学校代码 10530　　学　　号 201510171812

分 类 号 O241.82　　密　　级

湘潭大学

硕 士 学 位 论 文

数字域上混沌系统动力学的网络分析

学 位 申 请 人 冯兵兵

指 导 老 师 李澄清教授

学 院 名 称 信息工程学院

学 科 专 业 计算机科学与技术

研 究 方 向 多值逻辑与信息安全

二〇一八年四月十五日

数字域上混沌系统动力学的网络分析

学 位 申 请 人 冯兵兵

导师姓名及职称 李澄清教授

学 院 名 称 信息工程学院

学 科 专 业 计算机科学与技术

研 究 方 向 多值逻辑与信息安全

学位申请级别 工学硕士

学位授予单位 湘潭大学

论文提交日期 2018-04-15

Network analysis of dynamics of chaotic systems in digital domain

Candidate Bingbing Feng

Supervisor Prof. Chengqing Li

College College of Information Engineering

Program Computer Science and Technology

Specialization Multivalued Logic and Information Security

Degree Master of Engineering

University Xiangtan University

Date Apr. 15th, 2018

湘潭大学
学位论文原创性声明

本人郑重声明：所呈交的论文是本人在导师的指导下独立进行研究所取得的研究成果。除了文中特别加以标注引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写的成果作品。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律后果由本人承担。

作者签名：　　日期：　　年　　月　　日

学位论文版权使用授权书

本学位论文作者完全了解学校有关保留、使用学位论文的规定，同意学校保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅。本人授权湘潭大学可以将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存和汇编本学位论文。

涉密论文按学校规定处理。

作者签名：　　日期：　　年　　月　　日

导师签名：　　日期：　　年　　月　　日

摘　要

混沌系统被广泛用于设计真随机数发生器、伪随机数发生器和安全保密通信算法。然而，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。本文着重研究低维混沌映射在计算机数字域中实现时的动力学性质。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。

本文关于数字混沌系统动力学的研究涉及一维 Logistic 映射、Tent 映射和二维 Cat 映射，研究内容和主要成果包括如下几个方面：

1. 对已有相关研究进行综述发现迭代混沌映射的 SMN 与实现精度之间的一般性质。严格证明了定点运算模式下 Logistic 映射的 SMN 的无标度属性，并分析了浮点运算模式对该 SMN 的具体影响，进而给出了这两种运算模式下 Logistic 映射状态映射网络之间的强相关关系。

2. 将分析对象扩展到 Tent 映射，通过与 Logistic 映射状态映射网络进行对比，阐明了映射本身性质对状态映射网络结构的影响。

3. 进一步研究二维 Cat 映射的状态映射网络随实现精度增大时的变化性质，厘清了二维 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。

本文的研究成果有助于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。

关键词：混沌映射；状态映射网络；动力学退化；伪随机数发生器；周期分布。

Abstract

Chaotic systems are extensively used to design true random number generators, pseudo-random number generators and secure communication algorithms. However, in the digital world, the dynamic properties of the chaotic systems must be degraded to varying degrees due to the finite-precision effect. Understanding and controlling the dynamic properties are related to the basis of any chaos-related application. This thesis focuses on the dynamic properties of low-dimensional chaotic maps implemented in the digital domain. The state-mapping network corresponding to a chaotic map is established by the following way: every representable value in the definition domain of the chaotic map is considered as a node, while a directed edge between a pair of nodes is built if and only if the former node is mapped to the latter one by the chaotic map. Then, the dynamic degradation of the corresponding chaotic map was studied by the relationship between the state-mapping network (SMN) and implementation precision.

The study on the dynamics of digital chaotic systems involves one-dimensional Logistic map, Tent map and two-dimensional Cat map. The main achievements contained in this thesis are as follows:

1. First, we review the existing related studies of the topic and present some general properties between SMN and the implementation precision of iterative chaotic maps. Then, we prove the scale-free property of SMN of the Logistic map in fixed-point arithmetic domain and analyzes specific impact of floating-point operation mode on SMN. The strong correlation between the SMNs of Logistic map obtained with the two arithmetic mode is given.

2. To further disclose the influence of the nature of chaotic map on the structure of SMN, we extends the analysis to Tent map and compare the differences of SMNs of the two chaotic map in the same arithmetic domain.

3. Finally, we further study how SMN of two-dimensional Cat map change as increase of implementation precision and clarify the specific relationship between the cycle distribution of 2-D Cat map and the structure of its SMN.

The obtained results of this thesis are helpful to understand the real structure of digital chaotic system in the finite-precision arithmetic domain and may promote

more effective resistance and accurate evaluation of the dynamical degradation of the digital chaotic systems.
Key Words: Chaotic map, state-mapping network, dynamics degradation, pseudo-random number generator, cycle distribution.

目录

第 1 章　引 言

1.1　课题背景

1.1.1　数字混沌系统动力学退化与抵抗

混沌现象在自然界和数学模型中普遍存在，理解混沌现象中隐含的动力学行为很重要。作为非线性科学的一个令人难以置信的重要分支，混沌动力学是自二十世纪 70 年代迅速发展起来的一门交叉科学，涉及生物学 [1]、化学 [2]、物理学 [3–5]、数学 [6–9] 和工程领域 [10,11]，也是混沌理论和非线性科学领域的基础课题 [12–15]。由于混沌系统具有分形、初值敏感性和混沌吸引子等特性，因此其动力学行为很难预测。混沌因此用于设计真随机数发生器、伪随机数发生器和安全保密通信算法。

当我们在数字计算机上模拟混沌时，相应的动力学系统会在时间和空间上被离散化 [16,17]。对于数字化混沌系统而言，由于混沌系统都是在有限精度下实现的，数字设备的有限字长恶化了混沌系统的各项性能，降低了相关应用的效能 [18,19]。尽管一些研究者指出如果数字计算机的字长足够大（例如，大于 16 位），非线性混沌系统在计算机上有近似混沌行为，但在有限精度下数字混沌系统普遍存动力学特性退化 [20]，因为在有限精度数字域（或有限状态机）中舍入误差和截断误差（算法误差）会影响运算结果，使之与理论值存在偏差 [21,22]。1988 年，Yorke 等人发现 Ikeda 映射的轨道周期的期望值随着舍入精度的变化而变化 [23]。为了理解连续混沌变为数字混沌的过程中混沌系统动力学的退化，2005 年，S. LI 等人提出一些度量分段线性混沌映射的动力学退化程度的客观指标 [24]。混沌系统被广泛应用于安全保密通信算法，但数字混沌系统的动力学退化可能会大大降低混沌保密算法的安全性 [25]。

为了抵抗数字混沌系统的动力学特性退化，各种各样的应对策略被提出：增大精度 [26]、扰动混沌状态 [27–30]、扰动控制参数 [31]、级联两个或多个混沌映射 [32]、在多个混沌映射之间切换 [33,34] 和反馈控制 [35,36]。上述方法通常被用于改善混沌伪随机数发生器的随机性能。许多研究者认为通过混沌迭代生成的伪随机数序列很大程度上保留了原始混沌映射的复杂动力学特性 [37]。事实上，早在 1947 年，John von Neumann 已经提出将 Logistic 映射作为伪随机数发生器 (PRNG) [38]。此后，大量基于混沌映射及其演化的伪随机数发生器 (PRNG) 被提出，例如 Logistic 映射 [28–30,36,37]、Tent 映射 [39–41]、Sawtooth 映射 [42]、Rényi 混沌映射 [43]、Cat 映射 [44] 等。当我们应用混沌伪随机数发生器生成伪随机数时 [36,41,45]，面对如此多的可供选择的伪随机数生成器，一个很重要的问题是如何简单有效地从本质结构上检测其随机性缺陷，并对其进行改进。

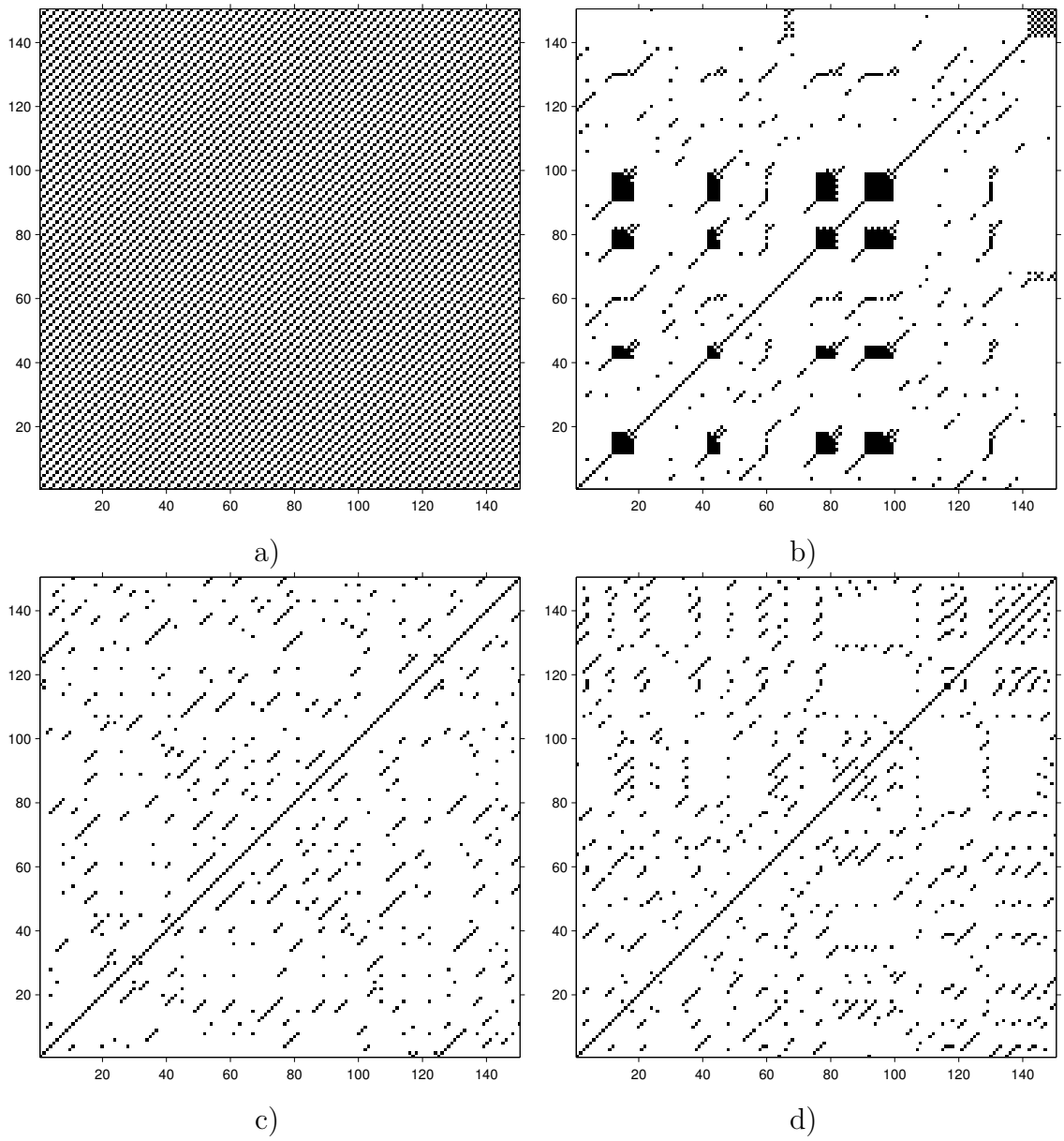


图 1.1 Logistic 映射不同动力学状态的递归图：a) $\mu = 3.830$；b) $\mu = 3.679$；c) $\mu = 3.791$；d) $\mu = 4$

1.1.2 数字混沌系统动力学退化程度的刻画

由于数字混沌系统动力学特性的退化对其在现实生活和工程领域中的应用有不可忽略的影响，对数字混沌动力学性质的研究开始受到人们的重视。事实上，对数字混沌系统动力学性质分析的忽视是一些安全保密通信算法容易被破解的本质原因。与混沌相关的早期研究发现，由于“鸽巢原理”和混沌系统可能状态的有限性，基于混沌迭代的伪随机状态序列经历一个暂态过程后将进入周期性循环 [46,47]。2007 年，Oteo 等人详细研究了 Logistic 映射在双精度计算中存在的舍入误差随控制参数的变化规律 [21]。2011 年，Takeru 等人给出的实验结果表明，不同舍入方法对 Logistic 映射拟混沌轨道的暂态分枝长度和循环 (*cycle*) 长度有不同影响，

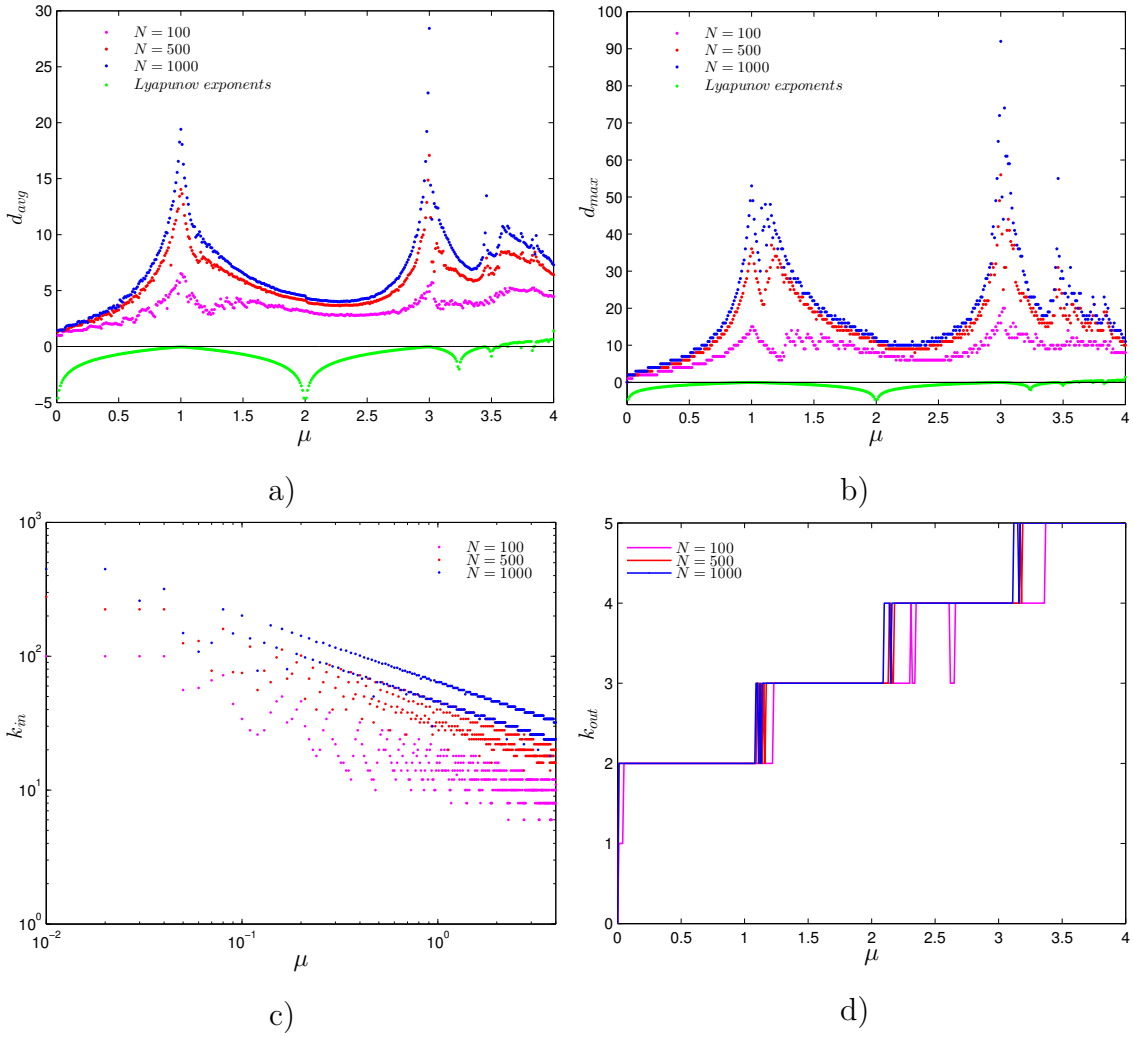


图 1.2 Logistic 映射的子区间映射网络的不同参数指标随控制参数 μ 的变化规律：a) 平均路径长度 d_{avg}；b) 最大路径长度 d_{max}；c) 最大入度 k_{in}；d) 最大出度 k_{out}

Logistic 映射产生的状态序列的性质严重依赖于舍入方法 [48]。2012 年，Persohn 等人使用高吞吐计算在单精度浮点域上穷举计算了 Logistic 映射拟混沌轨道的暂态分枝和循环 [20]。2016 年，Uehara 等人揭示了 Logistic 映射的控制参数对其状态序列的暂态分枝长度和循环长度的影响 [49]。Tsuchiya 在 2016 年也给出有限域上控制参数为 4 的 Logistic 映射产生的状态序列周期的一些性质，并通过数值实验发现状态序列具有较长周期时控制参数和初始值的条件以及周期的渐近性质 [50]。2017 年，X. Liao 等人进一步推导出了有限域 $\mathbb{Z}_{3^n}$ 上 Logistic 映射状态序列的最大周期 [51]。此外，2012 年、2013 年，F. Chen 使用 Hensel 上升法准确推导出了任意精度下二维离散 Cat 映射的周期分布，对离散 Cat 映射周期分布的充分认识有助于 Cat 映射在水印和加密算法设计与分析中的应用 [44,52]。2016 年，Yoshioka 首先详细分析了 2 的整数幂余数环上切比雪夫多项式产生的状态序列的周期性质，分析表明，基于 2 的整数幂余数环上切比雪夫多项式的公钥密码系统并不安全 [53]。最近，他又进一步推导出了奇素数的整数幂余数环上切比雪夫多项式的状态序列周期 [54]。

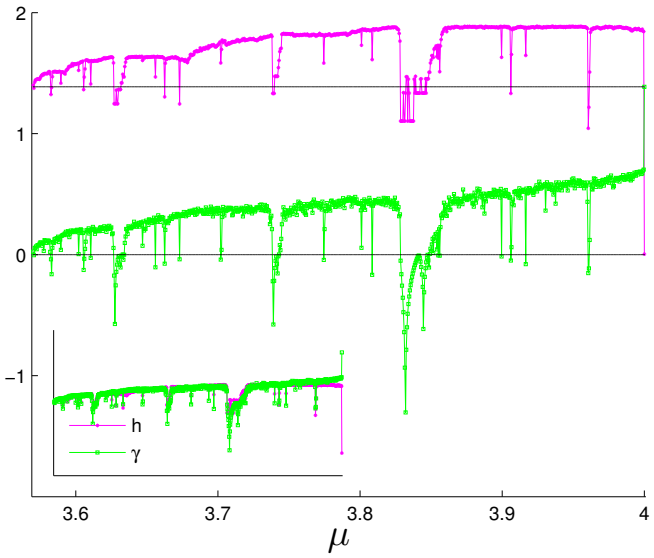


图 1.3 Logistic 映射网络熵 h 和 Lyapunov 指数 γ 随控制参数 μ 的变化规律

很多研究者侧重于状态网络中路径的分析，常常忽略数字域上给定混沌映射的所有可能状态之间的网络关系的存在 [55]。由于复杂网络可以用来研究传统理论数学模型不能准确描述的复杂非线性系统 [15,56–59]，它已经成为研究混沌系统动力学的有效工具。1986 年，Binder 等人绘制了 5 比特定点运算域上 Logistic 映射的状态网络，从复杂网络的角度对其动力学特性进行了分析，并指出混沌动力学特性的一些度量指标同样适用于状态映射网络 (SMN)，如李雅普诺夫指数和熵 [60]。1992 年，Binder 等人通过实验进一步研究了极限环数量和最大环周期随定点精度的变化规律 [61]。2007 年，Shreim 等人通过复杂网络参数对基于元胞自动机的时间序列动力学进行了分类 [62]，但 C. Xu 发现其中一些理论分析是错误的，基于状态映射网络的两个参数指标不能区分由一维元胞自动机组成的离散动力系统的复杂动力学行为 [63]。Kyriakopoulos 和 Thurner 也通过子区间映射网络进一步探讨了复杂网络参数与混沌动力学特性度量指标之间的一致性（详见图 1.2） [64]。2008 年，X. Xu 等人研究了混沌映射状态网络中指定 4 节点子图的相对频率，并根据指定 4 节点子图的相对频率对混沌映射进行了重新分类 [65]。2011 年，Luque 等人通过 Feigenbaum 图揭示了网络熵随控制参数的变化规律，发现其与李雅普诺夫指数随控制参数的变化规律相似（详见图 1.3） [66]。此外，为了进一步挖掘隐含在非线性时间序列中的重要信息，Donner 等人在 2011 年提出了一种基于网络的非线性时间序列分析框架（详见图 1.1） [67]。

