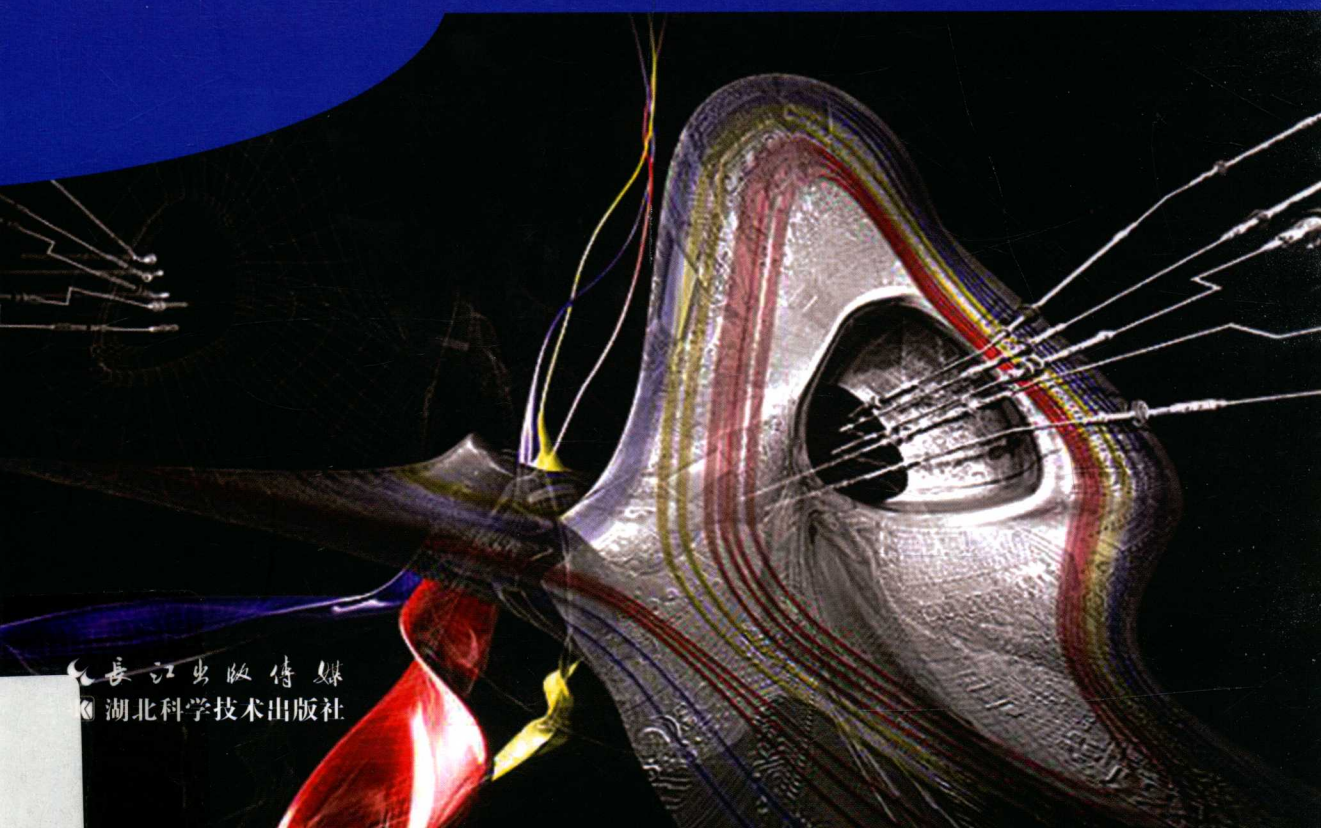
国家科学技术学术著作出版基金
NFAPST

“十二五”国家重点出版物出版规划项目
长江科学技术文库

胡汉平 著

混沌保密通信学

CHAOTIC SECURE COMMUNICATIONS



长江出版传媒
湖北科学技术出版社

国家科学技术学术著作出版基金资助出版
“十二五”国家重点出版物出版规划项目
长江科学技术文库

胡汉平 著

混沌保密通信学

CHAOTIC SECURE COMMUNICATIONS

长江出版传媒
湖北科学技术出版社

图书在版编目（CIP）数据

混沌保密通信学 / 胡汉平著. — 武汉 ： 湖北科学技术出版社，2015.9
(长江科学技术文库）
ISBN 978-7-5352-6986-7

Ⅰ. ①混… Ⅱ. ①胡… Ⅲ. 混沌理论—应用—保密通信 Ⅳ. ①TN918.6

中国版本图书馆CIP数据核字（2014）第202495号

策　　划：李海宁　　责任校对：蒋 静
责任编辑：李海宁 刘 辉 黄主梅 谢俊波 宋志阳 韩小婷　　封面设计：王 梅

出版发行：湖北科学技术出版社　　电话：027-87679468
地　　址：武汉市雄楚大街268号　　邮编：430070
（湖北出版文化城B座13-14层）
网　　址：http：//www.hbstp.com.cn

印　　刷：武汉中远印刷有限公司　　邮编：430034

787 × 1092　1/16　　19印张　480千字
2015年9月第1版　　2015年9月第1次印刷
定价：90.00元

内 容 提 要

本书主要以作者近年来在混沌保密通信学的理论和应用研究成果为主体，同时紧抓国际上学科发展的脉搏，总结了国内外该领域的最新研究成果和发展方向。本书分为两大部分：理论基础与实现技术。前者主要包括混沌动力学、混沌同步控制、反控制及混沌混合系统的建模与控制等理论与方法；后者主要包括混沌对称、非对称密码和混沌保密通信的实现技术、混沌密码的安全性评价方法及混沌保密通信的安全性分析等内容。全书不仅具有内容的先进性和主题的鲜明性，还实现了理论与实际应用的紧密结合，结构严谨，重点突出。

· 本书可供高等院校数学、通信、控制、信息安全的教学、科研人员及硕士、博士研究生，也可供对混沌动力学、混沌密码和保密通信感兴趣的读者作为参考书。

