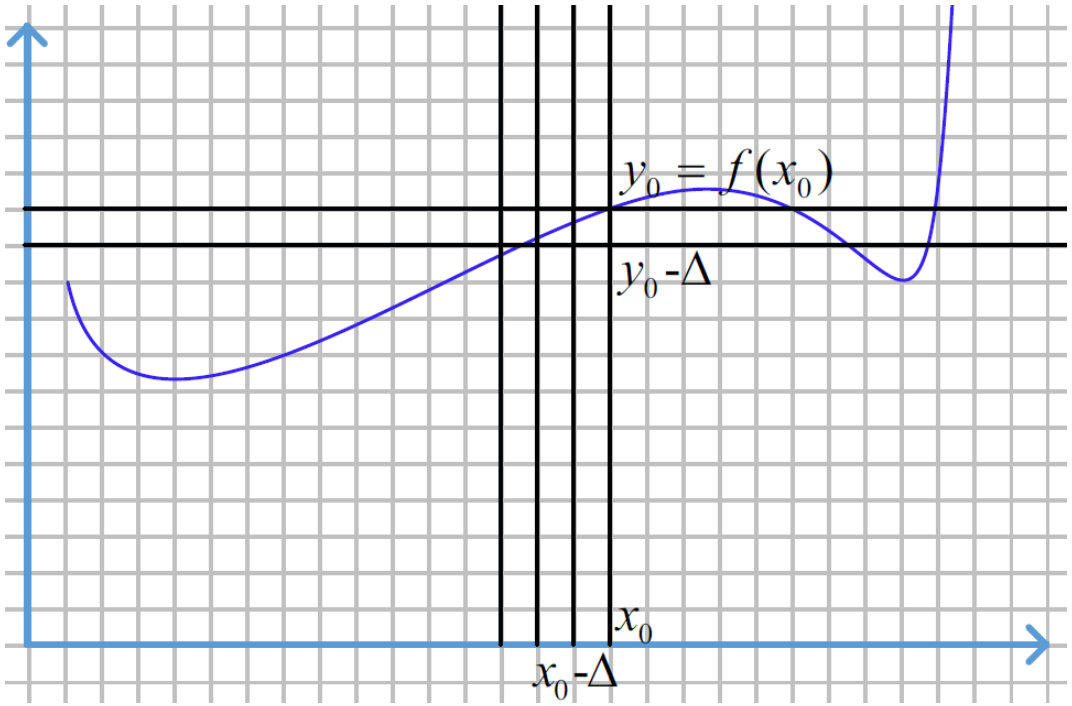
研究结果



***Logistic*映射*SMN* F_6^*与*SMN* F_5^*中对应节点的偏差分布**

研究结果

- 定点运算模式下*Logistic*映射的SMN的无标度属性



数字域上映射原像对应的区间

- 等间隔划分一维映射的定义域和值域，固定间隔$\Delta = 1/2^n$

研究结果

定理1 *Logistic*映射对应*SMN* F_n^* 的节点累积入度分布满足关系

$$P(k)=\left(\frac{2}{\mu k}-\frac{k}{2^{n+1}}\right)^2.$$

$$\Downarrow$$

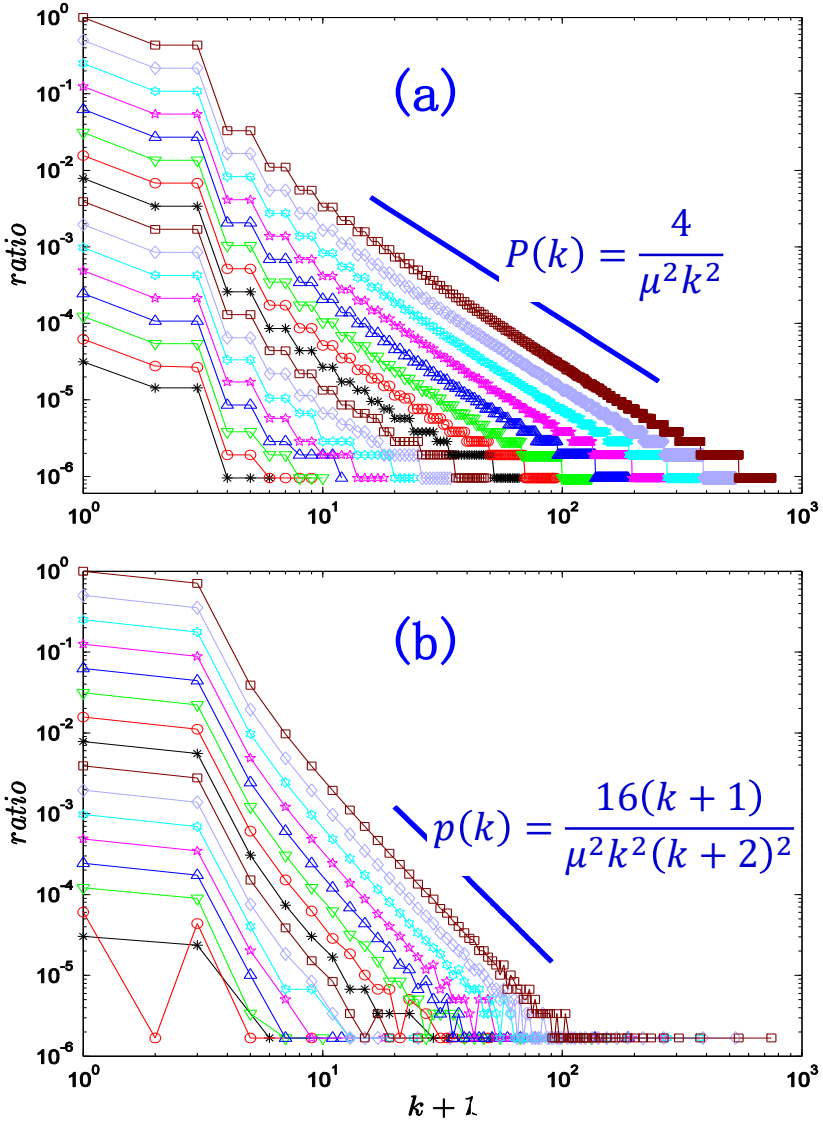
$$\lim_{n\to\infty}P(k)=\frac{4}{\mu^2k^2}.$$