尽管在数字混沌动力学领域有为数不多的研究者考虑过这个问题，我们认为关于数字混沌系统动力学性质的讨论是非常重要的。更重要的是，在非线性科学领域，大多数人并不关心计算机如何执行浮点运算，而是将计算机作为黑匣子来实现混沌系统，因此，在计算机上实现的数字混沌系统的本质结构仍未可知。此外，由于随机实验的局限性，很多研究者常常忽略可能以很低概率出现的某些重要细节。

1.2 主要内容

本文将以一维 Logistic 映射、Tent 映射和二维离散 Cat 映射为主要分析对象，从状态映射网络的角度出发研究数字域上混沌系统的动力学性质，论文后续章节的内容安排如下：

第二章首先揭示了定点运算域上一维混沌系统状态映射网络的基本性质，对定点运算域上 Logistic 映射的 SMN F_e 与 SMN F_{e+1} 对应节点间的关系进行了具体分析；其次，从理论上推导出了定点运算域上 Logistic 映射状态网络的节点入度分布和累积入度分布，发现 Logistic 映射状态网络具有无标度属性；然后，以 Logistic 映射为例厘清了浮点运算域上系统量化误差对运算的影响，发现运算顺序和参与运算的数值范围会对运算结果产生影响，即改变运算顺序，运算结果可能不同；最后，利用有限域上混沌系统的状态映射网络对混沌伪随机数发生器进行了分类，分析发现，混沌系统状态映射网络可对其随机性能进行粗检测。

第三章主要讨论了分段线性 Tent 映射的相关动力学性质，首先推导分析了定点运算域上其 SMN F_e 与 SMN F_{e+1} 对应节点间的准确关系；其次，揭示了定点运算域上 Tent 映射状态网络的节点入度分布和累积入度分布，发现其节点入度仅有三种可能取值；然后，从理论上推导出了计算机内存中 Tent 映射迭代初值 $x(0)$ 尾数位的无效位数 i 的数学期望及 $x(0)$ 的阶码 e 的数学期望，进而推导出了数字计算机上 Tent 映射迭代值趋于零所需迭代次数；最后，厘清了定点运算域上混沌系统状态映射网络与浮点运算域上其对应状态映射网络之间的关系，即浮点运算域上混沌系统状态映射网络可由定点运算域上其对应状态映射网络生成。

第四章首先厘清了 F. Chen 等人于 2013 年提出的有限域上周期为 T 的不同 Cat 映射的数量 N_T 与二维离散 Cat 映射周期 T 之间的关系；其次，采用降维的方法对定点运算域上二维离散 Cat 映射 SMN F_e 与 SMN F_{e+1} 之间的关系进行了深入分析；最后，通过随机实验揭示了二维离散 Cat 映射的环分布规律，发现其环分布呈指数为 1 的幂律分布。

最后一章总结全文，对本文研究过程中遇到的一些问题进行了归纳整理。

第 2 章　一维 Logistic 映射的状态网络分析

2.1　定点域上一维混沌映射的基本性质

给定映射 f: $[0,1] \to [0,1]$，定点运算精度 n 和量化策略，可通过以下方式构造对应的状态映射网络 F_n：1) 将 2^n 个可能状态看作 2^n 个节点；2) 若 $f(i/2^n) = j/2^n$，则节点 i 指向节点 j。为了表述方便，我们下面用 $f_n(i)$ 来表示 $f(i/2^n)$。令

$$F_n(i) = \mathrm{R}\left(f_n(i) \cdot 2^n\right),$$

其中 $\mathrm{R}(\cdot)$ 为量化函数，例如向下取整、向上取整和四舍五入 (这里只考虑四舍五入)。

根据上述定义，可以很容易证明以下关于 F_n 和 F_{n+1} 之间关系的性质。

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

$$F_{n+1}(2i) - 2F_n(i) = \begin{cases} 1 & r_n \in [0.25, 0.5); \\ -1 & r_n \in [0.5, 0.75); \\ 0 & \text{其他}, \end{cases} \tag{2.1}$$

其中

$$r_n = \mathrm{frac}(f_n(i) \cdot 2^n),$$

$\mathrm{frac}(x) = x - \lfloor x \rfloor$, $i \in \{0, \cdots, 2^n\}$，$\lfloor x \rfloor$ 表示不大于实数 x 的最大整数。

证 因为 $F_{n+1}(2i) = \mathrm{R}\left(2 \cdot f_{n+1}(2i) \cdot 2^n\right)$，另外，

$$f_{n+1}(2i) \equiv f_n(i), \tag{2.2}$$

根据上述条件可推知

$$F_{n+1}(2i) - 2F_n(i) = \mathrm{R}\left(2 \cdot f_n(i) \cdot 2^n\right) - \mathrm{R}\left(f_n(i) \cdot 2^n\right).$$

又因为

$$\mathrm{R}(2x) = 2 \cdot \mathrm{R}(x) + \begin{cases} 0 & 0 \le \mathrm{frac}(x) < 0.25; \\ 1 & 0.25 \le \mathrm{frac}(x) < 0.5; \\ -1 & 0.5 \le \mathrm{frac}(x) < 0.75; \\ 0 & 0.75 \le \mathrm{frac}(x) \le 1, \end{cases}$$

从而上述性质得以直接证明。 ■

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

$$\begin{aligned} |F_{n+1}(2i+1) - 2\cdot F_n(i)| \;\leq\; & \left|\mathrm{R}\left((f_{n+1}(2i+1) - f_{n+1}(2i))\cdot 2^{n+1}\right)\right| \\ & + \begin{cases} 2 & r_n \in [0.25, 0.75); \\ 1 & \text{其他}, \end{cases} \end{aligned} \tag{2.3}$$

其中 $i \in \{0, \cdots, 2^n - 1\}$。

证 根据绝对值三角不等式 $|a+b| \leq |a| + |b|$ 可得

$$|F_{n+1}(2i+1) - 2\cdot F_n(i)| \;\leq\; |F_{n+1}(2i+1) - F_{n+1}(2i)| + |F_{n+1}(2i) - 2\cdot F_n(i)|. \tag{2.4}$$

对任意实数 x，y，恒有

$$|\mathrm{R}(x) - \mathrm{R}(y)| \leq |\mathrm{R}(x-y)| + 1. \tag{2.5}$$

因此

$$\begin{aligned} |F_{n+1}(2i+1) - F_{n+1}(2i)| &= \left|\mathrm{R}\left(f_{n+1}(2i+1)\cdot 2^{n+1}\right) - \mathrm{R}\left(f_{n+1}(2i)\cdot 2^{n+1}\right)\right| \\ &\leq \left|\mathrm{R}\left(f_{n+1}(2i+1)\cdot 2^{n+1} - f_{n+1}(2i)\cdot 2^{n+1}\right)\right| + 1. \end{aligned} \tag{2.6}$$

将上述不等式和等式 *(2.1)* 代入不等式 *(2.4)*，该性质即可得证。 ■

性质 3 F_{n+1} 中节点 $(2i-1)$ 和 F_n 中节点 i 满足关系

$$\begin{aligned} |F_{n+1}(2i-1) - 2\cdot F_n(i)| \;\leq\; & \left|\mathrm{R}\left((f_{n+1}(2i-1) - f_{n+1}(2i))\cdot 2^{n+1}\right)\right| \\ & + \begin{cases} 2 & r_n \in [0.25, 0.75); \\ 1 & \text{其他}, \end{cases} \end{aligned} \tag{2.7}$$

其中 $i \in \{1, \cdots, 2^n\}$。

证 根据绝对值三角不等式 $|a+b| \leq |a| + |b|$ 可得

$$|F_{n+1}(2i-1) - 2\cdot F_n(i)| \;\leq\; |F_{n+1}(2i-1) - F_{n+1}(2i)| + |F_{n+1}(2i) - 2\cdot F_n(i)|. \tag{2.8}$$

根据性质 *3*，应用不等式 *(2.5)* 可得

$$\begin{aligned} |F_{n+1}(2i-1) - F_{n+1}(2i)| &= \left|\mathrm{R}\left(f_{n+1}(2i-1)\cdot 2^{n+1}\right) - \mathrm{R}\left(f_{n+1}(2i)\cdot 2^{n+1}\right)\right| \\ &\leq \left|\mathrm{R}\left(f_{n+1}(2i-1)\cdot 2^{n+1} - f_{n+1}(2i)\cdot 2^{n+1}\right)\right| + 1. \end{aligned} \tag{2.9}$$

将上述不等式和等式 *(2.1)* 代入不等式 *(2.8)* 中，该性质即可得证。 ■

2.2 定点域上 Logistic 映射的性质分析

2.2.1 数字化 Logistic 映射的定义

Logistic 映射是研究动力系统、混沌、分形等复杂系统行为的一个经典模型，早在 20 世纪 50 年代，就被生态学家用来描述种群的变化，在保密通信领域的应用也十分广泛，其数学表达式为

$$f(x) = \mu \cdot x \cdot (1 - x), \tag{2.10}$$

其中 $x \in [0, 1]$，$\mu \in (0, 4]$。

在精度为 n 的定点运算域上，Logistic 映射 $f(x) = \mu \cdot x \cdot (1 - x)$ 变为

$$f_n(i) = (N_\mu / 2^{n_\mu}) \cdot (i/2^n) \cdot (1 - i/2^n), \tag{2.11}$$

其中 N_μ 属于集合 $\{0, \cdots, 2^{n_\mu+2}\}$ 里的奇数，$\mu = N_\mu/2^{n_\mu}$，且 $n_\mu \le n$。

图 2.1为相同控制参数、不同运算精度下 Logistic 映射的状态映射网络。

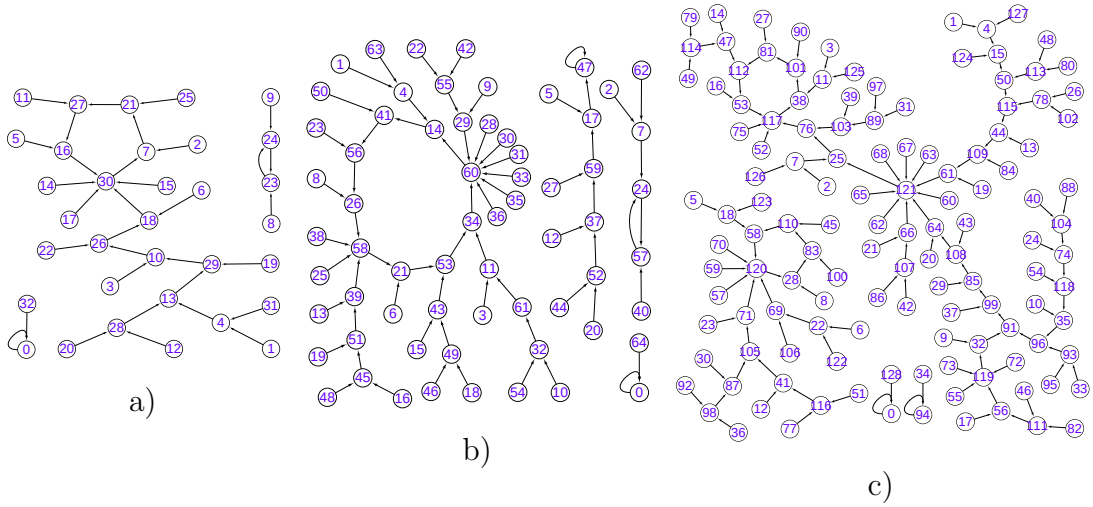


图 2.1 控制参数 $\mu = 121/2^5$ 时，Logistic 映射的状态映射网络：a) 5 比特精度；b) 6 比特精度；c) 7 比特精度

从图 2.1可观察到数字混沌系统状态映射网络的如下基本特征：

- 整个状态映射网络由少量弱连通分量构成。（弱连通分量是有向图的最大子图；有向图中任意两点之间有且只有一条有向路径相连。）
- 每个弱连通分量有且仅有一个自环或环路。
- 弱连通分量中的每个节点经过一个“暂态”过程都会连向其循环。

从图 2.1可以进一步观察到，Logistic 映射的状态映射网络具有以下特征，即最大弱连通分量的节点数占整个状态映射网络节点数的一半以上 [68]。

2.2.2 Logistic 映射的状态映射网络与实现精度之间的关系

推论 1 F^*_{n+1} 中节点 $(2i+1)$ 和 F^*_n 中节点 i 满足关系

$$\left|F^*_{n+1}(2i+1) - 2\cdot F^*_n(i)\right| \le \begin{cases} 6 & r_n \in [0.25, 0.75); \\ 5 & \text{其他}, \end{cases}$$

其中 $i \in \{0, \cdots, 2^n - 1\}$，且 $n \ge 3$。

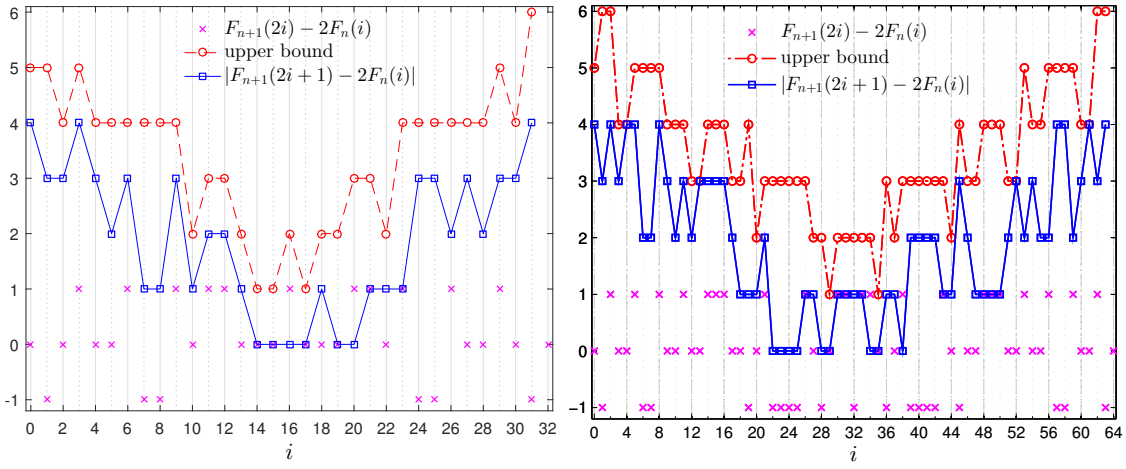
证 将等式 *(2.11)* 带入不等式 *(2.3)*，可得

$$\begin{aligned} \left|F^*_{n+1}(2i+1) - 2\cdot F^*_n(i)\right| &\le \left|\mathrm{R}\left(\left(N_\mu/2^{n_\mu+2}\right)\cdot\left(4-(1+4i)/2^{n-1}\right)\right)\right| \\ &\quad + \begin{cases} 2 & r_n \in [0.25, 0.75); \\ 1 & \text{其他}. \end{cases} \end{aligned}$$

由于 $(N_\mu/2^{n_\mu+2}) \in [0,1]$，进一步可得

$$\begin{aligned} \left|F^*_{n+1}(2i+1) - 2\cdot F^*_n(i)\right| &\le \left|\mathrm{R}\left(4-(1+4i)/2^{n-1}\right)\right| + \begin{cases} 2 & r_n \in [0.25, 0.75); \\ 1 & \text{其他}, \end{cases} \\ &\le \begin{cases} 6 & r_n \in [0.25, 0.75); \\ 5 & \text{其他}. \end{cases} \end{aligned}$$

■



a) b)

图 2.2 F^*_n 与 F^*_{n+1} 中对应节点的差值分布：a) $n=5$；b) $n=6$

根据推论 1可知，$|F^*_{n+1}(2i+1) - 2\cdot F^*_n(i)|$ 的上界取决于 i 和 N_μ。图 2.2 a) 为图 2.1 a) 中每个节点对应的差值 $|F^*_{n+1}(2i+1) - 2\cdot F^*_n(i)|$ 和 $F^*_{n+1}(2i) - 2F^*_n(i)$，为进一步分析比较 F^*_n 和 F^*_{n+1} 的关系，图 2.1 b) 中每个节点对应的差值如图 2.2 b) 所示。

性质 4 状态映射网络 $F^*_{n_\mu}$ 对 F^*_n 有决定性影响。

证 根据性质 *1*和推论 *1*，F^*_n 可由 F^*_j 逐步演化而来，其中 $j = n_\mu \sim n$。因为演化前后状态映射网络对应节点的量化误差可控，因此 $F^*_{n_\mu}$ 的初始结构对 F^*_n 有决定性影响。 ■

2.2.3 Logistic 映射 SMN 入度分布的理论推导

定理 1 *Logistic* 映射对应状态映射网络 F^*_n 的节点累积入度分布满足关系

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

证 给定量化策略，在精度为 n 的定点运算域上，任意一维映射的定义域和值域可被等间隔划分，其中 $\Delta = 1/2^n$，如图 *2.3*所示。

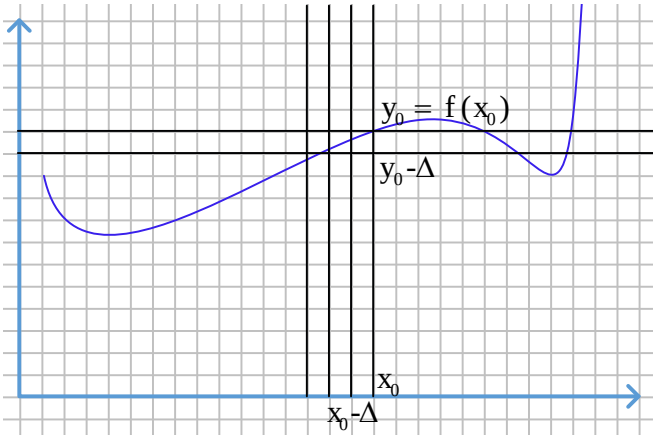


图 2.3 数字域上映射原像对应的区间数

对 $y_0 = f(x_0)$ 所在区间，其原像对应区间的个数为

$$c = \left\lceil \frac{|x - f^{-1}(f(x) - \Delta)|}{\Delta} \right\rceil,$$

其中 $\lceil x \rceil$ 表示大于等于实数 x 的最小整数。由于 *Logistic* 映射 *(2.10)* 具有对称性，即

$$f(x) = f(1 - x), \tag{2.12}$$

所以对应 $y = f(x)$ 的节点入度等于定义域左半部分入度的两倍。

映射 *(2.10)* 的反函数为

$$f^{-1}(y) = \left(1 - \sqrt{1 - 4y/\mu}\right)/2, \ x \in [0, 1/2).$$

当 $x \in [0, 1/2)$ 时，$f'(x) = \mu \cdot (1 - 2x) > 0$，$f(x)$ 关于 x 单调递增。因此对应 $y = f(x)$ 的节点入度为

$$\begin{aligned} k &= 2 \cdot \left\lceil \frac{f^{-1}(y) - f^{-1}(y - 1/2^n)}{2^{-n}} \right\rceil \\ &= 2 \cdot \left\lceil \frac{\sqrt{1 - 4(y - 1/2^n)/\mu} - \sqrt{1 - 4y/\mu}}{2^{1-n}} \right\rceil . \end{aligned}$$

根据上式，可得

$$y = \frac{\mu}{4} - \frac{1}{\mu \cdot (k + \epsilon)^2} - \frac{\mu \cdot (k + \epsilon)^2}{2^{2n+4}} + 2^{-n-1}, \tag{2.13}$$