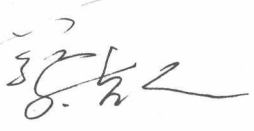
序

信息技术是一把“双刃剑”，随着以计算机技术和网络通信技术为代表的信息技术的不断发展和迅速普及，网络通信国际化、社会化、开放化以及个性化的特点，决定了它在给人们提供信息共享，为人类带来高效率、高效益以及高质量的同时，也投下了信息安全问题的阴影。信息安全已成为影响国家全局和长远利益的重大关键问题。密码技术是保障信息安全的基础，近 20 多年来它获得了空前的发展，应用领域不断拓展，理论与技术也实现了由传统密码向现代密码的重大变革。混沌密码、量子密码和生物密码等新型密码也应运而生。混沌理论被认为是继相对论、量子力学后，20 世纪人类科学研究领域的第三次革命。将混沌理论引入信息安全领域是当前国际非线性科学和信息科学两个学科交叉融合的热门前沿问题之一。作为其应用之一的混沌保密技术兴起于 1990 年前后，目前已成为当今世界信息安全研究的重要前沿领域之一。

在此背景下，整理编写有关混沌保密技术的著作，为从事混沌保密研究的相关人员提供最新的理论、方法与研究思路显得尤为必要。本专著作者及其课题组一直致力于混沌保密技术的理论、方法及应用研究工作，已承担并完成国家自然科学基金重大研究计划、国家自然科学基金、国家 863 计划和国家密码发展基金等多项课题的研究，在国内外发表了一系列高水平论文，获得了多项国内外发明专利授权，其自主研究的“混沌流密码”算法通过了国家密码局组织的算法审查，并纳入国家密码管理，被命名为“SSF46 密码算法”，取得了令人瞩目的成绩。该书以这些研究成果为基础，结合国际发展的主流，对国际上关于混沌保密技术的研究作了系统的总结与评述。书中探讨了混沌复杂动力学特性与密码学安全性之间的内在联系，为评估混沌密码系统的安全性、复杂性和可靠性提供了一套标准；揭示了数字混沌系统特性退化的本质，提出了多种可有效解决数字混沌系统

退化的方法，并借鉴混沌反控制的思想来探讨数字混沌系统特性退化问题的解决；提出的模/数混合混沌密码模型独具创新性，既使异地分离的连续混沌系统无需传输同步驱动信号就能稳定同步工作，又阻止了数字混沌系统出现特性退化，从而保证了整个混沌密码系统的安全性；提出了多种混沌保密系统安全性分析的新方法等。该书材料选择得当，组织合理，阐述清晰，条理分明，重点突出，对于相关的科研工作者，具有极高的可读性和参考价值。