推论1 *Logistic*映射对应*SMN* F_n^* 的节点入度分布满足关系

$$p(k)=(k+1)\left(\frac{16}{\mu^2k^2(k+2)^2}-\frac{1}{2^{2n}}\right).$$

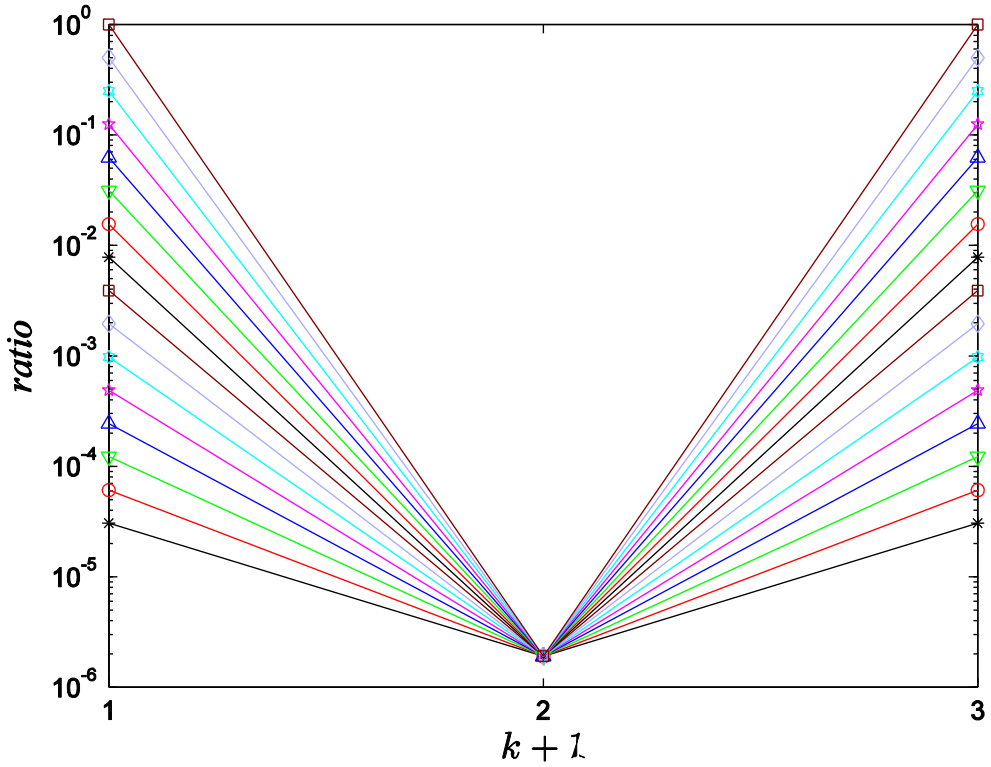
$$\Downarrow$$

$$\lim_{n\to\infty}p(k)=\frac{16(k+1)}{\mu^2k^2(k+2)^2}.$$



研究结果

- 定点运算模式下*Tent*映射的SMN的入度分布



$\boldsymbol{Tent}$映射的状态映射网络$\boldsymbol{F_5^*}$~$\boldsymbol{F_{20}^*}$的入度分布，参数$\boldsymbol{\mu = 31/2^4}$