其中 ϵ 为量化误差，且 $0 \le \epsilon < 0.5$。

由于误差 ϵ 在推导过程中产生的影响较小，因此在下面的讨论中忽略误差项。状态 y 的秩为

$$r = \left\lceil \frac{\mu/4 - y}{1/2^n} \right\rceil ,$$

状态映射网络节点数为

$$N = \left\lceil \frac{\mu/4}{1/2^n} \right\rceil .$$

根据累积分布的定义，则有

$$P(k) = 1 - \frac{4y}{\mu}.$$

将等式 *(2.13)* 代入上式，从而可得

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

根据上述推导可知，$P(k)$ 关于 n 单调增加，因此随着 n 的增大，*Logistic* 映射的状态映射网络中节点的累积入度分布 $P(k)$ 趋于其极限：

$$\lim_{n \to \infty} P(k) = \frac{4}{\mu^2 k^2}. \tag{2.14}$$

■

推论 2 *Logistic* 映射对应状态映射网络 F_n^* 的节点入度分布满足关系

$$p(k) \doteq \frac{16(k+1)}{\mu^2 k^2 (k+2)^2}.$$

证 由于 *Logistic* 映射具有对称性，所以除驻点 $f(1/2)$ 外，其状态映射网络的节点入度均为偶数。

根据累积入度分布的定义，入度分布 $p(k)$ 可表示为

$$p(k) = P(k) - P(k+2).$$

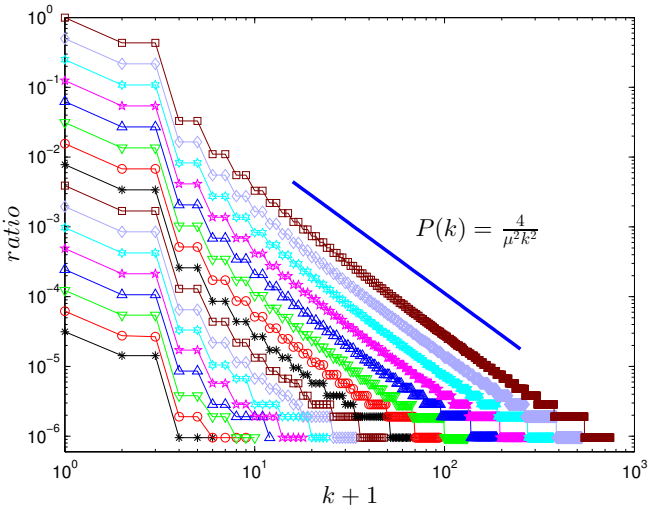


图 2.4 状态映射网络 $F_5^* \sim F_{20}^*$ 的节点累积入度分布，其中 $\mu = \frac{121}{2^5}$

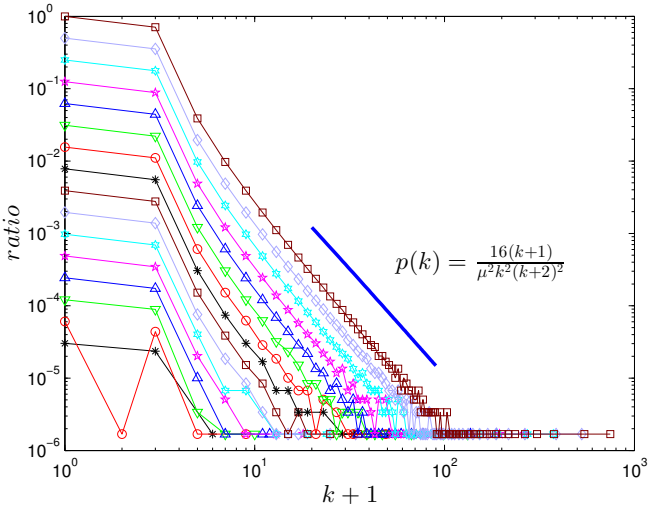


图 2.5 状态映射网络 $F_5^* \sim F_{20}^*$ 的节点入度分布，其中 $\mu = \frac{121}{2^5}$

从而可得

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

根据上述结论可知，随着 n 的增大，*Logistic* 映射的状态映射网络中节点的入度分布 $p(k)$ 逐渐趋于其极限：

$$\lim_{n\to\infty} p(k) = \frac{16(k+1)}{\mu^2 k^2 (k+2)^2}. \tag{2.15}$$

■

图 2.4、图 2.5分别为 Logistic 映射的状态映射网络中节点的累积入度分布和入度分布，这里 $N_{min} = 2^5$，$N_{max} = 2^{20}$。

2.3 浮点域上 Logistic 映射的性质分析

考虑到科学研究和工程技术中数的表示范围和表示精度，现代数字计算机采用两种二进制表示形式来表示实数，即定点格式和浮点格式。前者适用于表示具有固定精度的整数或实数，而后者适用于近似表示具有较高精度的实数，但浮点数的表示范围越大，浮点数的表示精度就降低。在浮点数标准被确定之前，不同的数字计算机采用不同的二进制表示形式来进行浮点运算。之后浮点数通常以 IEEE 754 标准存储在数字计算机中，其在内存中的表示形式如下图 2.6所示，其中 s 表示浮点数的符号，*exponent* 反映浮点数的表示范围，*mantissa* 反映浮点数的精度。

图 2.6 浮点数在计算机内存中的表示形式

浮点数 $\{b_i\}_{i=0}^{n-1}$ 的值为尾数与 2 的指数幂的乘积：

$$v=\begin{cases}0 & e=0, os=0;\\ (-1)^s\cdot\left(\sum\limits_{i=1}^{m} b_{l+i}\cdot 2^{-i}\right)\cdot 2^{2-2^{l-1}} & e=0, os\neq 0;\\ (-1)^s\cdot\infty & e=2^l-1, os=0;\\ \text{NaN} & e=2^l-1, os\neq 0;\\ (-1)^s\cdot\left(1+\sum\limits_{i=1}^{m} b_{l+i}\cdot 2^{-i}\right)\cdot 2^{e-os} & \text{其他,}\end{cases}$$

其中 $s=b_0$，$e=\sum\limits_{i=0}^{l-1} b_{1+i}\cdot 2^i$，$os=2^{l-1}-1$。

对于单精度浮点数 (binary32)，$(l,m)=(8,23)$，例如 C 语言中的 “float” 类型和 Matlab 中的 “single” 类型；对于双精度浮点数 (binary64)，$(l,m)=(11,52)$，例如 C 语言中的 “double” 类型和 Matlab 中的 “double” 类型；对于 IEEE 754-2008 标准中的半精度浮点数 (binary16)，$(l,m)=(5,10)$，其适用于对精度要求较低，对存储空间要求较高的场合。由于半精度浮点数 (binary16) 的表示范围相对较小，故其被广泛用于科学研究和数值仿真 [69]。

在浮点运算域上，由于量化误差的存在，等式 (2.12) 通常不成立，例如在 binary16 环境下，$x=0.0099945068359375$ 时，$f(x)\neq f(1-x)$，如表 2.1所示。

因为 $fl(x)$ 与 $fl(1-fl(1-fl(x)))$ 之间存在量化误差，所以

$$\mu\cdot x\cdot(1-x)\overset{?}{=}\mu\cdot(1-x)\cdot(1-(1-x))$$

不一定成立，$fl(x)$ 表示给定浮点运算域上最接近 x 的标准化浮点数。如果一个数

表 2.1 Binary16 环境下 $f(x) \neq f(1-x)$ 的部分情况

x	$1-x$	$1-(1-x)$	$f(x)$	$f(1-x)$
0.0099945068359375	0.98974609375	0.01025390625	0.037384033203125	0.038360595703125
0.04998779296875	0.94970703125	0.05029296875	0.179443359375	0.1805419921875
0.0899658203125	0.90966796875	0.09033203125	0.309326171875	0.310546875
0.0999755859375	0.89990234375	0.10009765625	0.340087890625	0.340576171875
0.199951171875	0.7998046875	0.2001953125	0.6044921875	0.60498046875
0.289794921875	0.7099609375	0.2900390625	0.77783203125	0.7783203125
0.389892578125	0.60986328125	0.39013671875	0.89892578125	0.8994140625
0.489990234375	0.509765625	0.490234375	0.9443359375	0.94482421875

落在区间 $[0.5, 1]$ 上，则 $1 - \mathit{fl}(x) = \mathit{fl}(1 - \mathit{fl}(x))$，因此

$$\mathit{fl}(1-\mathit{fl}(1-\mathit{fl}(x))) \equiv \begin{cases} 1-\mathit{fl}(1-\mathit{fl}(x)) & x \leq 0.5; \\ \mathit{fl}(x) & x > 0.5. \end{cases} \tag{2.16}$$

对任意 $x \in \mathbb{R} \cap [0,1]$，存在唯一整数 e 使得 $x = (\sum_{i=0}^{\infty} x_i \cdot 2^{-i}) \cdot 2^e$，其中 $x_0 = 1$。浮点数 x 在计算机内存中的表示形式为

$$\mathit{fl}(x) = \begin{cases} (\sum_{i=1}^{m} x_i \cdot 2^{-i}) \cdot 2^{2-2^{l-1}} & x \in (0, 2^{2-2^{l-1}}); \\ (1 + \sum_{i=1}^{m} x_i \cdot 2^{-i}) \cdot 2^e & x \in [2^e, 2^{e+1}), \end{cases} \tag{2.17}$$

其中 $e \in \{2-2^{l-1}, \cdots, -2\}$，$l$ 表示阶码位数，m 表示尾数位数。根据上述表示，进而可得

$$1-\mathit{fl}(x) = \begin{cases} \sum_{i=1}^{2^{l-1}-2} 2^{-i} + (\sum_{i=1}^{m} \bar{x}_i \cdot 2^{-i} + 2^{-m}) \cdot 2^{2-2^{l-1}} & x \in (0, 2^{2-2^{l-1}}); \\ \sum_{i=1}^{-(e+1)} 2^{-i} + (\sum_{i=1}^{m} \bar{x}_i \cdot 2^{-i} + 2^{-m}) \cdot 2^e & x \in [2^e, 2^{e+1}), \end{cases} \tag{2.18}$$

其中 $\bar{x}_i = 1 - x_i$。由于等式 (2.18) 第一种情况中 $(1 - \mathit{fl}(x))$ 的阶码为 -1，故

$$\mathit{fl}(1-\mathit{fl}(x)) = \left(1 + \sum_{i=1}^{m} \hat{x}_i \cdot 2^{-i}\right) \cdot 2^{-1}, \tag{2.19}$$

其中 $\hat{x}_i \in \{0, 1\}$，$2^{l-1} - 2 \geq m + 1$。根据浮点数在计算机内存中的表示形式，等式 (2.18) 可进一步表示为

$$\mathit{fl}(1-\mathit{fl}(x)) = \begin{cases} (\sum_{i=1}^{m+1} 2^{-i}) & x \in (0, 2^{2-2^{l-1}}); \\ (\sum_{i=1}^{m+1} 2^{-i}) & x \in [2^{e_1}, 2^{e_1+1}); \\ (\sum_{i=1}^{-e_2-1} 2^{-i}) + (\sum_{i=1}^{m+1+e_2} \bar{x}_i \cdot 2^{-i}) \cdot 2^{e_2} & x \in [2^{e_2}, 2^{e_2+1}), \end{cases} \tag{2.20}$$

其中 $e_1 \in \{2-2^{l-1}, \cdots, -m-2\}$，$e_2 \in \{-m-1, \cdots, -2\}$。

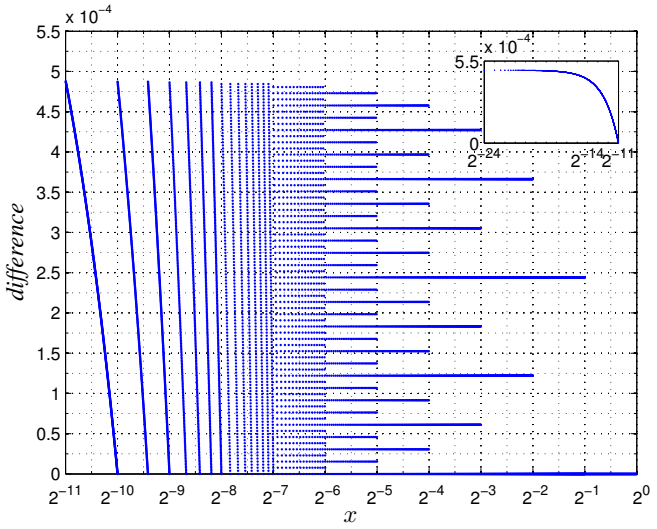


图 2.7 Binary16 中 $1-(1-x)$ 与 x 的差值关于 x 的变化规律

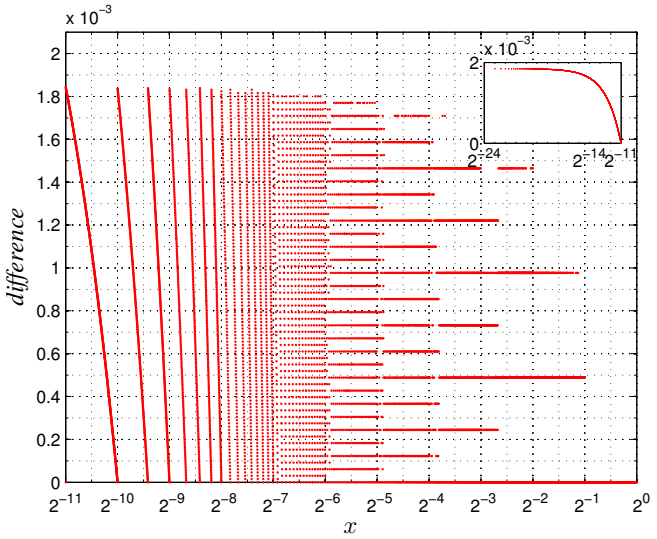


图 2.8 Binary16 中 $f(1-x)$ 与 $f(x)$ 的差值关于 x 的变化规律

根据等式 (2.16) 的第一种情况，等式 (2.18) 与等式 (2.20) 相减，则有

$$
\begin{aligned}
fl(1 \quad - \quad & fl(1-fl(x))) - fl(x) = (1-fl(x)) - fl(1-fl(x)) \\
= \quad & \begin{cases}
(\sum_{i=m+2}^{2^{l-1}-2} 2^{-i}) + (\sum_{i=1}^{m} \bar{x}_i \cdot 2^{-i} + 2^{-m}) \cdot 2^{2-2^{l-1}} & x \in (0, 2^{2-2^{l-1}}); \\
(\sum_{i=m+2}^{-(e_1+1)} 2^{-i}) + (\sum_{i=1}^{m} \bar{x}_i \cdot 2^{-i} + 2^{-m}) \cdot 2^{e_1} & x \in [2^{e_1}, 2^{e_1+1}); \\
(\sum_{i=m+2+e_2}^{m} \bar{x}_i \cdot 2^{-i} + 2^{-m}) \cdot 2^{e_2} & x \in [2^{e_2}, 2^{e_2+1}).
\end{cases}
\end{aligned} \tag{2.21}
$$

根据等式 (2.21)，在数字计算机中，$1-(1-x)$ 与 x 的差值关于 x 分段单调递减，如图 2.7所示。图 2.7右上角的插图对应等式 (2.21) 的前两种情况，可以观察到，区间 $[2^{-10+2-2^4}, 2^{2-2^4}] = [2^{-24}, 2^{-14}]$ 和 $\{[2^{e_1}, 2^{e_1+1}]\}_{e_1=2-2^4}^{-10-2} = \{[2^{e_1}, 2^{e_1+1}]\}_{e_1=-14}^{-12}$ 的对应曲线可以平滑连接。类似的，$f(1-x)$ 与 $f(x)$ 的差值关于 x 的变化规律如图 2.8所示。

2.4 混沌伪随机数发生器的随机性检测

伪随机数序列由数学表达式生成，但伪随机数并不是真正意义上随机，因为序列本身随着时间的推移必然会进入一个循环。对于伪随机数来说，衡量其序列随机性的指标主要有均匀性、相关性和周期性。均匀性是指随机序列服从均匀分布；相关性是指伪随机数发生器生成的随机序列中各个随机数是否相关，随机数之间的相关性应尽可能弱；周期性是指经过多久，随机序列进入循环，进入循环前的暂态分枝应尽可能长。由于混沌系统的不确定性、不可重复、不可预测等特性，混沌系统被广泛应用于设计伪随机数发生器，因此各种基于混沌的伪随机数发生器应运而生[28–30,36,37,41,43,45,70]。当我们在数字化应用中使用伪随机数发生器时，一个很重要的问题是如何检测混沌伪随机数发生器的随机性能。

SMN 可对基于混沌的伪随机数发生器进行分类，并对其随机性进行检测[71] [72]。根据 SMN 结构，基于混沌的伪随机数发生器可被归为以下六类：

- 选择状态和控制参数

  根据图 2.1可知，在数字混沌系统中少数节点很难通过随机性检测被发现，例如 SMN 中节点 ‘‘0” 和 ‘‘2^n”。2006 年，Addabbo 等人提出，离散 Tent 映射可以实现随机序列周期长度、比特序列统计属性和定点运算域上硬件复杂度之间的折衷优化[41]。给定运算环境，控制参数是影响 Tent 映射的状态映射网络结构的唯一因素，因此可以通过控制参数的选取来影响混沌系统状态映射网络的结构[28]。

- 增加运算精度

  1991 年，Lin 等人提出，增加运算精度可以增大混沌系统状态映射网络的平均路径长度，进而增强其结构复杂性[26]，但根据性质 4，增加运算精度并不能改变混沌系统状态映射网络的整体结构。2012 年，Persohn 等人也指出，增加运算精度，混沌系统状态映射网络的平均路径长度不一定增大[20]。因此可以在数的表示范围和表示精度允许范围内对数字混沌系统状态映射网络进行穷举分析。

- 扰动状态

  从本质上来说，扰动状态是指对混沌系统状态映射网络的边重定向[27–30]。1998 年，Tao 等人提出了一种基于位运算的状态扰动方法[27]，以图 2.1 b) 为例，用上述方法对 Logistic 映射的状态映射网络进行状态扰动，对 Logistic 映射输出值的最低有效位进行按位异或，扰动序列为 $(100)_2$。根据图 2.9 a) 可以看出，扰动后状态映射网络的循环长度较短。2006 年，Addabbo 等人提出基于反馈控制的混沌系统状态映射网络节点的自适性扰动[35,36]。

- 扰动控制参数

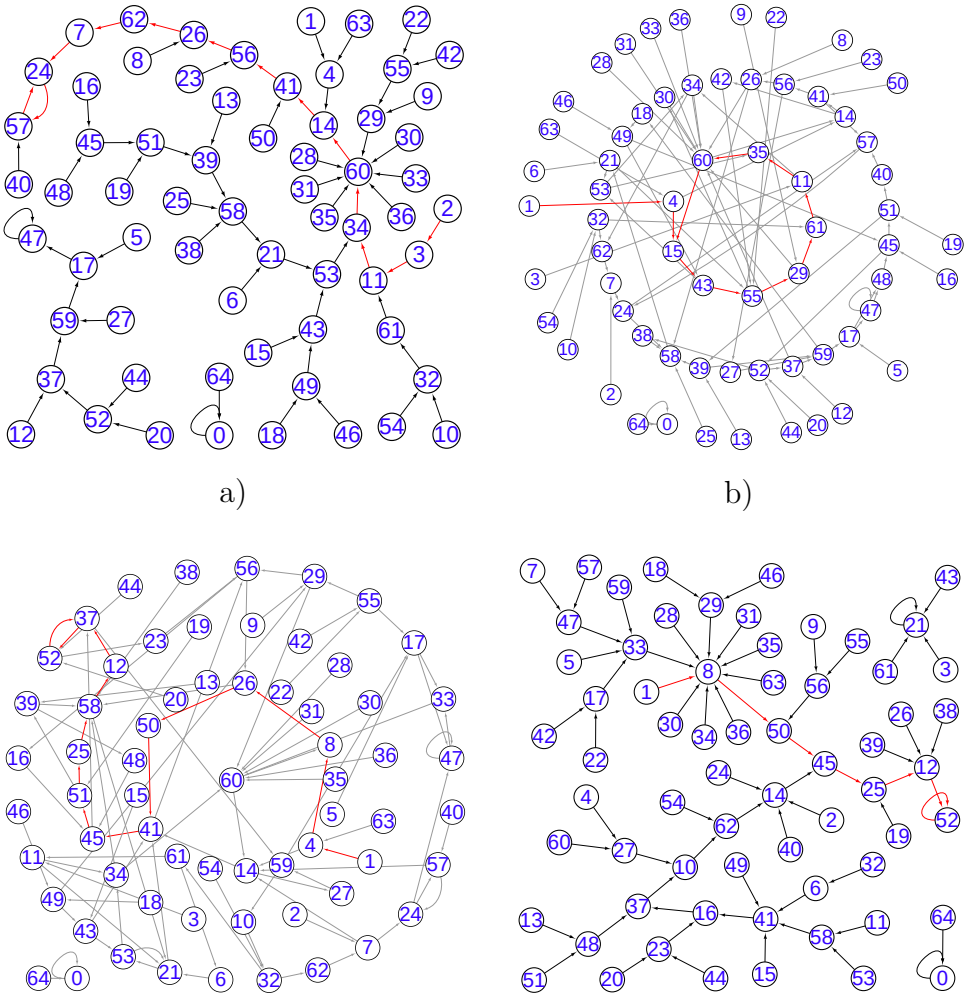


图 2.9 对图 2.1 b) 对应 SMN 进行增强：a) 扰动状态；b) 扰动控制参数；c) Logistic 映射和 Tent 映射之间的转换；d) Logistic 映射和 Tent 映射之间的级联