当前，混沌保密技术已成为信息安全领域的研究热点，及时整理这方面最新的前沿研究成果，引导更多的研究者参与该领域的研究，促进该领域研究的发展具有重要意义。本书的出版恰逢其时，对国内学术界混沌密码和保密通信的研究具有重要的理论意义和实际应用价值。



（国家信息化专家咨询委员会委员、中国工程院院士）

2014 年 5 月 8 日

前　言

20 世纪 60 年代，美国科学家 Lorenz 在研究大气对流的过程中首次发现混沌吸引子，自此引发了混沌科学的研究热潮。混沌是自然界中普遍存在的现象，它是由确定性的非线性系统产生的类随机行为，这种行为的产生不需要施加任何外来随机输入，是由系统本身引发的。它是有序与无序的统一，确定性与随机性的统一，整体稳定与局部不稳定的统一。混沌运动对初始条件具有极端敏感性，这使得无法对混沌运动进行长期预测。混沌的提出颠覆了人们关于确定式可预测的猜想。

随着对混沌研究的逐步深入，人们发现混沌系统所具有的宝贵动力学特性与 Shannon 提出的经典密码设计准则“混淆性”和“扩散性”相一致，这种相似性引起了密码学界的高度关注，拉开了混沌密码研究的序幕。

在现实生活中，某些系统中存在的混沌现象可能会导致整个系统的失控或崩溃。在这种情形下，抑制混沌是十分必要的。而在某些领域，人们又发现混沌有着潜在的应用，如生物医学、图像加密处理、保密通信等领域。此时，混沌又是需要人们特意去产生或强化的，这就是混沌化（混沌反控制）。随着现代信息科学技术的迅猛发展和广泛应用，工业生产也随之向着大型化、综合化发展，形成了复杂的生产过程。整个过程中不仅包含连续的物理、化学及生物反应（通常用连续变量动态过程来描述），而且还受到大量逻辑规则的限制（通常用离散事件动态过程来描述），这两种不同动态过程间的相互耦合作用以及整个系统所表现出来的特殊动力学特性，使得将连续变量和离散事件两者结合起来研究显得尤为必要，从而导致了混杂系统的诞生和发展。由于光通信的高速发展，特别是全光网已成为未来通信的发展趋势，它的高速数据接入、传输对信息保密及其加解密速度提出了新的要求，因此，对激光混沌及其保密通信系统的研究也至关重要。密码的设计和分析向来是相辅相成的，现有的混沌密码设计缺乏足够的理论依据，往往依赖于设计者的经验和直觉。在密码系统设计完成之后对其安全性进行检测，如果不满足密码学安全性的要求，又必须重新选取设计，这种先验性的设计方法显然缺乏足够的科学性。如果能建立混沌复杂动力学特性与密码学安全性之间的内在联系，就可以从根本上解决这个问题。本课题组针对上述问题做了细致的研