- $\boldsymbol{Tent}$映射的SMN的节点入度不会随着运算精度的增加而增加

研究结果

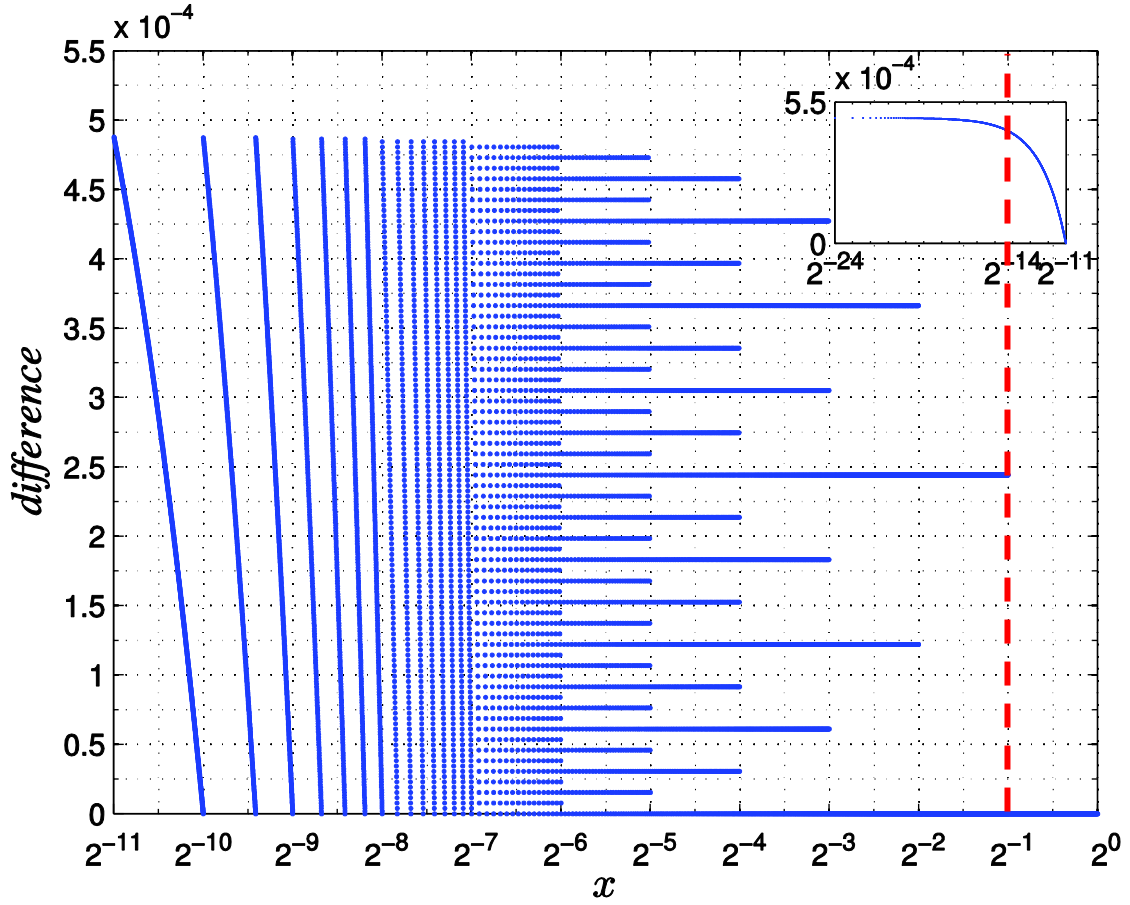
- 浮点运算模式对$Logistic$映射的具体影响

$fl(x)$与$fl\left(1-fl\left(1-fl(x)\right)\right)$有存储量化误差

$$fl\left(1-fl\left(1-fl\left(x\right)\right)\right)\equiv\begin{cases}1-fl\left(1-fl\left(x\right)\right) & x\le 0.5;\\ fl\left(x\right) & x>0.5.\end{cases}$$

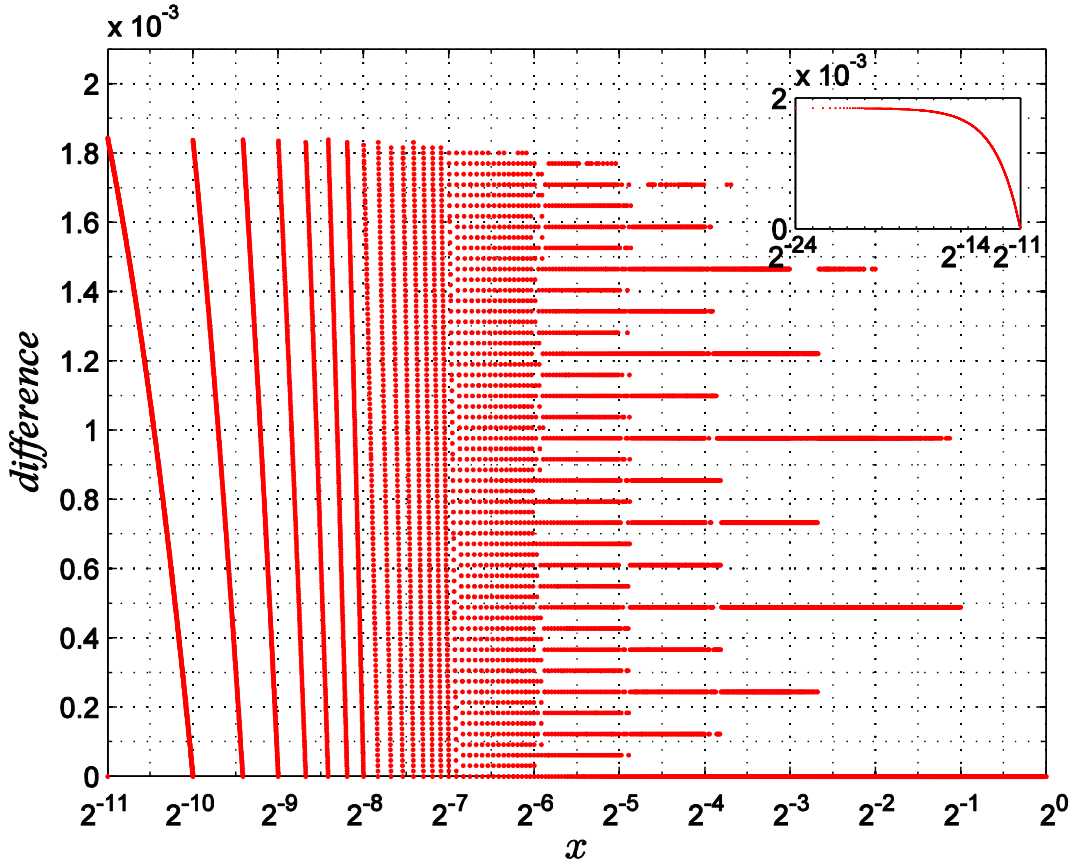
$$f\left(x\right)=\mu\cdot x\cdot\left(1-x\right)\overset{?}{=}f\left(1-x\right)=\mu\cdot\left(1-x\right)\cdot\left(1-\left(1-x\right)\right).$$