扰动控制参数是指对控制参数不同的混沌系统状态映射网络进行级联 [31, Sec. 4]。以 Logistic 映射的状态映射网络图 2.1 b)、图 3.10 b) 为例，将上述两个状态映射网络进行级联，扰动后状态映射网络如图 2.9 b) 所示。

- 混沌系统之间的转换

  混沌系统之间的转换是指在每次迭代中，交替改变混沌系统，前一个混沌系统的输出值为后一个混沌系统的输入值 [33,34]。以本文分析讨论的 Logistic 映射和 Tent 映射为例，在其状态映射网络上交替跳转，转换后状态映射网络如图 2.9 c) 所示，状态映射网络节点的最大入度与混沌系统的数量有关。

- 混沌系统之间的级联

  混沌系统之间的级联是指对不同混沌系统的状态映射网络进行级联 [32]。1994 年，Heidari 等人提出了一种混沌系统级联方法，一个混沌系统的输出值为另

一个混沌系统状态映射网络路径的起点[28]。以 Logistic 映射和 Tent 映射为例，对图 2.1 b)、图 3.1 b) 对应的状态映射网络进行级联，级联后状态映射网络如图 2.9 d) 所示。根据图 2.9 d) 可以看出，除孤立点 “0” 和 “2^n”，整个状态映射网络单向连通。

2.5 本章小结

本章讨论了隐含在数字化 Logistic 映射中的一些动力学性质，首先利用整数量化函数准确推导出了 Logistic 映射的状态映射网络 F_n^* 与实现精度 n 之间的关系，以累积入度为切入点理论上证明了定点运算域上 Logistic 映射的状态映射网络的无标度属性；其次，通过严格的数学推导，浮点运算域上系统量化误差对 Logistic 映射的影响被厘清，改变 Logistic 映射中因式 x 与因式 $(1-x)$ 的运算顺序可能使 Logistic 映射运算结果不同；最后，根据混沌映射的状态映射网络对基于混沌的伪随机数发生器发生器进行了分类，研究发现，该分类方法可以粗检测混沌伪随机数发生器的随机性能。

第 3 章　一维 Tent 映射的状态网络分析

3.1　定点域上 Tent 映射的性质分析

3.1.1　数字化 Tent 映射的定义

Tent 映射在数学中是指一种分段的线性映射，因其函数图像看似帐篷而得名，其数学表达式为

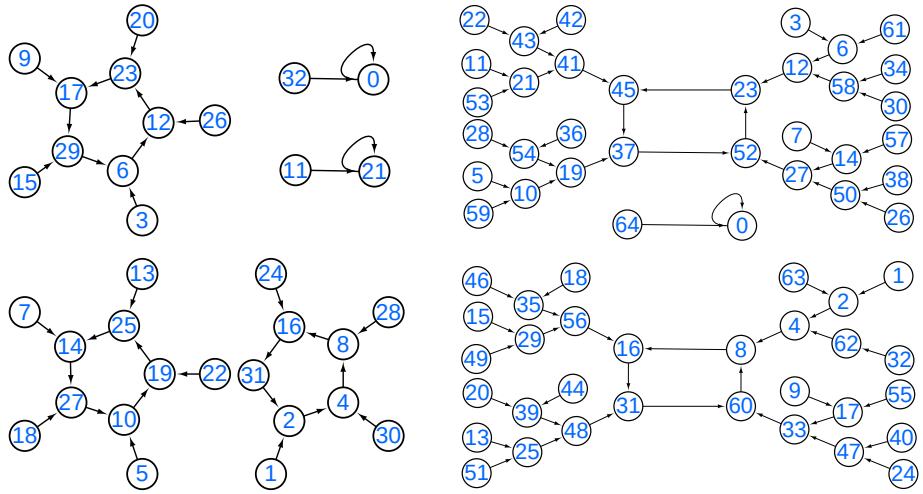
$$f(x) = \mu \cdot (1 - 2\,|x - 1/2|)\,, \tag{3.1}$$

其中 $x \in [0, 1]$，$\mu \in (0, 1]$。Tent 映射和 Logistic 映射实质上是拓扑共轭。

在精度为 n 的定点运算域上，Tent 映射 $f(x) = \mu \cdot (1 - 2\,|x - 1/2|)$ 变为

$$f_n(i) = ((N_\mu / 2^{n_\mu}) \cdot (1 - 2\,|(i/2^n) - 1/2|))\,. \tag{3.2}$$

图 3.1为相同控制参数，不同运算精度下 Tent 映射的状态映射网络 $F_n^\star$。



a)　　b)

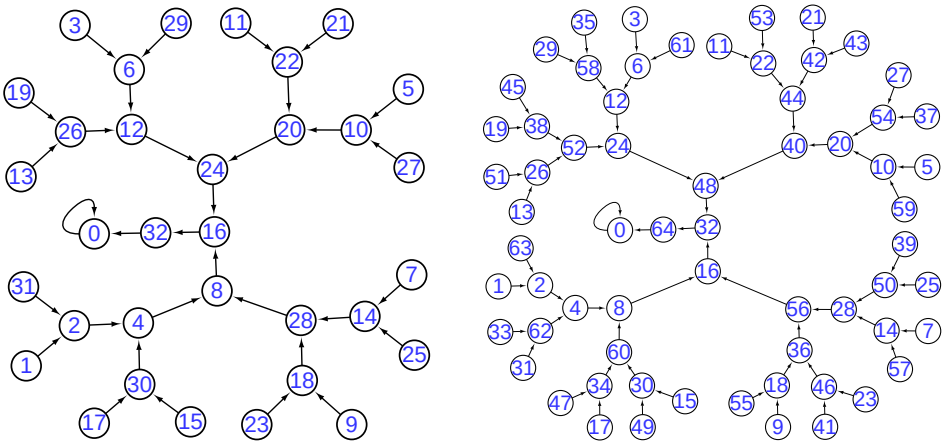
图 3.1 控制参数 $\mu = 31/2^5$ 时，Tent 映射的状态映射网络：a) 5 比特精度；b) 6 比特精度

3.1.2　Tent 映射的状态映射网络与实现精度之间的关系

推论 3 $F_{n+1}^\star$ 中节点 $(2i + 1)$ 和 $F_n^\star$ 中节点 i 满足关系

$$\left|F_{n+1}^\star(2i + 1) - 2 \cdot F_n^\star(i)\right| \le \begin{cases} 4 & r_n \in [0.25, 0.75); \\ 3 & \text{其他}, \end{cases}$$

其中 $i \in \{0, \cdots, 2^n - 1\}$。



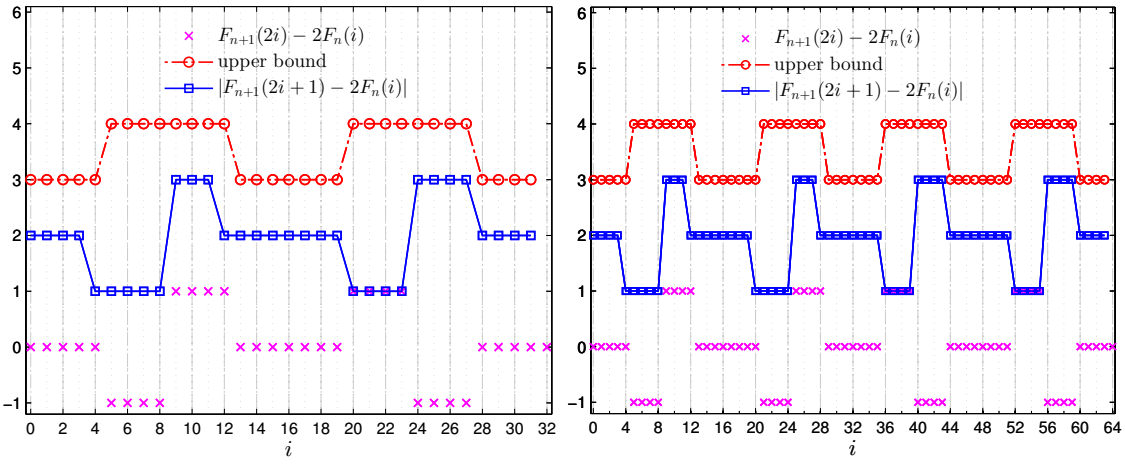
a) b)

图 3.2 控制参数 $\mu = 1$ 时，Tent 映射的状态映射网络：a) 5 比特精度；b) 6 比特精度

证 因为 $(N_\mu/2^{n_\mu-1}) \in [0,2]$，将等式 *(3.2)* 代入不等式 *(2.3)*，可得

$$\begin{aligned}\left|F^\star_{n+1}(2i+1) - 2\cdot F^\star_n(i)\right| &\leq \left|\mathrm{R}\left(N_\mu/2^{n_\mu-1}\right)\right| + \begin{cases} 2 & r_n \in [0.25, 0.75); \\ 1 & \text{其他}, \end{cases} \\ &\leq \begin{cases} 4 & r_n \in [0.25, 0.75); \\ 3 & \text{其他}. \end{cases}\end{aligned}$$

■



a) b)

图 3.3 $F^\star_n$ 与 $F^\star_{n+1}$ 中对应节点的差值分布：a) $n = 5$；b) $n = 6$

根据推论 3可知，$|F^\star_{n+1}(2i+1) - 2\cdot F^\star_n(i)|$ 的上界仅仅取决于 N_μ。图 3.3 a) 为图 3.1 a) 中每个节点对应的差值 $|F^\star_{n+1}(2i+1) - 2\cdot F^\star_n(i)|$ 和 $F^\star_{n+1}(2i) - 2F^\star_n(i)$，类

似地，为进一步分析比较 F_n^* 和 F_{n+1}^* 的关系，图 3.1 b) 中每个节点对应的差值如图 3.3 b) 所示。

3.1.3 Tent 映射 SMN 入度分布的理论推导

性质 5 *Tent* 映射对应状态映射网络的节点入度仅有三种可能取值：

$$k=\begin{cases}1 & \text{最大值对应节点;}\\ 2 & \text{其他具有原像的节点;}\\ 0 & \text{其他节点.}\end{cases}$$

证 当 $x=1/2$ 时，$f(x)=\mu$ 取最大值。$x=1/2$ 所在区间对应节点唯一指向 $y=\mu$ 所在区间对应节点，因此 $y=\mu$ 所在区间对应节点的入度 $k=1$。

由于 *Tent* 映射具有对称性，这里只考虑定义域的左半部分。*Tent* 映射 $y=f(x)$ 的反函数为

$$f^{-1}(y)=y/\left(2\mu\right),\ x\in[0,1/2].$$

当 $x\in[0,1/2]$ 时，$f'(x)=2\mu>0$，$f(x)$ 关于 x 单调递增。根据定理 *1*的证明可知，$y\neq\mu$ 所在区间对应节点的入度为

$$\begin{aligned}k &= 2\cdot\left\lceil\frac{f^{-1}(y)-f^{-1}(y-(1/2^n))}{2^{-n}}\right\rceil\\ &= 2\cdot\left\lceil\frac{y/(2\mu)-(y-1/2^n)/(2\mu)}{2^{-n}}\right\rceil\\ &= 2\cdot\lceil 1/(2\mu)\rceil\\ &= 2.\end{aligned}$$

由此上述关于 *Tent* 映射的状态映射网络入度分布的性质得以证明，即 *Tent* 映射对应状态映射网络的节点入度仅有三种可能取值：*1*，*2*，*3*。 ■

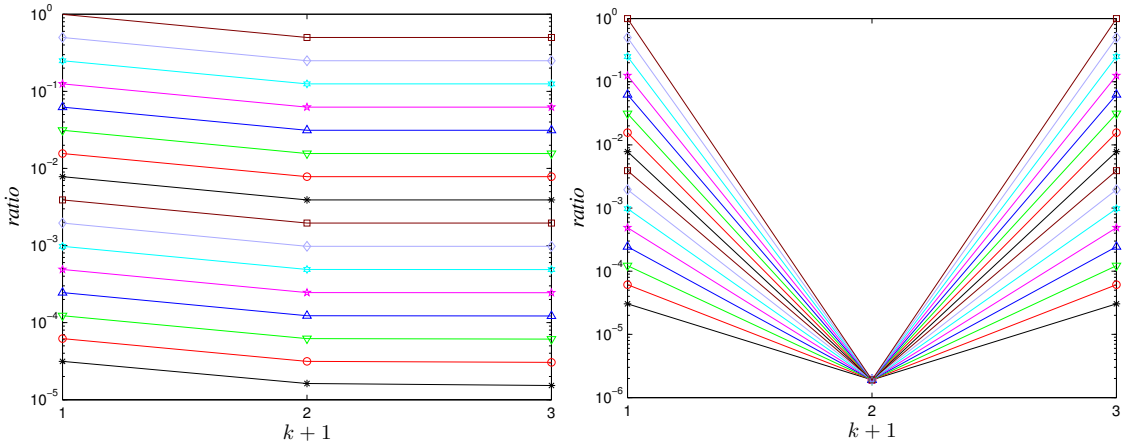
根据性质 5可知，Tent 映射对应状态映射网络的节点入度不会随着运算精度的增加而累积（详见图 3.4），这与 Logistic 映射不同。

基于上述讨论，可以得出结论：$f''(x)>0$ 是混沌映射对应状态映射网络的节点入度满足幂律分布的充分而非必要条件。

3.2 浮点域上 Tent 映射的性质分析

假设 Tent 映射的迭代初值 $x(0)=(0.b_1b_2\cdots b_j\cdots b_{L-1}b_L)_2\neq 0$，其中 $b_L=1$（最低有效位），则 $1-x(0)=(0.b_1'b_2'b_3'\cdots b_j'\cdots b_{L-1}'b_L)_2$。根据上述假设，可得

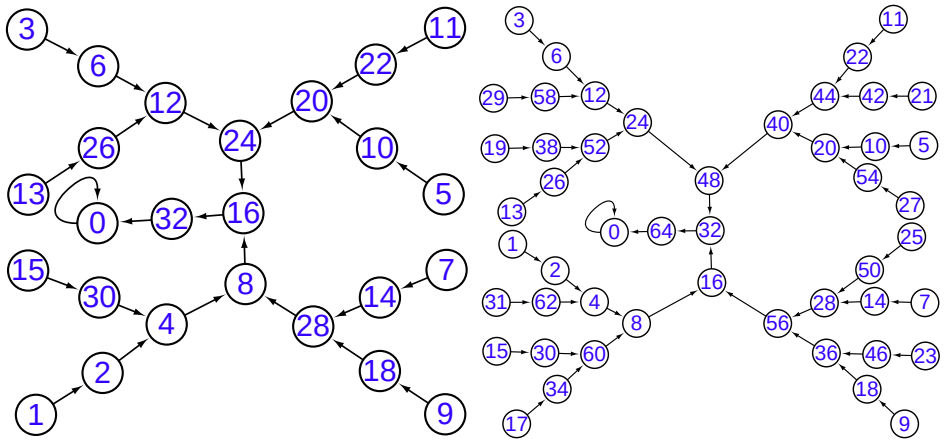
$$x(1)=\begin{cases}2x(0)=x(0)\ll 1=(0.b_2\cdots b_j\cdots b_{L-1}b_L)_2 & 0\le x(0)<0.5;\\ 2(1-x(0))=(b_1'.b_2'b_3'\cdots b_j'\cdots b_{L-1}'b_L)_2 & 0.5\le x(0)\le 1,\end{cases}$$



a) b)

图 3.4 控制参数 $\mu = 31/2^5$ 时，状态映射网络 $F_5^\star \sim F_{20}^\star$ 的节点度分布：a) 累积入度分布；b) 入度分布

其中 $\ll$ 表示左移运算。注意到，当 $0 \leq x(0) < 0.5$ 时，$b_1 = 0$。Tent 映射迭代 $L-1$ 次，有 $x(L-1) \equiv (0.b_L)_2 = (0.1)_2$，进而可知 $x(L) \equiv 1$，$x(L+1) \equiv 0$，即 x 趋于 0 所需迭代次数为 $N_r = L+1$。特别地，当 $x(0) = 0$ 时，$N_r = 0$。以图 3.5 a) 中节点 "13" 为例，Tent 映射的迭代过程如下：$(0.01101)_2 \to (0.1101)_2 \to (0.011)_2 \to (0.11)_2 \to (0.1)_2 \to (1)_2 \to (0)_2$。



a) b)

图 3.5 控制参数 $\mu = 1$ 时，浮点运算域上 Tent 映射的状态映射网络：a) $(l, m) = (3, 3)$；b) $(l, m) = (3, 4)$

通常在数字混沌系统的迭代过程中不可避免地要引入量化误差，这种系统量化误差会使数字混沌系统的混沌轨道变得异常复杂且难以预测，进而偏离连续域上混沌系统的实际混沌轨道。根据上述分析过程可知，$\mu = 1$ 时，Tent 映射 (3.1) 的迭代过程可利用左移运算 $\ll$ 在计算机上准确执行，不会引入任何量化误差。有效数位 L 的值可根据 $x(0) \neq 0$ 的表示形式来确定：

- 当 $x(0)$ 为规格化数：$x(0) = (1.b_{m-1}\cdots b_0)\times 2^{-e} = (0.\overbrace{0\cdots 0}^{e-1}1b_{m-1}\cdots b_0)_2$。假设 $x(0)$ 的最低有效位为 $b_i = 1$，则 $x(0) = (0.\overbrace{0\cdots 0}^{e-1}1\overbrace{b_{m-1}\cdots b_i}^{m-i}\overbrace{0\cdots 0}^{i})_2$，$L = (e-1)+1+(m-i) = e+(m-i)$。当 $e\in[1,2^{l-1}-2]$，$i\in[0,m-1]$ 时，$L\in[2,2^{l-1}-2+m]$；

- 当 $x(0)$ 为非规格化数：$x(0) = (0.b_{m-1}\cdots b_0)\times 2^{2-2^{l-1}} = (0.\overbrace{0\cdots 0}^{2^{l-1}-2}b_{m-1}\cdots b_0)_2$。假设 $x(0)$ 的最低有效位为 $b_i = 1$，则 $x(0) = (0.\overbrace{0\cdots 0}^{2^{l-1}-2}\overbrace{b_{m-1}\cdots b_i}^{m-i}\overbrace{0\cdots 0}^{i})_2$，$L = 2^{l-1}-2+(m-i) = 2^{l-1}-2+m-i$。当 $i\in[0,m-1]$ 时，$L\in[2^{l-1}-1,2^{l-1}-2+m]$。

根据上述讨论可知，无论哪种 $x(0)$ 的表示形式，总有 $L\le 2^{l-1}-2+m$。

首先，考虑 $i\in\{0,\cdots,m-1\}$ 的数学期望。不失一般性，假设尾数 $(b_{m-1}\cdots b_0)_2$ 在集合 $\{0,\cdots,2^m-1\}$ 上均匀分布 [73]，则有

$$Prob[(b_i = 1, b_{i-1} = \cdots = b_0 = 0)] = \frac{2^{m-1-i}}{2^m} = \frac{1}{2^{i+1}},$$
$$Prob[(b_{m-1} = \cdots = b_0 = 0)] = \frac{1}{2^m},$$