究,这些研究工作使作者对混沌密码学理论及其应用有了更深入的了解,并促使作者写出此书,希望它的出版能为推动国内该领域的研究尽一份绵薄之力。

本书共9章,在结构上分为两大部分:混沌密码学的理论基础和混沌密码学的设计、实现与分析。第1章主要对混沌动力学的基础知识进行了总结。主要介绍了混沌的基本概念、性质、判定和一些经典的混沌系统。第2章主要介绍了混沌同步控制的相关理论、模型及其实现方法。第3章主要介绍了混沌反控制的相关理论及其实现方法。着重介绍了两种不同反控制方法——时变脉冲反控制方法和基于连续系统采样的反控制方法。第4章主要介绍了混合混沌系统的相关理论及控制方法。提出了一种新的混合系统模型——模数混合混沌系统模型,并在此基础上着重探讨了一种单向耦合的模数混合混沌系统的脉冲同步控制理论与方法。第5章主要介绍了混沌对称密码理论及其实现技术。提出了两种理想的混沌序列密码算法——具有可控统计特性的伪随机密钥流生成器和基于Chen混沌系统的伪随机密钥流生成器。提出了三种不同的解决混沌系统在有限精度下的动力学退化问题的新思路:变参数补偿方法、变参数控制方法以及模数混合混沌系统模型。并在此基础上构建了相应的序列密码系统或伪随机密钥流生成算法。第6章主要介绍了混沌非对称密码(混沌公钥密码)的设计方法和研究思路。阐述了几种常用的混沌公钥密码算法,提出了一种基于Logistic混沌映射的背包公钥算法。第7章主要介绍了基于混沌同步的混沌保密通信系统设计所涉及的关键理论和关键技术。从混沌源的选取、混沌同步控制方式的设计和调制方式的选择三个方面介绍了基于混沌同步的混沌保密通信系统设计的关键技术。并在此基础上提出了运用激光混沌来实现保密通信的新思路。第8章主要介绍了混沌密码的一些安全性评价方法。定量刻画了密码学复杂度与动力学复杂度之间的内在关系,为选取或构造满足密码学意义上安全性的混沌系统提供了坚实的理论依据。第9章主要介绍了基于混沌保密通信系统的安全性分析方法:针对两种不同情况——未知模型和已知模型,从不同侧面阐述了对混沌保密通信系统的安全性分析,提出了一系列新的密码分析方法,并特别提出了针对时滞混沌系统的安全性分析方法。

本书的出版得到了国家科学技术学术著作出版基金的资助,本书的编写得到了“十二五”国家密码发展基金“基于混沌的公钥密码研究”、“十一五”国家863计划“混沌密码系统的理论与实现技术”、国家密码发展基金“模数混合混沌密码系统的理论与研究方法”,“十五”国家863计划“混沌流密码及其密码芯片设计”、国家密码发展基金“混沌变码本流密码系统的理论与方法研究”,总参预研基

金“混沌序列密码编码理论与技术研究”，湖北省自然科学基金“混沌加密方法研究”、“混沌加密的应用研究”及“混沌密码系统的理论及其实现技术”等的资助，在此表示衷心的感谢！

感谢国家密码管理局及其北京电子技术研究所多年来对研究小组所给予的支持和帮助！在此特别要感谢蔡吉人院士、沈昌祥院士、冯登国教授及张焕国教授等给予的指导和支持！湖北科学技术出版社，尤其是李海宁编审对于本书成功申请到国家科学技术学术著作出版基金的资助作出了很大的努力，在此表示感谢！

本书的编写还得到了王祖喜副教授的具体帮助，研究生邓涯双、刘凌锋、高孝婧、郑鑫、谢飞龙、宋庆燕、陈笑风等参与了相应的研究工作和部分书稿的编写与整理工作，在此，作者一并向他们表示衷心感谢！

由于作者水平有限，书中难免存在不足之处，敬请读者批评指正。

胡汉平

2014 年 9 月 6 日于华中科技大学

目　录

第 1 章　混沌动力学的基础理论

牛顿的经典力学理论是现代科学的奠基石，海水涨落、自由落体等大量自然现象都可用牛顿力学及其经典理论来解释。除此之外，该理论还可以用于发现天体或者预测天体的运动。牛顿定律给我们这样一个启示：当物体的初始条件和相互之间的作用给定时，物体的运动轨迹就确定了，即使初始条件存在微小的误差，物体的运动趋势依然可以被推测出来。然而，牛顿力学仅适用于描述单体或者二体问题，而不适用于三体问题。法国数学家 Poincaré 在 19 世纪末 20 世纪初对三体问题进行了深入细致的研究，发现三体之间的相互作用给问题的求解带来了巨大的复杂性，导致三体问题无法得到精确解。通过应用动力学和拓扑学相关知识，他发现在一定范围内，三体问题的解是随机的。这表明：即使在一个确定性的系统中，系统的运行轨迹也可能极度不稳定，初值任何细微的变化都会导致完全不同的结果。这使许多科学家首次认识到确定性系统中也可能存在着内在随机性——混沌现象。遗憾的是，Poincaré 并没有沿着这条路继续走下去，他说“这些东西太稀奇古怪了，我没有耐性仔细考虑它们”。