研究结果



Binary 16环境下$1-(1-x)$与x的差值关于x的变化规律

研究结果



***Binary* 16环境下$f(1-x)$与$f(x)$的差值关于x的变化规律**

研究结果

- $1-(1-x)$与x的差值关于x分段单调递减
- $f(1-x)$与$f(x)$的差值关于x的变化规律与之类似

***theoretical value*:**

$$fl\left(1-fl\left(1-fl\left(x\right)\right)\right)-fl\left(x\right)=\left(1-fl\left(x\right)\right)-fl\left(1-fl\left(x\right)\right)$$

$$=\begin{cases}\left(\sum_{i=m+2}^{2^{l-1}-2}2^{-i}\right)+\left(\sum_{i=1}^{m}\overline{x}_i\cdot 2^{-i}+2^{-m}\right)\cdot 2^{2-2^{l-1}} & x\in\left(0,2^{2-2^{l-1}}\right);\\ \left(\sum_{i=m+2}^{-(e_1+1)}2^{-i}\right)+\left(\sum_{i=1}^{m}\overline{x}_i\cdot 2^{-i}+2^{-m}\right)\cdot 2^{e_1} & x\in\left(2^{e_1},2^{e_1+1}\right);\\ \left(\sum_{i=m+2+e_2}^{m}\overline{x}_i\cdot 2^{-i}+2^{-m}\right)\cdot 2^{e_2} & x\in\left(2^{e_2},2^{e_2+1}\right);\end{cases}$$

研究结果

- 浮点运算模式对*Tent*映射的具体影响

$$x(0)=(0.b_1b_2\cdots b_j\cdots b_{L-1}b_L)_2\neq 0,\quad b_L=1$$

第*1*次迭代：
$$x(1)=\begin{cases}2x(0)=x(0)\ 1=(0.b_2\cdots b_j\cdots b_{L-1}b_L)_2 & 0\le x(0)<0.5;\\ 2(1-x(0))=(b_1'.b_2'\cdots b_j'\cdots b_{L-1}'b_L)_2 & 0.5\le x(0)<1.\end{cases}$$