从而可知 i 的数学期望为

$$E(i)\approx\sum_{i=0}^{m-1} i\cdot\frac{1}{2^{i+1}} + m\cdot\frac{1}{2^m} = \frac{1}{2}\cdot\sum_{i=1}^{m-1}\frac{i}{2^i} + \frac{m}{2^m} = 1-\frac{1}{2^m}.$$

下面分析 $e\in\{1,\cdots,2^{l-1}-2\}$ 的数学期望。根据 $x(0)$ 在区间 [0,1] 上的均匀分布 [73]，可知

$$Prob[2^{-e}\le x(0) < 2^{-(e-1)}] = 2^{-e}.$$

因此 e 的数学期望为

$$E(e)\approx\sum_{e=1}^{2^{l-1}-2}\frac{e}{2^e} = 2-\frac{2^{l-1}}{2^{2^{l-1}-2}}\approx 2.$$

根据上述推导，进一步可得

$$\begin{aligned}
E(L) &= Prob[\text{normalized numbers}]\cdot(E(e)+(m-E(i)))+ \\
&\quad Prob[\text{denormalized numbers}]\cdot\left(2^{l-1}-2+m-E(i)\right) \\
&= \frac{2^{l-1}-2}{2^{l-1}-1}\cdot(E(e)+(m-E(i)))+ \\
&\quad \frac{1}{2^{l-1}-1}\cdot\left(2^{l-1}-2+m-E(i)\right) \\
&\approx \frac{2^{l-1}-2}{2^{l-1}-1}\cdot(2+(m-1))+\frac{1}{2^{l-1}-1}\cdot(2^{l-1}-2+m-1) \\
&= \frac{(2^{l-1}-2)(m+2)+m-1}{2^{l-1}-1}.
\end{aligned} \tag{3.3}$$

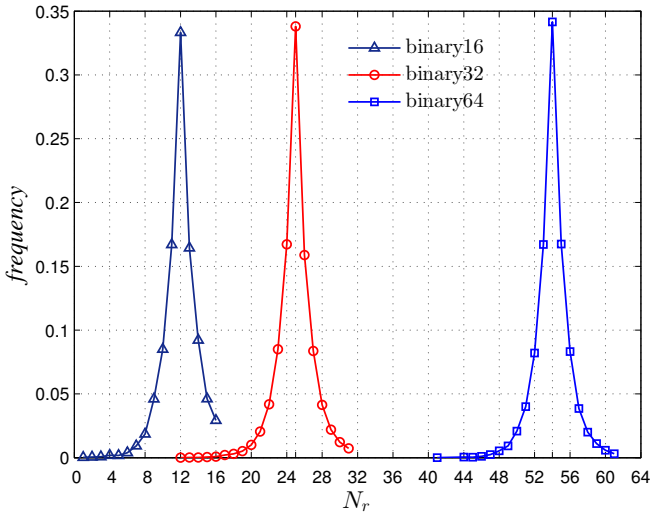


图 3.6 N_r 的不同值的出现频率

因为 $N_r = L + 1$，所以 $E(N_r) = E(L) + 1$。在计算机上随机进行 10000 次实验，可以看到，N_r 的分布由运算环境决定。图 3.6中三条曲线分别表示 binary16，binary32，binary64 环境下 N_r 的分布规律，其均值分别为 11.95，24.97，54.01，这与 (3.3) 式计算产生的理论值一致。

3.3 不同域上混沌映射状态网络之间的关系

根据浮点数在计算机中的表示形式可知，数与数之间的最小间隔为 $2^{(1-(2^{l-1}-1))} \cdot 2^{-m} = 2^{2-2^{l-1}-m}$。在精度为 n 的定点运算域上，数与数之间的间隔为 2^{-n}。如果 $2^{2-2^{l-1}-m} = 2^{-n}$，即 $n = m + 2^{l-1} - 2$，那么基于不同运算环境实现的混沌映射，其对应的状态映射网络有强相关性。

定理 2 给定二进制浮点格式参数 l，m，则 $F_{l,m}$ 中节点 i 和 F_n 中节点 i 满足关系

$$F_n(i) - F_{l,m}(i) \leq \begin{cases} 1 & F_n(i) \in [0, 2^m); \\ 2^{n-m-1-j} & F_n(i) \in [2^{n-j-1}, 2^{n-j}), \end{cases} \tag{3.4}$$

其中 $j \in \{2^{l-1} - 3, 2^{l-1} - 4, \cdots, 1, 0\}$，且

$$n = m + 2^{l-1} - 2. \tag{3.5}$$

证 因为 $|x - \mathrm{R}(y)| = |\mathrm{R}(x - y)|,\ x \in \mathbb{Z}, y \in \mathbb{R}$，所以

$$\begin{aligned} |F_{l,m}(i) - F_n(i)| &= |f_{l,m}(i) \cdot 2^n - \mathrm{R}\left(f_n(i) \cdot 2^n\right)| \\ &= |\mathrm{R}\left((f_{l,m}(i) - f_n(i)) \cdot 2^n\right)|, \end{aligned} \tag{3.6}$$

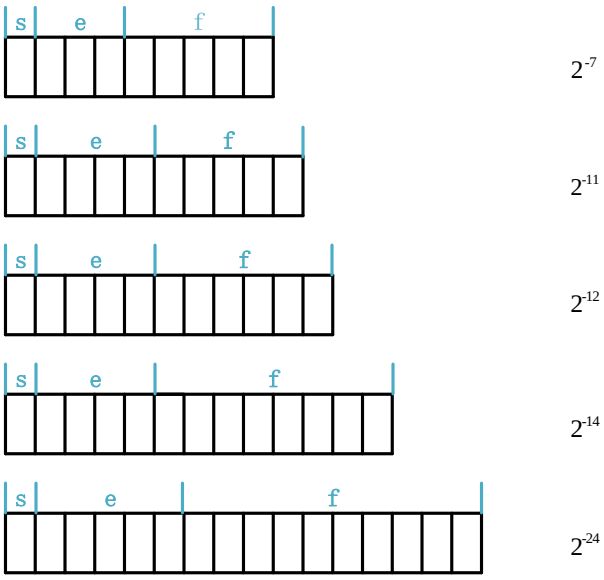


图 3.7 浮点数在计算机中的表示形式及数与数之间的最小间隔

其中 $F_{l,m}(i) = f_{l,m}(i) \cdot 2^n$。

对 *SMN* F_n 中节点 "i"，其对应值 $i/2^n$ 可在计算机内存中准确表示。不失一般性，假设在定点和浮点运算域上 $f(i/2^n)$ 的中间运算或处理过程相同，$f_{l,m}(i)$ 与 $f_n(i)$ 的差值仅由最终量化误差引起。当 $F_n(i) \in [2^{n-1-j}, 2^{n-j})$ 时，有

$$f_{l,m}(i) = 2^{-j-1} \cdot \left(1 + \sum_{i=1}^{m} a_i \cdot 2^{-i}\right), \tag{3.7}$$

$$f_n(i) = 2^{-j-1} \cdot \left(1 + \sum_{i=1}^{n} c_i \cdot 2^{-i}\right), \tag{3.8}$$

其中 $j \in \{0, \cdots, 2^{l-1} - 3\}$，对任意 $i \in \{1, 2, \cdots, m\}$，$a_i = c_i$。根据上述条件，进一步可推得

$$f_n(i) - f_{l,m}(i) = 2^{-j-1} \cdot \left(\sum_{i=m+1}^{n} c_i \cdot 2^{-i}\right) < 2^{-m-j-1}. \tag{3.9}$$

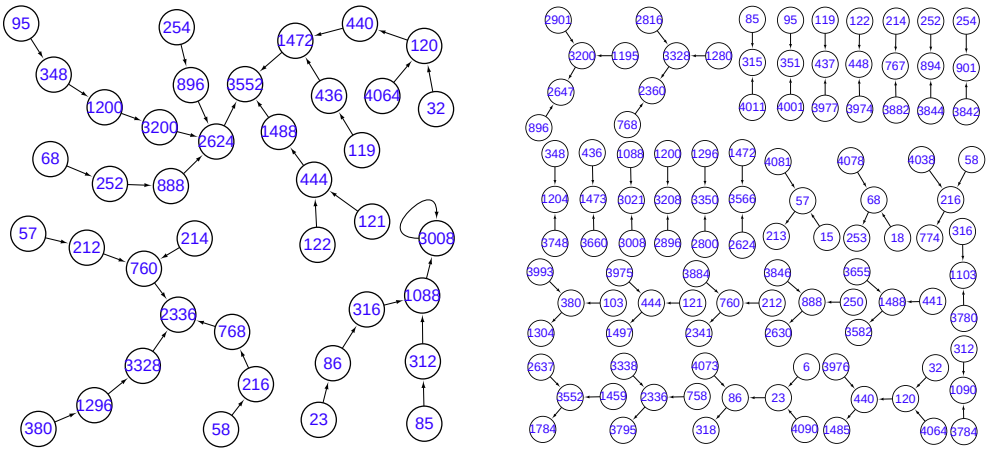
将 *(3.9)* 式代入 *(3.6)* 式，则有

$$\begin{aligned} F_n(i) - F_{l,m}(i) &= \mathrm{R}\left((f_n(i) - f_{l,m}(i)) \cdot 2^{m+1+j} \cdot 2^{n-m-1-j}\right) \\ &\leq \mathrm{R}\left(2^{n-m-1-j}\right) = 2^{n-m-1-j}. \end{aligned} \tag{3.10}$$

当 $F_n(i) \in [0, 2^m)$ 时，$f_{l,m}(i)$ 为非规格化数，$f_{l,m}(i)$ 和 $f_n(i)$ 可分别表示为

$$f_{l,m}(i) = 2^{2-2^{l-1}} \cdot \left(\sum_{i=1}^{m} a_i \cdot 2^{-i}\right), \tag{3.11}$$

$$f_n(i) = 2^{2-2^{l-1}} \cdot \left(\sum_{i=1}^{n} c_i \cdot 2^{-i}\right). \tag{3.12}$$



a) b)

图 3.8 控制参数 $\mu = 121/2^5$ 时，浮点运算域上 Logistic 映射的状态映射网络的连通分量及对应定点运算域上其状态映射网络节点间的相对关系：a) $(l, m) = (4, 6)$；b) $n = 12$

表 3.1 定点和浮点运算域上 Logistic 映射的状态映射网络部分对应节点的差值

i	$F_n(i)$	$F_{l,m}(i)$	$\lvert F_n(i) - F_{l,m}(i)\rvert$	$2^{n-m-1-j}$	i	$F_n(i)$	$F_{l,m}(i)$	$\lvert F_n(i) - F_{l,m}(i)\rvert$	$2^{n-m-1-j}$
6	23	22	1	1	156	567	560	7	8
18	68	67	1	1	238	848	840	8	8
33	124	123	1	1	284	999	992	7	8
40	150	148	2	2	316	1103	1088	15	16
53	198	196	2	2	576	1872	1856	16	16
67	249	248	2	2	648	2063	2048	15	16
82	304	300	4	4	768	2360	2336	24	32
112	412	408	4	4	1280	3328	3296	32	32
130	476	472	4	4	2080	3871	3840	31	32

类似地，可推得

$$f_n(i) - f_{l,m}(i) = 2^{2-2^{l-1}} \cdot \left(\sum_{i=m+1}^{n} c_i \cdot 2^{-i} \right) < 2^{-m+2-2^{l-1}} = 2^{-n}. \tag{3.13}$$

根据 *(3.13)* 式，进一步有

$$|F_{l,m}(i) - F_n(i)| = \mathrm{R}\left(|(f_{l,m}(i) - f_n(i)) \cdot 2^n|\right) \leq \mathrm{R}(1) = 1. \tag{3.14}$$

■

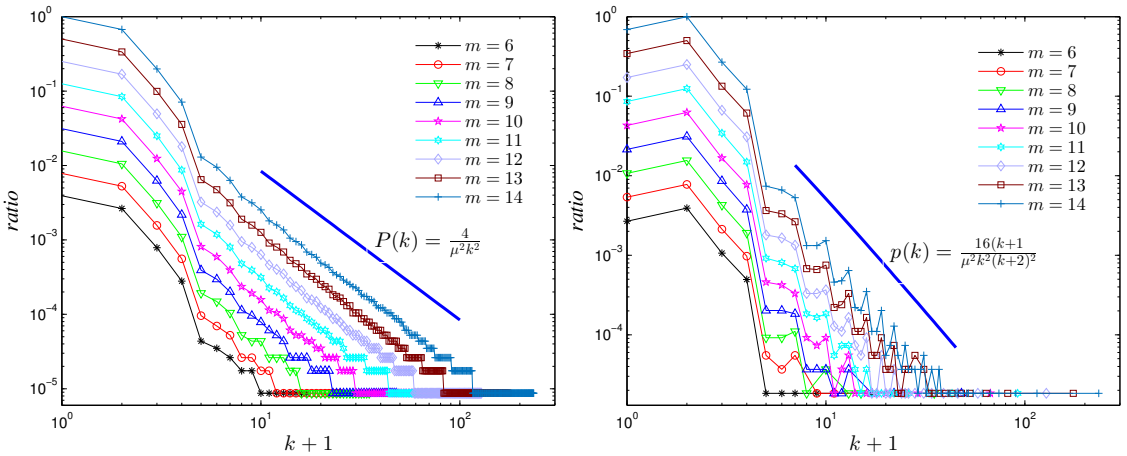
图 3.8 a) 为定点运算域上 Logistic 映射的状态映射网络 F_{12} 的其中三个连通分量，图 3.8 b) 为浮点运算域上 Logistic 映射的状态映射网络 $F_{4,6}$ 节点间的相对关系，图 3.8 b) 为图 3.8 a) 中对应节点及其邻接点。表 3.1给出 Logistic 映射 SMN F_{12} 与 SMN $F_{4,6}$ 部分对应节点的差值及其理论值，Logistic 映射的控制

表 3.2 定点和浮点运算域上 Tent 映射的状态映射网络部分对应节点的差值

i	$F_n(i)$	$f_n(i)-f_{l,m}(i)$	$2^{-(m+1+j)}$	i	$F_n(i)$	$f_n(i)-f_{l,m}(i)$	$2^{-(m+1+j)}$
17	32	0.013671875	0.03125	34	56	0.00390625	0.03125
19	36	0.025390625	0.03125	38	49	0.01171875	0.03125
21	39	0.021484375	0.03125	42	41	0.01953125	0.03125
23	43	0.017578125	0.03125	46	34	0.02734375	0.03125
25	47	0.013671875	0.03125	50	26	0.00390625	0.015625
27	51	0.009765625	0.03125	54	19	0.01171875	0.015625
29	54	0.005859375	0.03125	58	11	0.00390625	0.015625
31	58	0.001953125	0.03125	62	4	0.01171875	0.015625

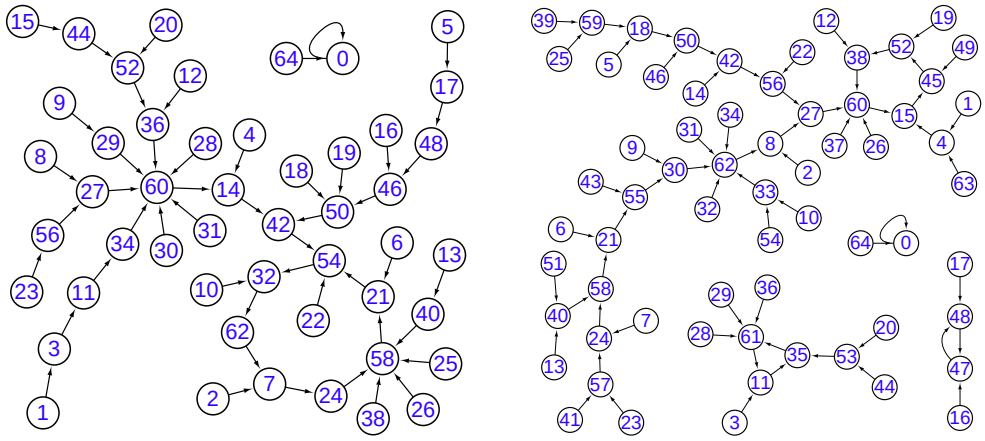
参数 $\mu = 121/2^5$，浮点运算模式下浮点数格式参数 $(l,m) = (4,6)$，定点运算精度 $n = 12$。表 3.2列出 Tent 映射 SMN F_6 与 SMN $F_{3,4}$ 部分对应节点的差值及其理论值，Tent 映射的控制参数 $\mu = 15/2^4$，浮点运算模式下浮点数格式参数 $(l,m) = (3,4)$，定点运算精度 $n = 6$。这里 $f_{l,m}(i)$ 由低精度浮点运算模拟器计算得到，其中 $i \in \{0,\cdots,2^n\}$。从这些仿真数据又可以进一步检验定理 2的正确性。

根据定理 2可知，浮点运算域上混沌映射的状态映射网络可以看作定点运算域上其对应状态映射网络的子网络重构。更准确地说，SMN $F_{l,m}$ 可由 SMN F_n 生成，当 $2^{n-j}-(k+1)\cdot 2^{n-m-1-j} < F_n(i) < 2^{n-j}-k\cdot 2^{n-m-1-j}$ 时，指向 $F_n(i)$ 的所有节点重新指向节点 $2^{n-j}-(k+1)\cdot 2^{n-m-1-j}$；当 $F_n(i) = 2^{n-j}-k\cdot 2^{n-m-1-j}$ 时，除节点“2^n”，指向 $F_n(i)$ 的其余节点重新指向节点 $2^{n-j}-k\cdot 2^{n-m-1-j}$ 和 $2^{n-j}-(k+1)\cdot 2^{n-m-1-j}$，$j \in \{2^{l-1}-4,\cdots,1,0\}$，$k = 0 \sim 2^m-1$；当 $0 < F_n(i) < 2^{m+1}$ 时，指向 $F_n(i)$ 的所有节点重新指向节点 $F_n(i)$ 和 $F_n(i)-1$。SMN $F_{l,m}$ 生成过程可以通过分析图 3.10和图 3.11进一步验证。



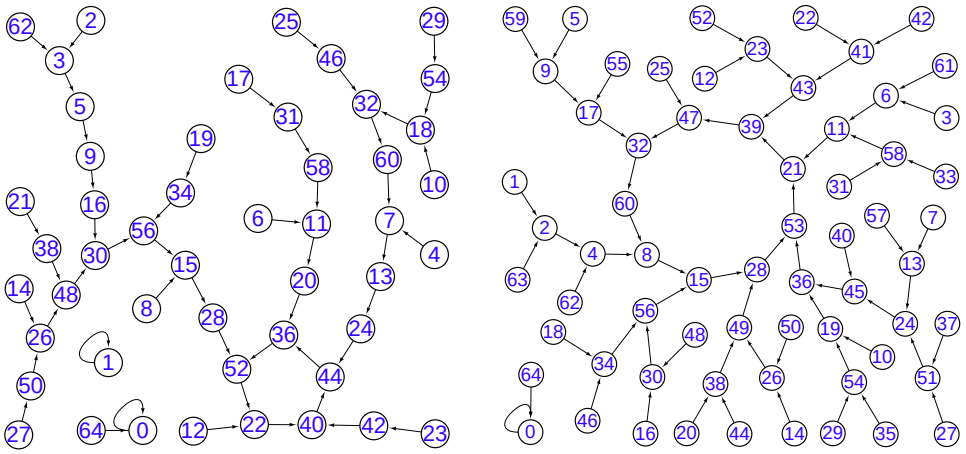
a) b)

图 3.9 浮点运算域上 Logistic 映射的状态映射网络的节点累积入度分布和入度分布



a) b)

图 3.10 控制参数 $\mu = 62/2^4$ 时，Logistic 映射的状态映射网络：a) $(l, m) = (3, 4)$；b) $n = 6$



a) b)

图 3.11 控制参数 $\mu = 15/2^4$ 时，Tent 映射的状态映射网络：a) $(l, m) = (3, 4)$；b) $n = 6$

图 3.9 a) 为浮点运算域上 Logistic 映射的状态映射网络的节点累积入度分布，图 3.9 b) 为其入度分布。根据定理 1和定理 2可知，浮点运算域上 Logistic 映射的状态映射网络的节点累积入度分布和入度分布逼近对应定点运算域上其幂律分布。上述讨论可以通过图 2.4、图 2.5和图 3.9之间的对比分析进一步得到验证，这里 $l = 4$。

3.4 本章小结

本章讨论了数字计算机上分段线性混沌映射 Tent 映射的相关动力学性质，首先利用整数量化函数准确推导出了 Tent 映射的状态映射网络 F_n^* 与实现精度 n 之

间的关系，理论上证明了 Tent 映射的状态映射网络的节点入度取值范围；其次，严格证明了 Tent 映射的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，当初始条件 $x(0)$ 在浮点域上均匀分布时，平均迭代次数通常比最大迭代次数要小得多。该结论可以直接推广到其他类似混沌映射，如 Bernoulli 移位映射、V-映射、Baker 映射；最后，初步揭示了定点和浮点运算域上混沌映射的状态映射网络 f_n 与 $f_{l,m}$ 之间的关系，根据它们之间的关系，对混沌系统的分析可能会变得容易一些。

第 4 章　二维离散 Cat 映射的状态网络分析

4.1　二维离散 Cat 映射的定义

Arnold's Cat 映射 $f(x,y)=(x+y,x+2y)\pmod 1$ 是最著名的混沌映射之一，它在有限区域内进行反复折叠、拉伸变化，可用来置换图像像素的位置 [74, Fig. 1.17]，其矩阵表示形式为

$$f(\mathbf{x})=(\Phi\cdot\mathbf{x})\pmod N, \tag{4.1}$$

其中 N 为正整数，$\mathbf{x}$ 为 $n\times 1$ 向量，Φ 为 $n\times n$ 矩阵，且其行列式为 1。Cat 映射可以通过各种方法进行扩展，如改变变换矩阵 Φ 的元素范围 [75]；将变换矩阵扩展到 2 维，3 维甚至更高维 [76]；修改模数 N [77]。

二维有限整数域上的扩展离散 Cat 映射 (GDCM) 在密码学领域有着十分广泛的应用，例如其可以直接应用于图像像素位置置乱，其矩阵表示形式为

$$f\begin{bmatrix}x_n\\ y_n\end{bmatrix}=\begin{bmatrix}x_{n+1}\\ y_{n+1}\end{bmatrix}=\begin{bmatrix}1 & p\\ q & 1+p\cdot q\end{bmatrix}\cdot\begin{bmatrix}x_n\\ y_n\end{bmatrix}\bmod N, \tag{4.2}$$

这里 $x_n,y_n\in\mathbb{Z}_N$，$p,q,N\in\mathbb{Z}^+$。

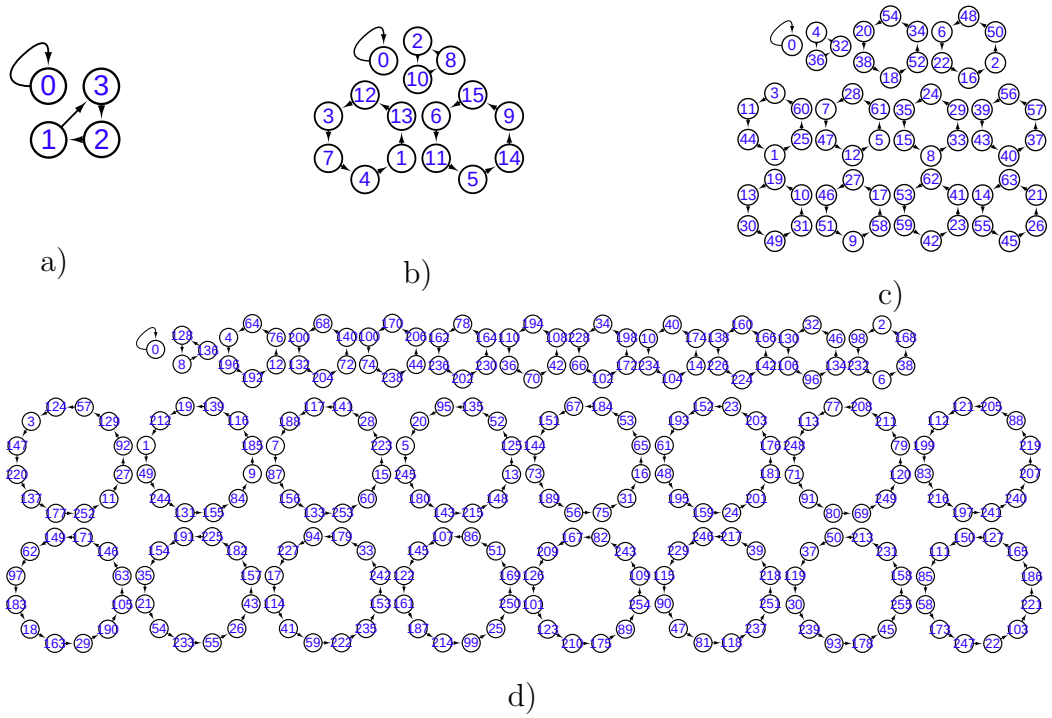


图 4.1 有限域 $\mathbb{Z}_{2^e}$ 上 GDCM (4.2) 的状态映射网络，其中 $(p,q)=(1,3)$：a) $e=1$；b) $e=2$；c) $e=3$；d) $e=4$

1992 年，Dyson 等人从理论上推导出了控制参数 $(p,q)=(1,1)$ 时 GDCM (4.2) 的周期上界和下界 [78]；2012 年，J. Bao 等人进一步揭示了某些约束条件下 GDCM (4.2) 的相关性质 [79]；在 [80–83] 中，F. Chen 使用 Hensel 上升法准确推导出了任意参数 p,q 下 GDCM (4.2) 的周期分布，整个分析根据 N 对 $(\mathbb{Z}_N,+,\cdot)$ 的代数性质的影响分为三部分：N 为素数时 $(\mathbb{Z}_N,+,\cdot)$ 为伽罗瓦域 [81]；N 为素数的幂时 $(\mathbb{Z}_N,+,\cdot)$ 为伽罗瓦环 [80,82]；N 为常见复合数时 $(\mathbb{Z}_N,+,\cdot)$ 为交换环 [83]。根据所用分析方法，第二种情况又分为两种子情况 $N=p^e$ 和 $N=2^e$，其中 p 为大于等于 3 的素数，e 为整数。从数字设备中实际应用的角度来看，Galois 环的情况最为重要，因为它与 e 比特定点运算格式表示的数字集同构。

4.2 定点域上离散 Cat 映射的性质分析

性质 6 T 的表示形式由 p 和 q 的奇偶性决定：

$$T=\begin{cases}2^k, & 2\mid p \text{ 或 } 2\mid q;\\ 3\cdot 2^{k'}, & 2\nmid p \text{ 且 } 2\nmid q.\end{cases} \tag{4.3}$$

其中 $k\in\{0,1,\cdots,e\}$，$k'\in\{0,1,\cdots,e-2\}$。

GDCM (4.2) 的周期 T 的表示形式如 (4.3) 式所示，这里 $N=2^e$。周期为 T 的不同 Cat 映射的数量 N_T 与周期 T 之间的关系被准确推导：

$$N_T=\begin{cases}1 & T=1;\\ 3 & T=2;\\ 2^{e+1}+12 & T=4;\\ 2^{e-1}+2^e & T=6;\\ 2^{e+k-2}+3\cdot 2^{2k-2} & T=2^k,\ k\in\{3,4,\cdots,e-1\};\\ 2^{2e-2} & T=2^e;\\ 2^{e+k-1} & T=3\cdot 2^k, k\in\{0,2,3,\cdots,e-2\},\end{cases} \tag{4.4}$$

其中 $e\geq 4$。

当 $e=3$ 时，

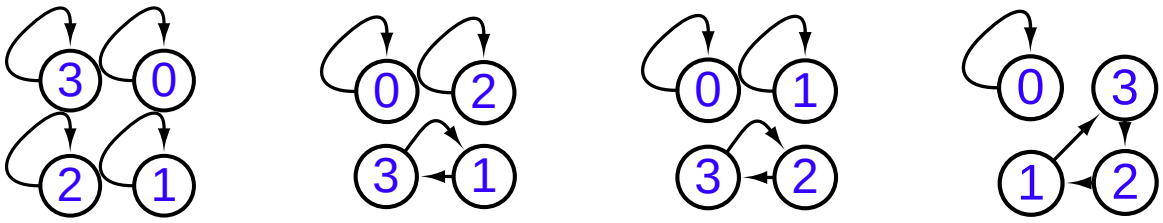
$$N_T=\begin{cases}1 & T=1;\\ 3 & T=2;\\ 2^{e-1} & T=3;\\ 2^{e+1}+12 & T=4;\\ 2^{e-1}+2^e & T=6;\\ 2^{2e-2} & T=8,\end{cases}$$

不可以表示为表 [82, Table III] 所示一般形式 (4.4)，例如当 $e = k = 3$ 时，$2^{2e-2} \neq 2^{e+k-2} + 3 \cdot 2^{2k-2}$。根据 (4.4) 式可知：当 $T \leq 6$ 时，GDCM (4.2) 的数量 $N_T = (1 + 3 + 2^{e-1} + 2^{e+1} + 12 + 2^{e-1} + 2^e) = 2^{e+2} + 16$。$e \geq 32$ 时，这对普通数字计算机来说是一个巨大的数字。

GDCM (4.2) 对应的状态映射网络 F_e 可通过以下方式构造：1) 将 N^2 个可能状态看作 N^2 个节点；2) 若 $\mathbf{x}_2 = f(\mathbf{x}_1)$，则对应向量 $\mathbf{x}_1 = (x_1, y_1)$ 的节点指向对应向量 $\mathbf{x}_2 = (x_2, y_2)$ 的节点。为方便起见，采用双射 $z_n = x_n + (y_n \cdot N)$ 对 GDCM (4.2) 的二维向量进行降维处理。为进一步阐明 GDCM (4.2) 的状态映射网络关于定点运算精度 e 的变化，令

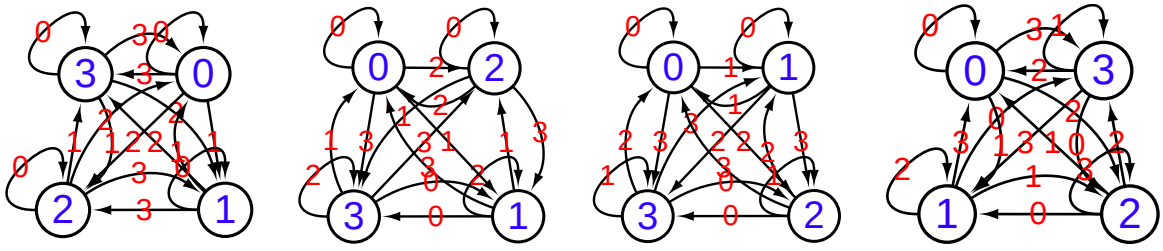
$$z_{n,e} = x_{n,e} + (y_{n,e} \cdot 2^e), \tag{4.5}$$

其中 $x_{n,e}, y_{n,e}$ 分别表示 $N = 2^e$ 时 GDCM (4.2) 的向量分量 x_n, y_n。图 4.1为 $(p, q) = (1, 3)$ 时有限域上 GDCM (4.2) 的状态映射网络 F_e。根据图 4.1可以看出，GDCM (4.2) 的状态映射网络随着定点运算精度 e 的增大呈现出很强的规律性。



a) b) c) d)

图 4.2 $N = 2$ 时，GDCM (4.2) 的 4 个可能状态映射网络：a) p 和 q 都为偶数；b) p 为偶数，q 为奇数；c) p 为奇数，q 为偶数；d) p 和 q 都为奇数



a) b) c) d)

图 4.3 (4.8) 式中 $(a_n + 2b_n)$ 与 $(a_{n+1} + 2b_{n+1})$ 之间的映射，箭头旁边所示为 $(k_x + 2k_y)$ 的值：a) p 和 q 都为偶数；b) p 为偶数，q 为奇数；c) p 为奇数，q 为偶数；d) p 和 q 都为奇数

性质 7 *GDCM (4.2)* 定义集合 $(0, 1, 2, \cdots, N^2 - 1)$ 上的双射。

证 因为 *Cat* 映射 (4.2)为保面积映射，所以其为有限域 $\mathbb{Z}_N^2$ 上的双射，根据 *(4.5)* 式，*Cat* 映射可进一步转换为有限域 $\mathbb{Z}_{N^2}$ 上的双射。 ■

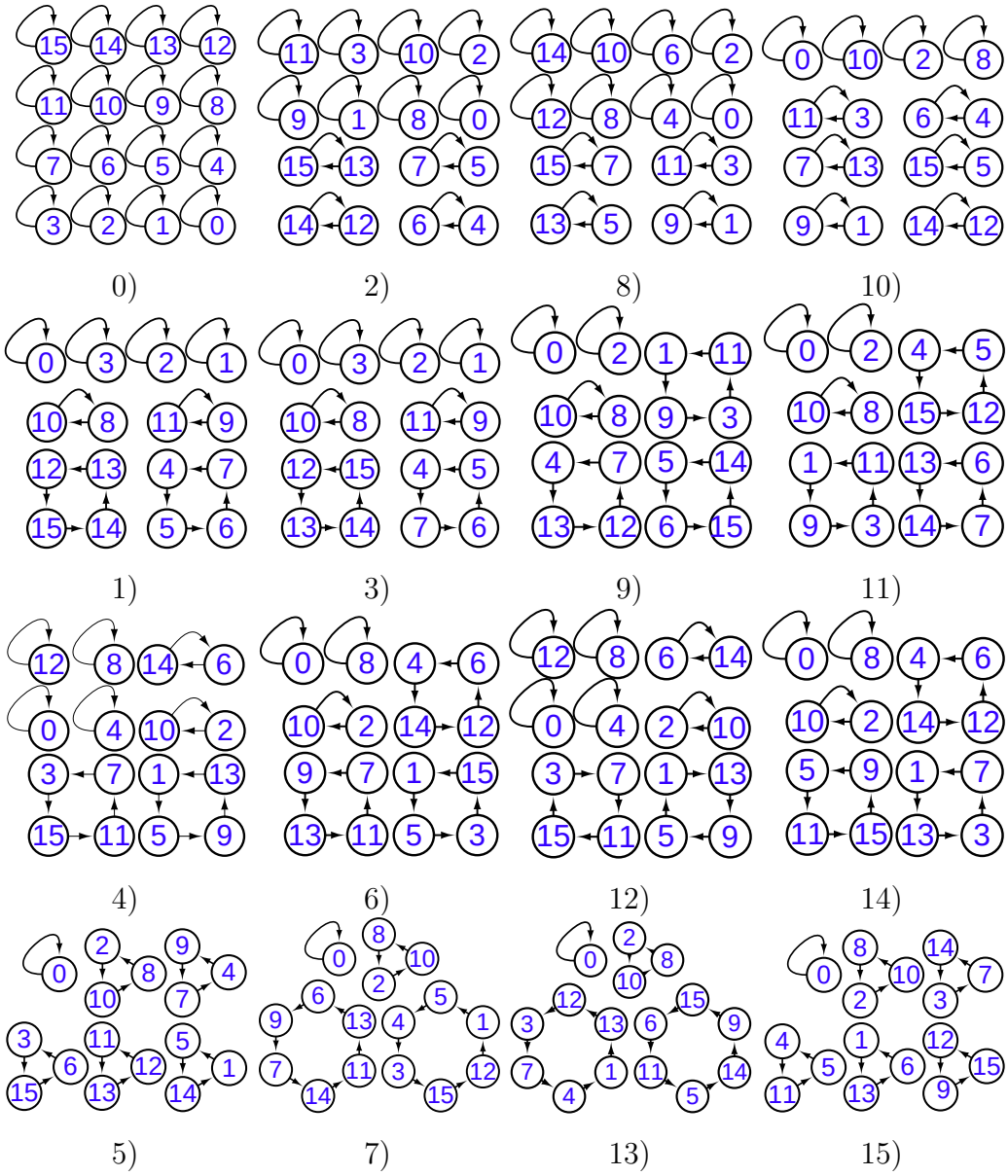
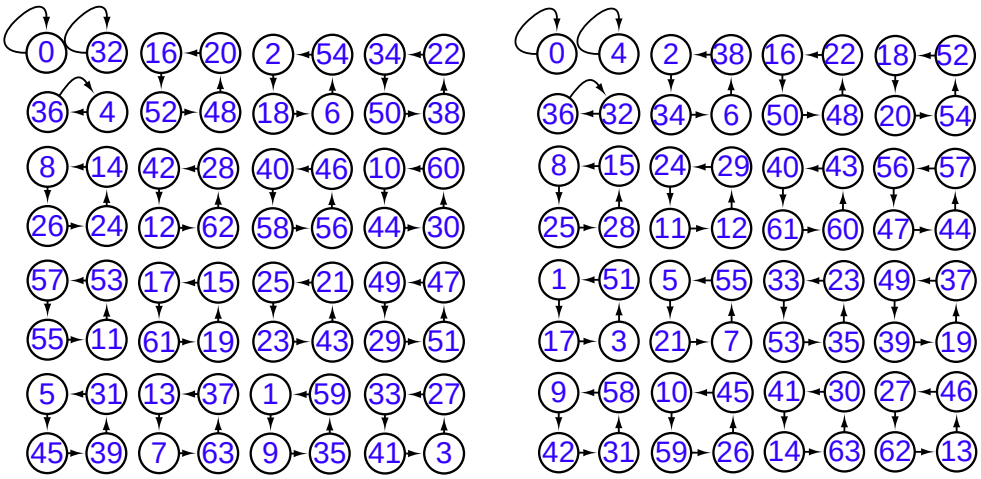


图 4.4 $N = 2^2$ 时，GDCM (4.2) 的所有可能状态映射网络，第 i 个子图对应参数 (p, q) 满足 $i = p \bmod 4 + (q \bmod 4) \cdot 4$

性质 8 给定 N，*GDCM (4.2)* 状态映射网络的任何节点仅且只属于一个环，*GDCM (4.2)* 将环上每个节点依次迭代映射到环上另一个节点。

证 根据 *[84, Theorem 5.1.1]* 可知，集合 $(0, 1, 2, \cdots, N^2 - 1)$ 关于 *GDCM (4.2)* 被划分为若干个不相交的子集，且每个子集构成一个环。 ■

GDCM (4.2) 的状态映射网络由许多短周期环构成，图 4.1 d) 所示状态映射网络由 16 个周期为 12 的环，10 个周期为 6 的环，1 个周期为 3 的环和 1 个自环构成。GDCM (4.2) 的周期为对应状态映射网络中所有可能周期的最小公倍数，但参数 p, q 与 GDCM (4.2) 周期之间的具体关系仍未可知 [85]。



a) b)

图 4.5 $N = 2^3$ 时，GDCM (4.2) 的状态映射网络：a) $(p, q) = (2, 1)$；b) $(p, q) = (1, 2)$

F_e 与 F_{e+1} 之间存在强相关关系，F_e 中节点 $z_{n,e} = x_{n,e} + y_{n,e}2^e$ 被演化为 F_{e+1} 中节点

$$\begin{aligned} z_{n,e+1} &= (x_{n,e} + a_n 2^e) + (y_{n,e} + b_n 2^e)2^{e+1} \\ &= z_{n,e} + (a_n 2^e + y_{n,e}2^e + b_n 2^{2e+1}), \end{aligned} \tag{4.6}$$

其中 $a_n, b_n \in \{0, 1\}$。性质 9揭示了 F_e 中节点 $z_{n,e}$ 的迭代节点与 F_{e+1} 中对应节点之间的演化规律，性质 10揭示了 F_e 中给定环与 F_{e+1} 中对应环之间的具体关系。

性质 9 若 $N = 2^e$ 时 *GDCM (4.2)* 的输入与 $N = 2^{e+1}$ 时 *GDCM (4.2)* 的输入满足关系

$$\begin{bmatrix} x_{n,e+1} - x_{n,e} \\ y_{n,e+1} - y_{n,e} \end{bmatrix} = \begin{bmatrix} a_n \\ b_n \end{bmatrix} \cdot 2^e, \tag{4.7}$$