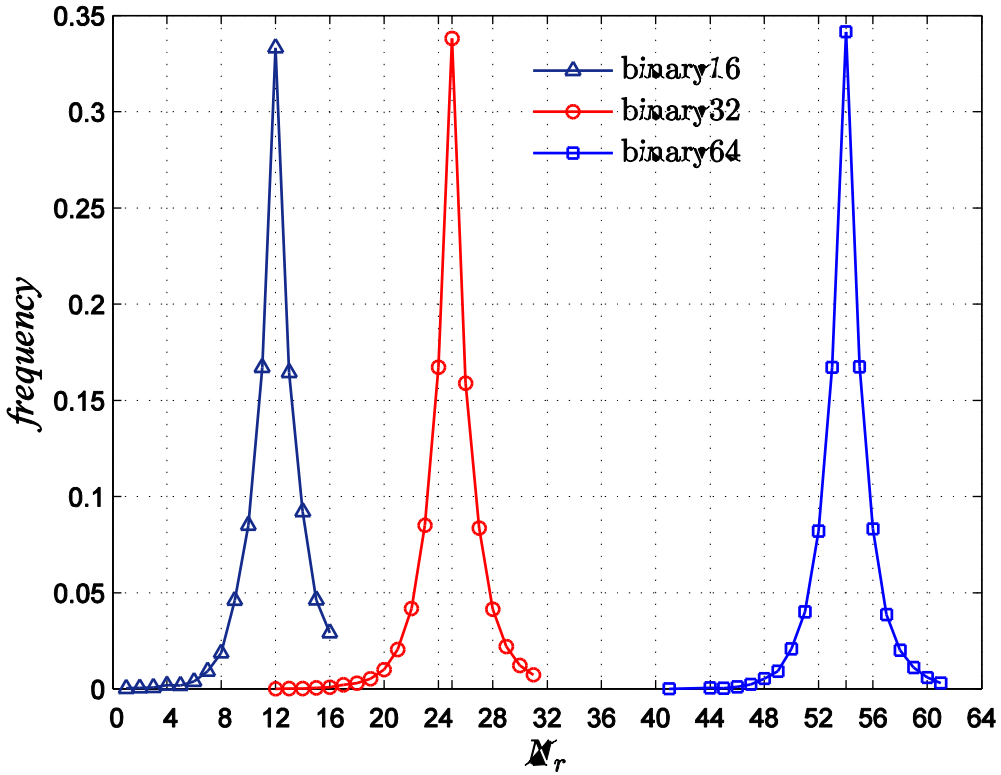
⋮

第*L−1*次迭代：
$$x(L-1)\equiv(0.b_L)_2=(0.1)_2$$

第*L*次迭代：
$$x(L)\equiv 1$$

第*L+1*次迭代：
$$x(L+1)\equiv 0$$

研究结果



x趋于0所需迭代次数N_r的可能数值的出现频率

- 在浮点运算模式中，*Tent*映射的混沌轨道将在有限次迭代中收敛于零，其平均迭代次数通常远小于最大迭代次数

研究结果

$$
\begin{aligned}
E(L) &= Prob[\text{normalized numbers}]\cdot\left(E(e)+\left(m-E(i)\right)\right)+ \\
&\quad Prob[\text{denormalized numbers}]\cdot\left(2^{l-1}-2+m-E(i)\right) \\
&= \frac{2^{l-1}-2}{2^{l-1}-1}\cdot\left(E(e)+\left(m-E(i)\right)\right)+\frac{1}{2^{l-1}-1}\cdot\left(2^{l-1}-2+m-E(i)\right) \\
&\approx \frac{2^{l-1}-2}{2^{l-1}-1}\cdot\left(2+\left(m-1\right)\right)+\frac{1}{2^{l-1}-1}\cdot\left(2^{l-1}-2+m-1\right) \\
&= \frac{\left(2^{l-1}-2\right)\left(m+2\right)+m-1}{2^{l-1}-1}
\end{aligned}
$$

	实验数值	理论数值
binary16	11.95	11.8000
binary32	24.97	24.9764
binary64	54.01	53.9971

研究结果

- 两种运算模式下混沌映射状态映射网络之间的强相关关系

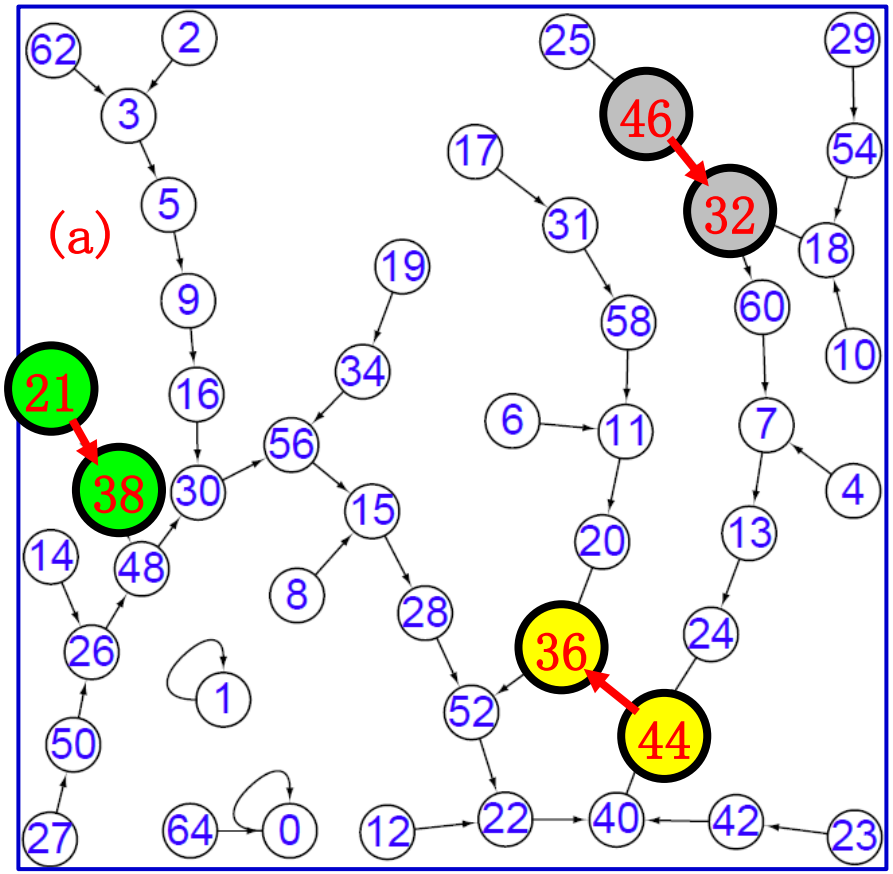
$$\boldsymbol{minimum\ fixed\ interval}: \quad 2^{1-(2^{l-1}-1)} = 2^{2-2^{l-1}-m} \quad \Leftrightarrow \quad \boldsymbol{fixed\ point\ interval}: \quad 2^{-n}$$

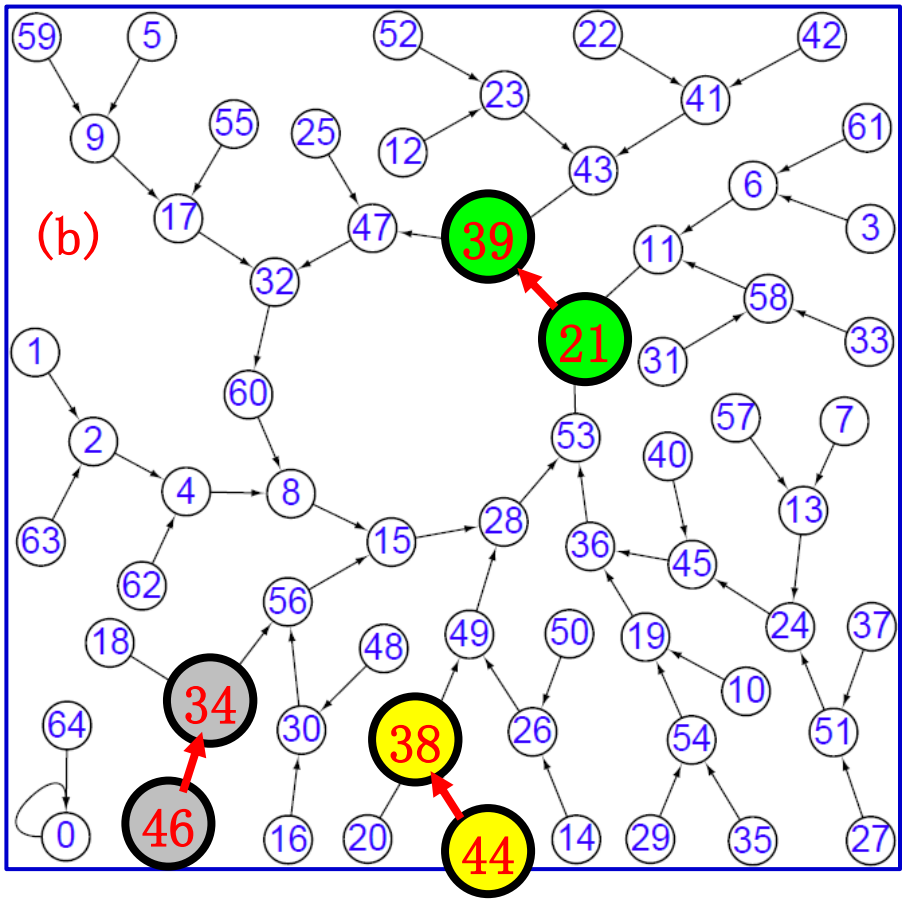
约束条件： $n = m + 2^{l-1} - 2.$

定理2 给定二进制浮点格式参数 l，m，则浮点域上$SMN\ F_{l,m}$与定点域上$SMN\ F_n$满足关系

$$F_n(i) - F_{l,m}(i) \le \begin{cases} 1 & F_n(i) \in [0, 2^m); \\ 2^{n-m-1-j} & F_n(i) \in [2^{n-j-1}, 2^{n-j}). \end{cases}$$

研究结果





(a) 8bit(l=3, m=4)浮点运算下*Tent*映射对应的48个状态构成的状态映射网络

(b) 定点运算精度6bit时*Tent*映射对应的64个状态构成的状态映射网络

研究结果

- 二维Cat映射的状态映射网络随实现精度增大时的变化性质

离散Cat映射矩阵表示：

$$f\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & 1+p\cdot q \end{bmatrix} \cdot \begin{bmatrix} x_n \\ y_n \end{bmatrix} \left(\mathrm{mod}\, N\right), N = 2^e.$$

离散Cat映射对应SMN F_e：

- 将N^2个可能状态看作N^2个节点；
- 若$\mathbb{x}_2 = f(\mathbb{x}_1)$，则对应向量$\mathbb{x}_1 = (x_1, y_1)$的节点指向对应向量$\mathbb{x}_2 = (x_2, y_2)$的节点

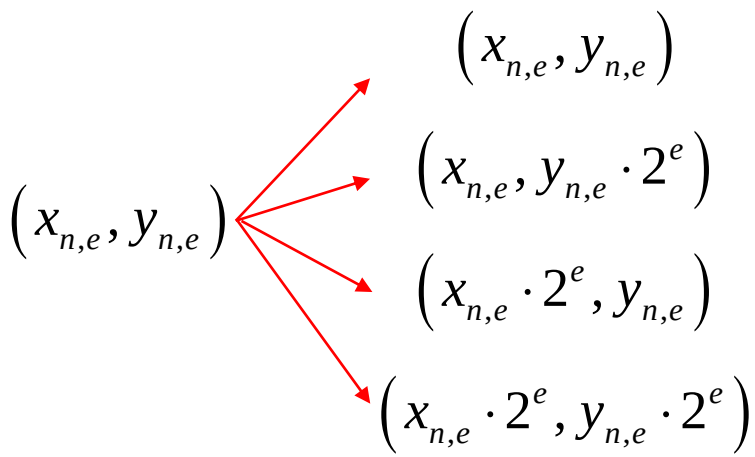
降维处理：$$z_{n,e} = x_{n,e} + \left(y_{n,e}\cdot 2^e\right).$$

研究结果

Cycle：SMN F_e中周期为T_c的*cycle*随着精度增加演化为以下5种可能情况：

- 4个周期为T_c的*cycle*
- 1个周期为$2T_c$的*cycle*和2个周期为T_c的*cycle*
- 2个周期为$2T_c$的*cycle*
- 1个周期为$3T_c$的*cycle*和1个周期为T_c的*cycle*
- 1个周期为$4T_c$的*cycle*