则有

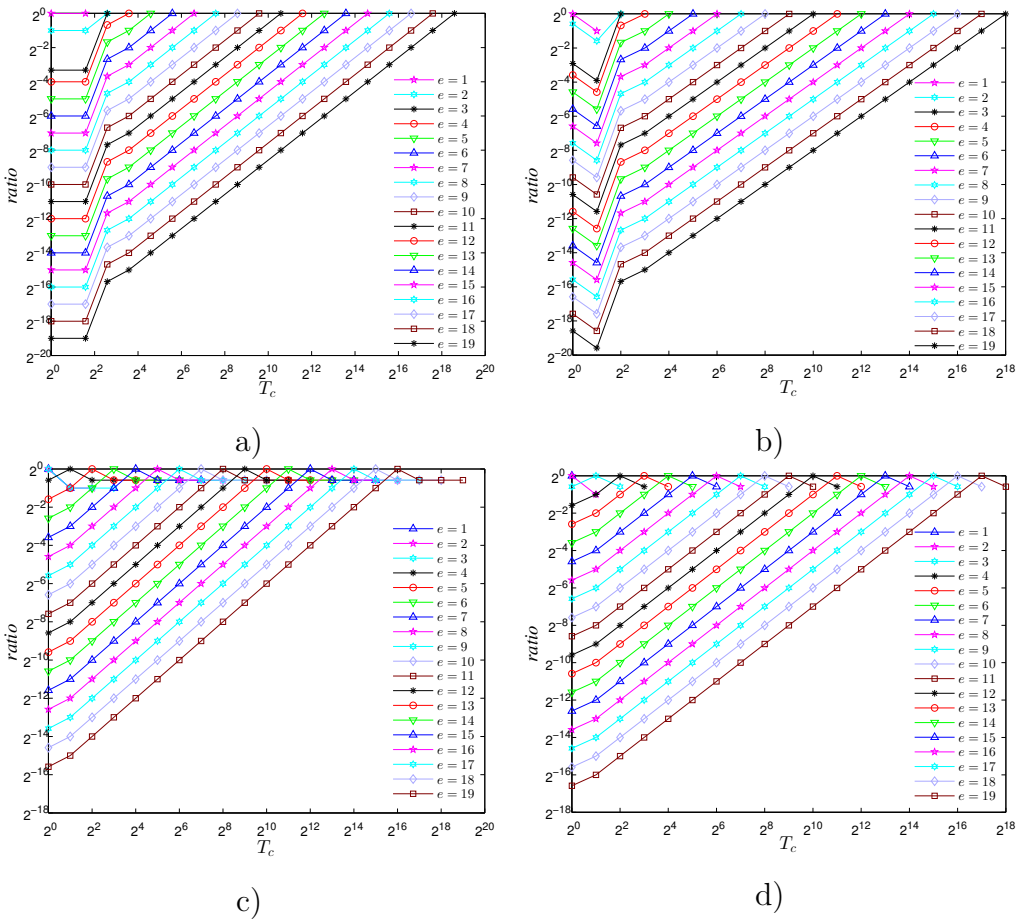
$$\begin{bmatrix} a_{n+1} \\ b_{n+1} \end{bmatrix} = \left[\begin{bmatrix} 1 & p \\ q & 1 + p \cdot q \end{bmatrix} \cdot \begin{bmatrix} a_n \\ b_n \end{bmatrix} + \begin{bmatrix} k_x \\ k_y \end{bmatrix} \right] \bmod 2, \tag{4.8}$$

$a_n, b_n \in \{0, 1\}$，$k_x = \lfloor k'_x/2^e \rfloor$, $k_y = \lfloor k'_y/2^e \rfloor$，且

$$\begin{bmatrix} k'_x \\ k'_y \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & 1 + p \cdot q \end{bmatrix} \cdot \begin{bmatrix} x_{n,e} \\ y_{n,e} \end{bmatrix}. \tag{4.9}$$

证 根据 $N = 2^e$ 时 *GDCM (4.2)* 与 $N = 2^{e+1}$ 时 *GDCM (4.2)* 之间的线性关系，可得

$$\begin{bmatrix} x_{n+1,e+1} - x_{n+1,e} \\ y_{n+1,e+1} - x_{n+1,e} \end{bmatrix} \equiv \begin{bmatrix} 1 & p \\ q & 1 + p \cdot q \end{bmatrix} \begin{bmatrix} x_{n,e+1} - x_{n,e} \\ y_{n,e+1} - y_{n,e} \end{bmatrix} + 2^e \begin{bmatrix} k_x \\ k_y \end{bmatrix} \bmod 2^{e+1}. \tag{4.10}$$



a) b) c) d)

图 4.6 有限域 $\mathbb{Z}_{2^e}$ 上 GDCM (4.2) 的环分布，其中 $e = 1 \sim 19$：a) $(p, q) = (5, 7)$；b) $(p, q) = (6, 7)$；c) $(p, q) = (7, 8)$；b) $(p, q) = (12, 14)$

$$k \cdot a \equiv k \cdot a' \bmod m \tag{4.11}$$

当且仅当

$$a \equiv a' \left(\bmod \frac{m}{\gcd(m, k)} \right), \ a_{n+1,e}, b_{n+1,e} \in \{0, 1\}. \tag{4.12}$$

将条件 *(4.7)* 代入余式 *(4.10)*，根据 *(4.12)* 式，余式两边和模数同除以 2^e 即可证明上述性质。 ■

性质 10 给定 *SMN* F_e 中环 $\boldsymbol{Z}_e = \{z_{n,e}\}_{n=0}^{T_c-1} = \{(x_{n,e},\ y_{n,e})\}_{n=0}^{T_c-1}$ 及其上任意节点 $z_{n_0,e}$，*SMN* F_{e+1} 中节点 $z_{n_0,e+1}$ 所在环为

$$\boldsymbol{Z}_{e+1} = \{z_{n,e+1}\}_{n=n_0}^{n_0+kT_c-1},$$

其中

$$k = \#\{(a_{n_0}, b_{n_0}), (a_{n_0+T_c}, b_{n_0+T_c}), (a_{n_0+2T_c}, b_{n_0+2T_c}), (a_{n_0+3T_c}, b_{n_0+3T_c})\}, \tag{4.13}$$

对任意 $n \geq T_c$，$n' = n \bmod T_c$，存在 $z_{n,e} = z_{n',e}$。$\{(a_n, b_n)\}_{n=n_0}^{n_0+3T_c}$ 由 (4.8)式迭代生成，$\#(\cdot)$ 返回集合基数。

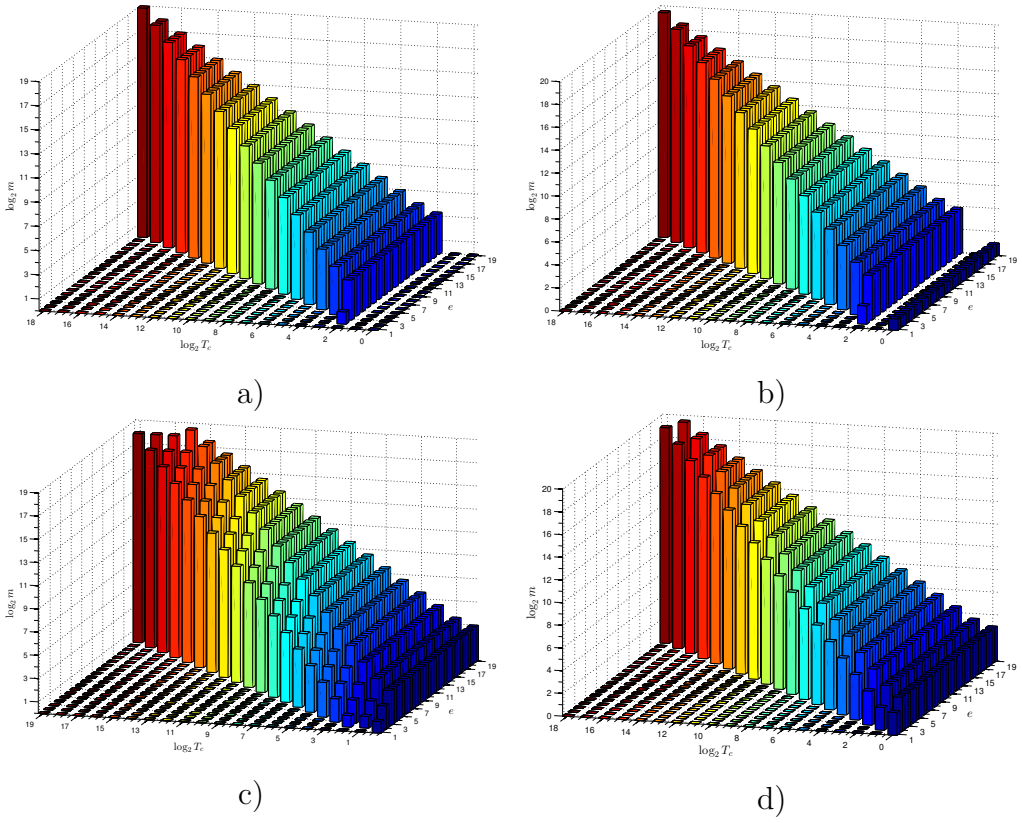


图 4.7 有限域 $\mathbb{Z}_{2^e}$ 上 GDCM (4.2) 的环分布，其中 $e = 1 \sim 19$：a) $(p, q) = (5, 7)$；b) $(p, q) = (6, 7)$；c) $(p, q) = (7, 8)$；b) $(p, q) = (12, 14)$

证 给定环 $\boldsymbol{Z}_e$ 上任意节点 $z_{n_0,e}$ 和 *(4.8)* 式中向量 (k_x, k_y)，则 *(4.8)* 式为集合上 $\{(0,0),(0,1),(1,0),(1,1)\}$ 的双射。$z_{n,e+1} \in \{z_{j,e+1}\}_{j=n_0}^{n}$ 当且仅当 $(n-n_0) \bmod T_c = 0$，且 $n > n_0$。 ■

性质 11 若 *SMN* F_e 中环 $\boldsymbol{Z}_e$ 和 *SMN* F_{e+1} $\boldsymbol{Z}_{e+1}^i$ 满足条件 *(4.7)*，则

$$\begin{bmatrix} a_{n+1,e+1}^d \\ b_{n+1,e+1}^d \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & 1+p\cdot q \end{bmatrix} \cdot \begin{bmatrix} a_{n,e+1}^d + a_{n,e}^d \\ b_{n,e+1}^d + b_{n,e}^d \end{bmatrix} \bmod 2, \tag{4.14}$$

其中 $a_{n,e}^d, a_{n,e}^d \in \{-1, 0, 1\}$，$i = 1 \sim 2$。

证 将 (4.7)式代入 (4.9)式，可得

$$\begin{bmatrix} k_x' \\ k_y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & 1+p\cdot q \end{bmatrix} \cdot \begin{bmatrix} x_{n,e} + a_{n,e}^i \cdot 2^e \\ y_{n,e} + b_{n,e}^i \cdot 2^e \end{bmatrix}, \tag{4.15}$$

且 $k_x^i = \lfloor k_x'/2^e \rfloor$，$k_y^i = \lfloor k_y'/2^e \rfloor$。

将上述计算结果代入 (4.8)式，进一步可得

$$\begin{bmatrix} a_{n+1,e+1}^1 \\ b_{n+1,e+1}^1 \end{bmatrix} = \left[\begin{bmatrix} 1 & p \\ q & 1+p\cdot q \end{bmatrix} \begin{bmatrix} a_{n,e+1}^1 \\ b_{n,e+1}^1 \end{bmatrix} + \begin{bmatrix} k_x^1 \\ k_y^1 \end{bmatrix} \right] \bmod 2, \tag{4.16}$$

$$\begin{bmatrix} a^2_{n+1,e+1} \\ b^2_{n+1,e+1} \end{bmatrix} = \left[\begin{bmatrix} 1 & p \\ q & 1+p\cdot q \end{bmatrix} \begin{bmatrix} a^2_{n,e+1} \\ b^2_{n,e+1} \end{bmatrix} + \begin{bmatrix} k^2_x \\ k^2_y \end{bmatrix} \right] \bmod 2. \tag{4.17}$$

故将 (4.16)式与 (4.17)式相减即可证明上述性质。 ■

表 4.1 $p, q \in \mathbb{Z}_{17}$ 时满足猜想 1的阈值 e_s, T_s

e, T_c \ q / p	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	3,6	4,8	4,12	2,4	4,6	5,8	5,12	1,2	3,6	4,8	4,12	2,4	5,6	6,8	6,12	1,2
2	4,8	3,4	5,8	2,2	4,8	3,4	6,8	2,2	4,8	3,4	5,8	2,2	4,8	3,4	7,8	2,2
3	4,12	5,8	3,6	2,4	6,12	4,8	4,6	1,2	4,12	7,8	3,6	2,4	5,12	4,8	5,6	1,2
4	2,4	2,2	2,4	3,2	2,4	2,2	2,4	3,2	2,4	2,2	2,4	3,2	2,4	2,2	2,4	3,2
5	4,6	4,8	6,12	2,4	3,6	7,8	4,12	1,2	5,6	4,8	5,12	2,4	3,6	5,8	4,12	1,2
6	5,8	3,4	4,8	2,2	7,8	3,4	4,8	2,2	5,8	3,4	4,8	2,2	6,8	3,4	4,8	2,2
7	5,12	6,8	4,6	2,4	4,12	4,8	3,6	1,2	8,12	5,8	5,6	2,4	4,12	4,8	3,6	1,2
8	1,2	2,2	1,2	3,2	1,2	2,2	1,2	4,2	1,2	2,2	1,2	3,2	1,2	2,2	1,2	4,2
9	3,6	4,8	4,12	2,4	5,6	5,8	8,12	1,2	3,6	4,8	4,12	2,4	4,6	9,8	5,12	1,2
10	4,8	3,4	7,8	2,2	4,8	3,4	5,8	2,2	4,8	3,4	6,8	2,2	4,8	3,4	5,8	2,2
11	4,12	5,8	3,6	2,4	5,12	4,8	5,6	1,2	4,12	6,8	3,6	2,4	6,12	4,8	4,6	1,2
12	2,4	2,2	2,4	3,2	2,4	2,2	2,4	3,2	2,4	2,2	2,4	3,2	2,4	2,2	2,4	3,2
13	5,6	4,8	5,12	2,4	3,6	6,8	4,12	1,2	4,6	4,8	6,12	2,4	3,6	5,8	4,12	1,2
14	6,8	3,4	4,8	2,2	5,8	3,4	4,8	2,2	9,8	3,4	4,8	2,2	5,8	3,4	4,8	2,2
15	6,12	7,8	5,6	2,4	4,12	4,8	3,6	1,2	5,12	5,8	4,6	2,4	4,12	4,8	3,6	1,2
16	1,2	2,2	1,2	3,2	1,2	2,2	1,2	4,2	1,2	2,2	1,2	3,2	1,2	2,2	1,2	5,2

SMN F_e 中周期为 T_c 的环演化结果对应 SMN F_{e+1} 中以下 5 种可能情况：1) 4 个周期为 T_c 的环；2) 1 个周期为 $2T_c$ 的环和 2 个周期为 T_c 的环；3) 2 个周期为 $2T_c$ 的环；4) 1 个周期为 $3T_c$ 的环和 1 个周期为 T_c 的环；5) 1 个周期为 $4T_c$ 的环。举例来说，图 4.1 a) 中自环 "$0 \to 0$" 被演化为图 4.1 b) 中自环 "$0 \to 0$" 和环 "$(0+2^1)=2 \to (0+2^3)=8 \to (0+2^1+2^3)=10 \to 2$"。类似的，图 4.1 a) 中环 "$1 \to 3 \to 2 \to 1$" 被演化为图 4.1 b) 中环 "$1 \to (3+2^1+2^3)=13 \to (2+2^3+2)=12 \to (1+2^1)=3 \to (3+2^1+2)=7 \to (2+2^1)=4 \to 1$" 和环 "$(1+2^3)=9 \to (3+2^1+2^3+2)=15 \to (2+2^1+2)=6 \to (1+2^1+2^3)=11 \to (3+2^1)=5 \to (2+2^1+2^3+2)=14 \to 9$"。根据上述分析可知，$e \geq 3$ 时 GDCM (4.2) 状态映射网络是由 $e=1$ 其状态映射网络演化而来的，例如 SMN F_e 中周期为 3 的倍数的环由 SMN F_1 中周期为 3 的基环生成。图 4.4第 6 个子图中自环 "$8 \to 8$" 被扩展为图 4.5中环 "$16 \to 52 \to 48 \to 20 \to 16$"，图 4.4第 9 个子图中自环 "$2 \to 2$" 被扩展为图 4.5中环 "$2 \to 34 \to 6 \to 38 \to 2$"。注意到，图 4.2 c) 中环 "$1 \to 1$" 被扩展为图 4.4中第 9 个子图中环 "$1 \to 9 \to 3 \to 11 \to 1$"，图 4.2 c) 中环 "$0 \to 0$" 被扩展为对应状态映射网络中 3 个环："$0 \to 0$"，"$2 \to 2$"，"$8 \to 10 \to 8$"。此外，图 4.1 b) 中环 "$1 \to 13 \to 12 \to 3 \to 7 \to 4 \to 1$" 被扩展为 4.1 c) 左下侧所示周期相同的 4 个环。因此上述 5 种可能情况均可在图 4.1、4.2、4.4中被发现。

根据图 4.6可以看出，SMN F_e 中环的周期分布呈幂律分布，图 4.7为其 3 维柱状图，其中 T_c 表示 SMN F_e 中环的周期。

猜想 1 存在阈值 e_s 和 T_s，使得 *SMN* F_e 中周期为 T_c 的环数与 *SMN* F_{e+1} 中周期为 $2T_c$ 的环数满足关系

$$2N_{T_c,e} = \begin{cases} N_{2T_c,e+1} & T_c \geq T_s; \\ 2N_{T_c,e_s} & T_c < T_s, \end{cases} \tag{4.18}$$

这里 $e \geq e_s$。

表 4.2 $(p,q) = (9,14)$ 时 SMN F_e 中周期为 T_c 的环数

$N_{T_c,e}$ T_c / e	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7
1	2	1	0	0	0	0	0	0
2	2	1	3	0	0	0	0	0
3	2	1	15	0	0	0	0	0
4	2	1	63	0	0	0	0	0
5	2	1	255	0	0	0	0	0
6	2	1	1023	0	0	0	0	0
7	2	1	4095	0	0	0	0	0
8	2	1	16383	0	0	0	0	0
9	2	1	16383	24576	0	0	0	0
10	2	1	16383	24576	49152	0	0	0
11	2	1	16383	24576	49152	98304	0	0
12	2	1	16383	24576	49152	98304	196608	0
13	2	1	16383	24576	49152	98304	196608	393216

根据性质 10可知，SMN F_e 中环 $\mathbf{Z}_e$ 由 F_1 中对应基环逐渐扩展而来，因此 SMN F_{e+1} 中给定周期的环数与 SMN F_e 中对应周期的环数满足某种线性关系，其与参数 p,q 有关。这里将其归结为猜想 1，该猜想可以通过 (p,q) 上的大量随机实验进一步得到验证，表 4.1给出 $p,q \in \mathbb{Z}_{17}$ 时满足猜想 1的 e_s, T_s。根据表 4.1，阈值 e_s, T_s 相对较小，$Prob[e_s \leq \log_2(16) = 4] = 25/32$。从图 4.6可以看出，等式 (4.18) 中第一种情况表示当 e 足够大时 SMN F_e 中环的周期分布呈指数为 1 的幂律分布，当 $e \geq e_s$ 时 SMN F_{e+1} 中任意周期的环数可以依据 SMN F_e 中对应周期的环数推导出来，此外，根据图 4.7，等式 (4.18) 中第二种情况表示任意周期的环数关于 e 单调增加，趋于常数。表 4.2给出 $(p,q) = (9,14)$ 时 SMN F_e 中周期为 T_c 的环量，可进一步验证上述分析讨论。

4.3 关于离散 Cat 映射 UPO's 的讨论

混沌系统中不稳定周期轨道 (UPO's) 的识别一直都是周期轨道理论的研究热点，构成混沌吸引子基本架构的无穷多不稳定周期轨道 (UPO's) 的稳定性取决于其与相空间中相邻轨道距离的变化趋势 [86]。在 [82] 中摘要部分，F. Chen 等人认为其研究有助于识别原始 Cat 映射的不稳定周期轨道，但其与通过分析 GDCM (4.2) 内部结构的演化过程所得结论不一致。图 4.8为图 4.1 c) 中环的相对位置，结合图 4.1和图 4.8可以发现，拥有指定周期的 Cat 映射的数量与对应状态映射网络中环的数量和相邻环之间的距离没有任何关系，因此依据指定周期的 Cat 映射的数量无法识别嵌入在混沌吸引子中的不稳定周期轨道 (UPO's)。

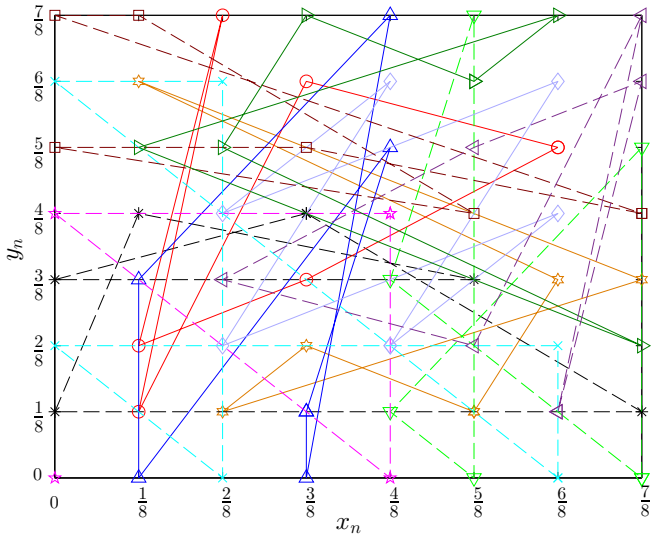


图 4.8 $N = 2^3, (p, q) = (1, 3)$ 时 GDCM (4.2) 的二维图形表示

4.4 本章小结

本章讨论了定点运算域上离散 Cat 映射的动力学特性，厘清了有限域上周期为 T 的不同离散 Cat 映射的数量 N_T 与周期 T 之间的关系，揭示了定点运算域上离散 Cat 映射的状态映射网络 F_e 与 F_{e+1} 之间的关系，即状态映射网络与实现精度之间的关系，研究发现，离散 Cat 映射状态网络中环的分布呈指数为 1 的幂律分布，但其幂律分布仍需进一步理论证明。

第 5 章　总结与展望

本文采用复杂网络的方法对几种典型的数字混沌系统的动力学性质进行了研究，主要研究成果如下：

- 利用整数量化函数准确推导出了定点运算域上一维混沌系统的状态映射网络(SMN)F_e 与 F_{e+1} 对应节点间的强相关性；以 Logistic 映射、Tent 映射为例，对定点运算域上一维混沌系统的 SMN F_e 与 SMN F_{e+1} 对应节点间的关系进行了具体分析。

- 理论上证明了定点运算域上 Logistic 映射状态网络的无标度属性；厘清了浮点运算域上系统量化误差对 Logistic 映射运算结果的影响，分析发现，在浮点运算中，运算顺序和数值范围会对运算结果产生影响；根据有限域上混沌系统的状态映射网络可对混沌伪随机数发生器进行分类，并可从本质结构上查找常规检测工具很难发现的随机性缺陷。

- 严格证明了数字计算机上 Tent 映射迭代值趋于零所需迭代次数 N_r；准确推导出了定点运算域上 Tent 映射状态网络的入度分布，Tent 映射状态网络的节点仅有 3 种可能入度取值；一定程度上厘清了定点和浮点运算域上混沌系统状态映射网络之间的关系，即浮点运算域上混沌系统的状态映射网络可以看作定点运算域上其对应状态映射网络的子网络重构。

- 对有限域上二维离散 Cat 映射周期为 T 的不同 Cat 映射的数量 N_T 与周期 T 之间的关系进行了分析讨论；采用降维的方法揭示了定点运算域上二维离散 Cat 映射 SMN F_e 与 SMN F_{e+1} 之间的关系；通过有限域 $\mathbb{Z}_{2^e}$ 上的随机实验发现二维离散 Cat 映射中环的分布呈指数为 1 的幂律分布。

在本论文的准备过程中，作者受限于水平和时间，有些问题没有得到妥善解决，这里简列如下：(1) 定点和浮点运算域上混沌系统状态映射网络之间的具体关系有待进一步深入探讨；(2) 二维离散 Cat 映射的环分布有待进一步理论证明。

参考文献

[1] MAY R M. Simple mathematical models with very complicated dynamics[J]. Nature, 1976, 261 : 459–467.

[2] ZAIKIN A N, ZHABOTINSKY A M. Concentration wave propagation in two-dimensional liquid-phase self-oscillating system[J]. Nature, 1970, 225 : 535–537.

[3] RöSSLER O E. An equation for continuous chaos[J]. Physics Letters A, 1976, 57(5) : 397 – –398.

[4] HéNON M. A two dimensional mapping with a strange attractor[J]. Communications in Mathematical Physics, 1976, 261 : 459– – 467.

[5] FEIGENBAUM M J. Quantitative universality for a class of nonlinear transformations[J]. J. Statistical Physics, 1978, 19(1) : 25–52.

[6] SHARKOVSKII A N. Coexistence of cycles of a continuous map of a line into itself (in Russian, English summaries)[J]. Ukrainskii Matemacheskii Zhurnal(Ukrainian Mathematical Journal), 1964, 16(1) : 61 – 71.

[7] LI T Y, YORKE J A. Period three implies chaos[J]. American Mathematical Monthly, 1975, 82(10) : 985 – 992.

[8] RUELLE D. Strange attractor[J]. The Mathematical Intelligencer, 1980, 2(1) : 126 – 137.

[9] SHARKOVSKII A N. Coexistence of cycles of a continuous map of a line into itself[J]. Int. J. Bifurcation and Chaos, 1995, 5 : 1263– – 1273.

[10] LORENZ E N. Deterministic non-periodic flow[J]. J. Atmospheric Sciences, 1963, 20 : 130–141.

[11] LORENZ E N. The predictability of hydrodynamic flow[J]. Trans. NY. Academy of Sciences Series II, 1963, 25 : 409–432.

[12] 郝柏林. 从抛物线谈起: 混沌动力学引论 [M]. 中国北京 : 北京大学出版社, 2013.

[13] 胡岗，肖井华，郑志刚. 混沌控制 [M]. 中国上海 : 上海科技教育出版社, 2001.

[14] 李树钧. 数字化混沌密码的分析与设计 [D]. 中国西安 : 西安交通大学电子与信息工程学院, 2003.

[15] 武相军. 复杂混沌动力学网络系统的同步及其应用研究 [D]. 中国上海: 上海交通大学电子信息与电气工程学院, 2011.

[16] KOCAREV L, SZCZEPANSKI J, AMIGÓ J M, et al. Discrete chaos–I: Theory[J]. IEEE Transactions on Circuits and Systems–I: Regular Papers, 2006, 53(6): 1300 – 1309.

[17] BLANK M. Discreteness and Continuity in Problems of Chaotic Dynamics, volume 161 of Translations of Mathematical Monographs[M]. [S.l.]: American Mathematical Society, Providence, Rhode Island, 1997.

[18] VOSS D F. Chaos on computers[J]. Science, 1989, 246(4934): 1172 – 1172.

[19] UMENO K, SATO A-H. Chaotic method for generating q-Gaussian random variables[J]. IEEE Transactions on Information Theory, 2013, 59(5): 3199 – 3209.

[20] PERSOHN K, POVINELLI R. Analyzing Logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation[J]. Chaos Solitons & Fractals, 2012, 45(3): 238 – 245.

[21] OTEO J, ROS J. Double precision errors in the Logistic map: Statistical study and dynamical interpretation[J]. Physical Review E, 2007, 76(3): 036214.

[22] GALIAS Z. The dangers of rounding errors for simulations and analysis of nonlinear circuits and systems–and how to avoid them[J]. IEEE Circuits and Systems Magazine, 2013, 13(3): 35 – 52.

[23] GREBOGI C, OTT E, YORKE J A. Roundoff-induced periodicity and the correlation dimension of chaotic attractors[J]. Physical Review A, 1988, 38(7): 3688.

[24] LI S, CHEN G, MOU X. On the Dynamical Degradation of Digital Piecewise Linear Chaotic Maps[J]. International Journal of Bifurcation and Chaos, 2005, 15(10): 3119 – 3151.

[25] ALVAREZ G, LI S. Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems[J], 2006, 16(8): 2129 – 2151.

[26] LIN T, CHUA L O. On chaos of digital filters in the real world[J]. IEEE Transactions on Circuits and Systems, 1991, 38(5): 557 – 558.

[27] SANG T, WANG R, YAN Y. Perturbance-based algorithm to expand cycle length of chaotic key stream[J]. Electronics Letters, 1998, 34(9): 873 – 874.

[28] HEIDARI-BATENI G, MCGILLEM C D. A chaotic direct-sequence spread-spectrum communication system[J]. IEEE Transactions on Communications, 1994, 42(234): 1524–1527.

[29] CHEN S-L, HWANG T, LIN W-W. Randomness enhancement using digitalized modified logistic map[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2010, 57(12): 996–1000.

[30] LI C-Y, CHEN Y-H, CHANG T-Y, et al. Period extension and randomness enhancement using high-throughput reseeding-mixing PRNG[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2012, 20(2): 385–389.

[31] ČERNÁK J. Digital generators of chaos[J]. Physics letters A, 1996, 214(3-4): 151–160.

[32] HUA Z, ZHOU Y. One-Dimensional Nonlinear Model for Producing Chaos[EB]. 2017.

[33] NAGARAJ N, SHASTRY M C, VAIDYA P G. Increasing average period lengths by switching of robust chaos maps in finite precision[J]. The European Physical Journal Special Topics, 2008, 165(1): 73–83.

[34] WU Y, ZHOU Y, BAO L. Discrete wheel-switching chaotic system and applications[J]. IEEE Transactions on Circuits and Systems I-Regular Papers, 2014, 61(12): 3469–3477.

[35] ADDABBO T, ALIOTO M, FORT A, et al. A feedback strategy to improve the entropy of a chaos-based random bit generator[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2006, 53(2): 326–337.

[36] DENG Y, HU H, XIONG W, et al. Analysis and design of digital chaotic systems with desirable performance via feedback control[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2015, 45(8): 1187–1200.

[37] PHATAK S C, RAO S S. Logistic map: A possible random-number generator[J]. Physical Review E, 1995, 51(4): 3670–3678.

[38] ULAM S M, von NEUMANN J. On combination of stochastic and deterministic processes[J]. Bulletin of the American Mathematical Society, 1947, 53(11): 1120.

[39] JESSA M. The period of sequences generated by Tent-like maps[J]. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 2002, 49(1): 84–89.

[40] MASUDA N, AIHARA K. Cryptosystems with discretized chaotic maps[J]. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 2002, 49(1): 28–40.

[41] ADDABBO T, ALIOTO M, FORT A, et al. The digital Tent map: performance analysis and optimized design as a low-complexity source of pseudorandom bits[J]. IEEE Transactions on Instrumentation and Measurement, 2006, 55(5): 1451–1458.

[42] JESSA M. Designing security for number sequences generated by means of the sawtooth chaotic map[J]. IEEE Transactions on Circuits and Systems–I: Regular Papers, 2006, 53(5): 1140–1150.

[43] ADDABBO T, ALIOTO M, FORT A, et al. A class of maximum-period nonlinear congruential generators derived from the Rényi chaotic map[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2007, 54(4): 816–828.

[44] CHEN F, WONG K-W, LIAO X, et al. Period distribution of the generalized discrete Arnold Cat map for $N = 2^e$[J], 2013, 59(5): 3249–3255.

[45] KOCAREV L, JAKIMOSKI G. Pseudorandom bits generated by chaotic maps[J]. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 2003, 50(1): 123–126.

[46] SEDGEWICK R, SZYMANSKI T G, YAO A C. The complexity of finding cycles in periodic functions[J]. SIAM Journal on Computing, 1982, 11(2): 376–390.

[47] FLAJOLET P, ODLYZKO A M. Random Mapping Statistics[C] // Advances in Cryptology – Crypto'89: Vol 434. 1990: 329–354.

[48] MIYAZAKI T, ARAKI S, NOGAMI Y, et al. Rounding logistic maps over integers and the properties of the generated sequences[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, 94(9): 1817–1825.

[49] ARAKI S, MURAOKA H, MIYAZAKI T, et al. A design guide of renewal of a parameter of the Logistic map over integers on pseudorandom number generator[C] // International Symposium on Information Theory and Its Applications. 2016: 781–785.

[50] ANON. Periods of sequences generated by the logistic map over finite fields with control parameter four[C]. [S.l.]: IEEE, 2016: 155–159.

[51] YANG B, LIAO X. Period analysis of the Logistic map for the finite field[J]. Science China Information Sciences, 2017, 60(2): 022302.

[52] CHEN F, WONG K-W, LIAO X, et al. Period distribution of generalized discrete Arnold cat map for $N = p^e$[J]. IEEE Transactions on Information Theory, 2012, 58(1): 445–452.

[53] YOSHIOKA D, KAWANO K. Periodic Properties of Chebyshev Polynomial Sequences Over the Residue Ring $\mathbb{Z}/2^k\mathbb{Z}$[J/OL]. IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS II-EXPRESS BRIEFS, 2016, 63(8): 778–782. http://dx.doi.org/10.1109/TCSII.2016.2531058.

[54] YOSHIOKA D. Properties of Chebyshev Polynomials Modulo p^k[J]. IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS II-EXPRESS BRIEFS, 2018, 65(3): 386–390.

[55] ÖZTÜRK I, KILIÇ R. Cycle lengths and correlation properties of finite precision chaotic maps[J]. International Journal of Bifurcation and Chaos, 2014, 24(09): 1450107.

[56] ZHANG J, SMALL M. Complex network from pseudoperiodic time series: topology versus dynamics[J]. Physical Review Letters, 2006, 96(23): 238701.

[57] IBA T. Scale-Free Networks Hidden in Chaotic Dynamical Systems[EB]. 2010.

[58] BORGES E, CAJUEIRO D, ANDRADE R. Mapping dynamical systems onto complex networks[J]. The European Physical Journal B, 2007, 58(4): 469–474.

[59] IBA T. Hidden Order in Chaos: The Network-Analysis Approach To Dynamical Systems[C] // Proceedings of the Eighth International Conference on Complex Systems. 2011: 769–783.

[60] BINDER P M, JENSEN R V. Simulating chaotic behavior with finite-state machines[J]. Physical Review A, 1986, 34(5): 4460–4463.

[61] BINDER P. Limit-cycles in a quadratic discrete iteration[J]. Physica D, 1992, 57(1-2): 31–38.

[62] SHREIM A, GRASSBERGER P, NADLER W, et al. Network analysis of the state space of discrete dynamical systems[J]. Physical Review Letters, 2007, 98(19): 198701.

[63] XU C, LI C, Lü J, et al. On the network analysis of the state space of discrete dynamical systems[J/OL]. International Journal of Bifurcation and Chaos, 2017, 27(4): Article number 1750062. http://dx.doi.org/10.1142/S0218127417500626.

[64] KYRIAKOPOULOS F, THURNER S. Directed Network Representation of Discrete Dynamical Maps[C] // Lecture Notes in Computer Science, Vol 4488: International Conference on Computational Science. [S.l.]: Springer, 2007: 625–632.

[65] XU X, ZHANG J, SMALL M. Superfamily phenomena and motifs of networks induced from time series[J]. Proceedings of the National Academy of Sciences, 2008, 105(50): 19601–19605.

[66] LUQUE B, LACASA L, BALLESTEROS F J, et al. Feigenbaum graphs: a complex network perspective of chaos[J]. PLoS One, 2011, 6(9): art. no. e22411.

[67] DONNER R V, HEITZIG J, DONGES J F, et al. The geometry of chaotic dynamics–a complex network perspective[J]. European Physical Journal B, 2011, 84(4): 653–672.

[68] WANG S, LIU W, LU H, et al. Periodicity of chaotic trajectories in realizations of finite computer precisions and its implication in chaos communications[J]. International journal of modern physics B, 2004, 18(17): 2617–2622.

[69] RAU C. Half-precision floating point library[EB]. 2017.

[70] 周红，凌燮亭. 有限精度混沌系统的 m 序列扰动实现 [J]. 电子学报, 1997, 25(7): 95–97.

[71] RUKHIN A, et AL.. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications[EB]. 2010.

[72] ECUYER P L, SIMARD R. TestU01: A C library for empirical testing of random number generators[J]. ACM Transactions on Mathematical Software, 2007, 33(4): art. no. 22.

[73] 《现代应用数学手册》编委会. 现代应用数学手册: 概率论与随机过程卷 [M]. 中国北京: 清华大学出版社, 2000.

[74] ARNOL'D V I, AVEZ A. Mathematical methods of classical mechanics[M]. [S.l.]: New York: W. A. Benjamin, 1968.

[75] CHEN G, MAO Y, CHUI C K. A symmetric image encryption scheme based on 3D chaotic cat maps[J/OL]. Chaos Solitons & Fractals, 2004, 21(3): 749–761. http://dx.doi.org/10.1016/j.chaos.2003.12.022.

[76] KWOK H, TANG W K. A fast image encryption system based on chaotic maps with finite precision representation[J]. Chaos, Solitons & Fractals, 2007, 32(4): 1518–1529.

[77] WU Y, HUA Z, ZHOU Y. N-dimensional discrete cat map generation using laplace expansions[J/OL]. IEEE Transactions on Cybernetics, 2016, 46(11): 2622–2633. http://dx.doi.org/10.1109/TCYB.2015.2483621.

[78] DYSON F J, FALK H. Period of a discrete cat mapping[J]. The American Mathematical Monthly, 1992, 99(7): 603–614.

[79] BAO J, YANG Q. Period of the discrete arnold cat map and general cat map[J/OL]. Nonlinear Dynamics, 2012, 70(2): 1365–1375. http://dx.doi.org/10.1007/s11071-012-0539-3.

[80] CHEN F, WONG K-W, LIAO X, et al. Period distribution of generalized discrete Arnold cat map for $N = p^e$[J]. IEEE Transactions on Information Theory, 2012, 58(1): 445–452.

[81] CHEN F, LIAO X, WONG K-W, et al. Period distribution analysis of some linear maps[J/OL]. Communications in Nonlinear Science and Numerical Simulation, 2012, 17(10): 3848–3856. http://dx.doi.org/10.1016/j.cnsns.2012.02.021.

[82] CHEN F, WONG K-W, LIAO X, et al. Period distribution of the generalized discrete Arnold Cat map for $N = 2^e$[J], 2013, 59(5): 3249–3255.

[83] CHEN F, WONG K-W, LIAO X, et al. Period distribution of generalized discrete arnold cat map[J/OL]. Theoretical Computer Science, 2014, 552: 13–25. http://dx.doi.org/10.1016/j.tcs.2014.08.002.

[84] HALL M. The Theory of Groups[M]. [S.l.]: The Macmillan Co., New York, 1959.

[85] BOHME R, KEILER C. On the Security of "A Steganographic Scheme for Secure Communications Based on the Chaos and the Euler Theorem"[J]. IEEE Transactions on Multimedia, 2007, 9(6): 1325–1329.

[86] DAVIDCHACK R L, LAI Y-C. Efficient algorithm for detecting unstable periodic orbits in chaotic systems[J]. Physical Review E, 1999, 60(5): 6172–6175.

致　谢

行文至此，意味着我三年的硕士生涯已经进入尾声。回首过去三年的学术研究，有挣扎也有欣慰，但内心充盈最多的仍是感激。

首先我要感谢我的导师李澄清教授，李老师为我提供了力所能及的一切支持，不仅在学术上给予我耐心指导，在生活上也教会了我认真做事、踏实做人的人生哲学。在李老师的指导和鼓舞下，我的自主学习能力和心态有了很大提高。此外，他渊博的学术知识、严谨的治学态度和对问题敏锐的洞察力都使我受益匪浅。

感谢我的同门林东东和徐成、师弟李广和谭凯、师妹周黎和彭星，他们成熟稳重，朝气蓬勃，与他们的交流讨论让我对生活有了新的认知。感谢国家自然科学基金（61772447，61532020）对本文中研究的资助。

最后感谢我的妈妈和女友对我生活和学习无微不至的关怀和一如既往的支持与鼓励，让我可以心无旁骛地专注于学习和科研。

个人简历、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.