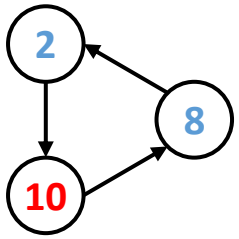
节点：



增加一位最高位

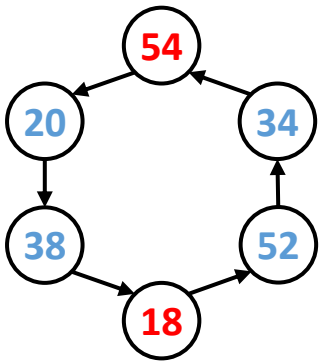
研究结果

$p=1$
$q=3$



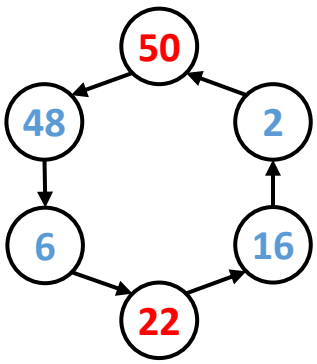
$(10_2, 10_2)$

$e=2$



$(110_2, 110_2)$

$(010_2, 010_2)$



$(010_2, 110_2)$

$(110_2, 010_2)$

$e=3$

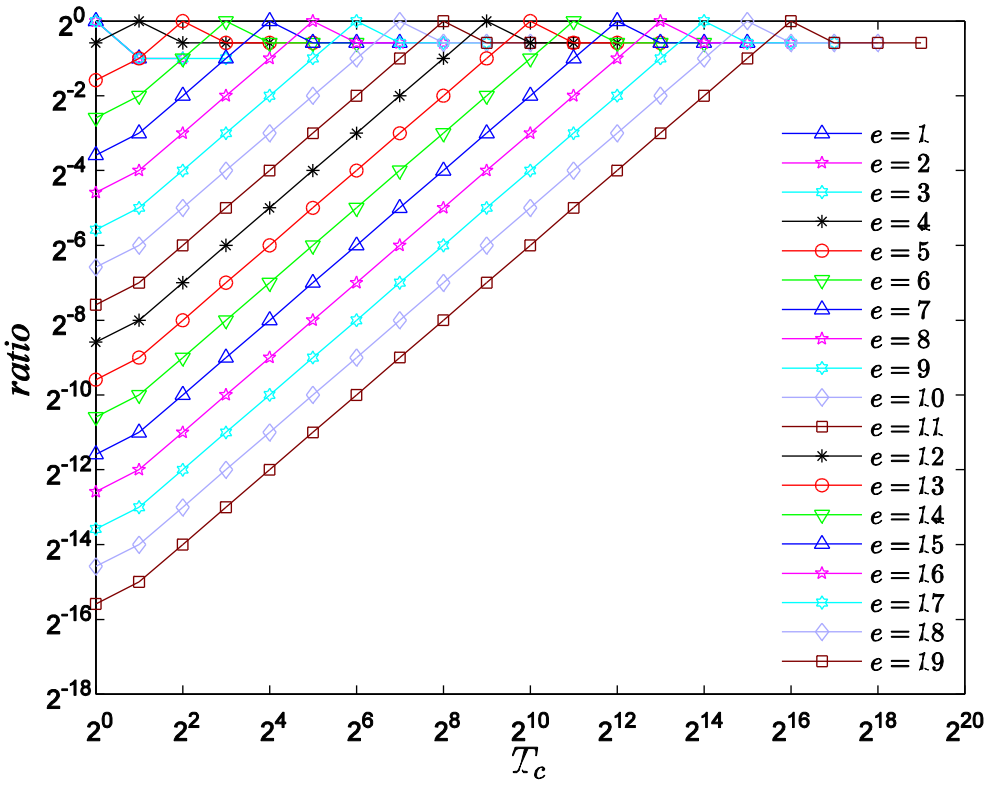
性质3 若$N=2^e$时GDCM的输入$(x_{n,e}, y_{n,e})$与$N=2^{e+1}$时GDCM的输入$(x_{n,e+1}, y_{n,e+1})$满足关系

$$\begin{bmatrix} x_{n,e+1}-x_{n,e} \\ y_{n,e+1}-y_{n,e} \end{bmatrix} = \begin{bmatrix} a_n \\ b_n \end{bmatrix} \cdot 2^e.$$

$$\begin{bmatrix} a_{n+1} \\ b_{n+1} \end{bmatrix} = \left(\begin{bmatrix} 1 & p \\ q & 1+p\cdot q \end{bmatrix} \cdot \begin{bmatrix} a_n \\ b_n \end{bmatrix} + \begin{bmatrix} \lfloor k_x^{'}/2^e \rfloor \\ \lfloor k_y^{'}/2^e \rfloor \end{bmatrix} \right) (\mathrm{mod}\, 2), \quad \begin{bmatrix} k_x^{'} \\ k_y^{'} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & 1+p\cdot q \end{bmatrix} \cdot \begin{bmatrix} x_{n,e} \\ y_{n,e} \end{bmatrix}.$$

研究结果

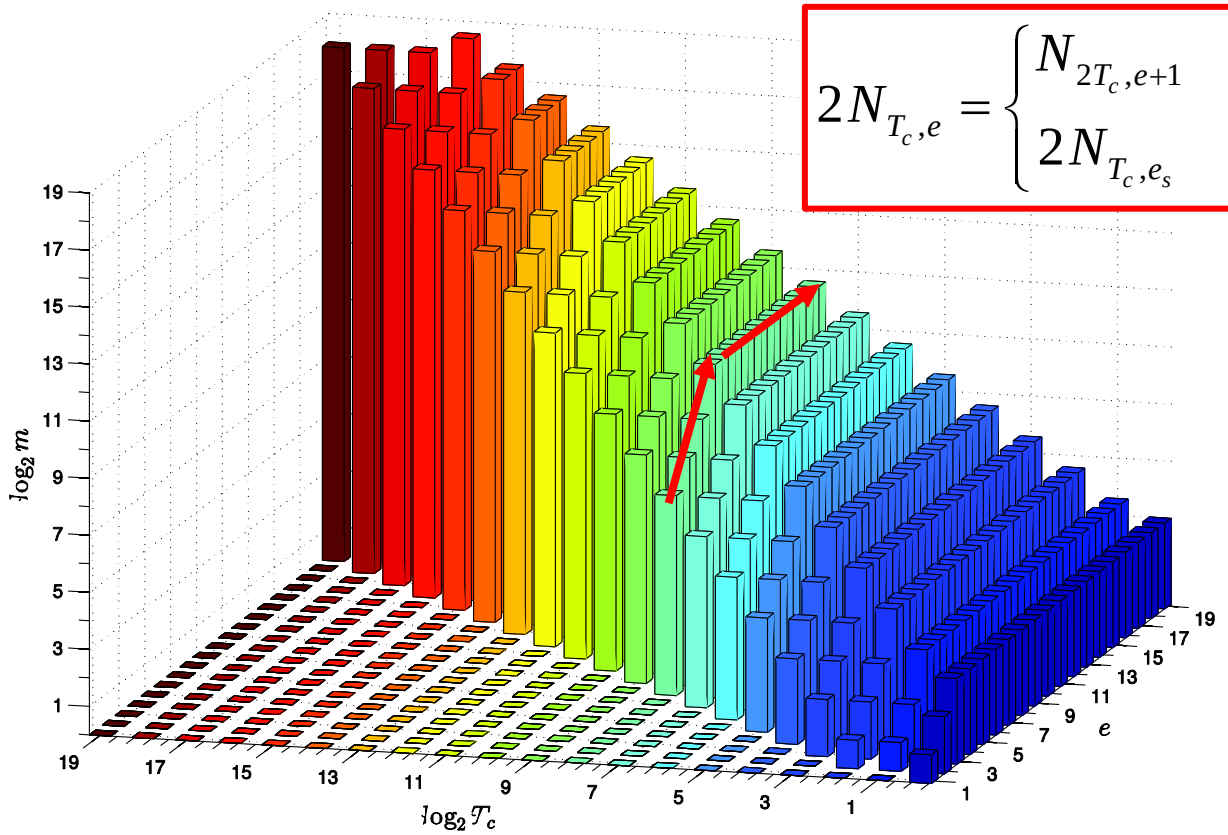
- 二维Cat映射的周期分布与其状态映射网络结构之间的具体关系



- 当e足够大时SMN F_e中$cycle$ 的分布呈指数为1的幂律分布

研究结果

$$2N_{T_c,e} = \begin{cases} N_{2T_c,e+1} & T_c \geq T_s; \\ 2N_{T_c,e_s} & T_c < T. \end{cases}$$



- 周期为T_c的$cycle$ 数量关于实现精度e单调增加，且趋于常数

总结展望

- 运算精度增大时SMN对应节点的量化误差可控，SMN F_{n_μ}的网络结构对SMN F_n的网络结构有决定性影响
- $f''(x) > 0$是混沌映射SMN的节点入度满足幂律分布的充分而非必要条件
- 在浮点运算模式中，数的运算顺序和表示范围会对运算结果产生影响，*Tent*映射的拟混沌轨道将在有限次迭代中收敛于零，其收敛于零的平均迭代次数和最大迭代次数由有关数字运算的细节唯一决定
- 二维*Cat*映射的SMN F_e与SMN F_{e+1}之间具有强相关关系，其周期分布可通过SMN进行准确分析

在学期间发表的学术论文及研究成果

1. Chengqing Li, Bingbing Feng, Shujun Li, Juergen Kurths and Guanrong Chen. Dynamic analysis of chaotic maps as complex networks in the digital domain. arXiv preprint arxiv.org/abs/1410.7694, 2017.
2. Chengqing Li, Bingbing Feng and Jinhu Lü. Comments on ”Period distribution of the generalized discrete Arnold Cat map for N=2e”. submitted to IEEE Transactions on Information Theory, Jan 2018.
3. Chengqing Li, Bingbing Feng and Jinhu Lü. Cryptanalysis of a Chaotic Image Encryption Algorithm Based on Information Entropy. submitted to International Journal of Bifurcation and Chaos, Mar 2018.

谢 谢

感谢母校提供的学习与实践的机会；

感谢导师团队，特别感谢李澄清教授给予的耐心指导；

感谢同学及舍友的帮助；

感谢答辩评审！