20 世纪 60 ~ 70 年代是混沌研究发展突飞猛进的时代。Kolmogorov 与他的学生 Arnold 及瑞士数学家 Moser 在 1960 年前后，先后深入研究了哈密顿系统中的运动稳定性，得出了著名的 KAM 定理，为混沌的研究奠定了基础。

1963 年，Lorenz 首次给出了一个混沌解的例子。同年，他在美国《大气科学杂志》上发表了混沌领域具有奠基性意义的文章——《确定性非周期流》。文中 Lorenz 利用一个三维自治系统来描述天气的变化情况，发现天气的演化与初始条件密切相关，也就是后来人们常说的初值敏感性。Lorenz 将这一现象比喻为“来自南美洲巴西的一只蝴蝶扇动几下翅膀，可能会改变美国德克萨斯州 3 个月后的气候”，即著名的“蝴蝶效应”。Lorenz 所提出的三维自治系统（Lorenz 系统）是第一个具有数学解析描述的混沌模型，Lorenz 本人也被誉为“混沌之父”。

1964 年，Henon 等人以 KAM 理论为背景，在研究球状星团及 Lorenz 吸引子的过程中发现了一个哈密顿系统中的内随机现象，也就是后来人们所说的 Henon 映射。

1971 年，“奇怪吸引子”的概念被 Ruelle 以及 Takens 首次提出，并将其应用到了耗散系统之中，提出了一种新的湍流机制。美国数学家 Smale 在研究湍流过程中发现了一种类似“马蹄”的结构——Smale 马蹄吸引子，这是继 Lorenz 吸引子发现之后的另一重要的混沌吸引子。Smale 马蹄吸引子可被看成在一团橡皮泥上任意取两点，然后将橡皮泥拉长，再折叠回来，不断拉长、折叠，使之错综复杂地自我嵌套起来，从而形成的几何结构。在此基础上他又提出了一种马蹄变换，为混沌理论研究奠定了基础。

1975 年，李天岩和他的导师 Yorke 在文章《周期 3 蕴含着混沌》中首次明确提出了“混沌”一词，并给出了其第一个数学定义。自此，“混沌”一词被正式使用[1]。该文有一个直接的结论：如果一连续映射有周期为 3 的点，那它必存在任意周期。随后，人们发现这个结论不过是

Sharkovskii 定理的一个特例[2]。十分巧合的是，早在中国古代，《老子》就有“道生一，一生二，二生三，三生万物”的奇妙论述。

1976 年，May 在《自然》上发表了一篇题为《具有复杂动力学特性的简单数学模型》的文章，着重研究了一维平方映射，并指出在这类简单的一维映射中也存在着倍周期分叉以及混沌现象[3]。1978 年，Feigenbaum 针对该类一维映射，利用重整化群思想，提出了倍周期分叉通向混沌的两个普适常数，该常数对研究一维映射的混沌行为奠定了基础，具有里程碑意义[4]。同年，Marotto 提出了“返回扩张不动点”的概念并将 Li - Yorke 给出的混沌定义推广至高维情形[5]。迄今为止，这一理论仍是分析离散混沌系统最有效的方法。

1981 年，Takens 提出了一种判定奇怪吸引子的实验方法[6]，而由 Holmes 转述并发展的 Melnikov 理论分析方法则可用于判别二维系统中是否存在 Smale 马蹄混沌。从 20 世纪 90 年代开始，混沌开始飞速发展。1989 年，Devaney 从拓扑学出发，给出了混沌的另一个数学定义，该定义表明一个混沌系统应具备初值敏感性、拓扑传递性以及周期点稠密性[7]。其中，初值敏感性是混沌最本质的属性。截至目前，该定义与 Smale 之前提出的马蹄混沌以及 Li - Yorke 提出的混沌定义仍被看作是混沌的三大基本定义。

1998 年，陈关荣等人指出，Marotto 在 1978 年提出的高维空间混沌判据中存在错误[8]，他们认为该判据的证明过程中用到了一个错误的结论，这直接导致了判据的错误。自此，大批的研究者致力于对 Marotto 定理的改进研究[9-11]。

2004 年，史玉明等人给出了 Marotto 定理的一个改进方案，并进一步将 Marotto 定理推广至 Banach 空间[12]，随后又进一步建立了完备度量空间中的混沌反控制理论框架[13]，使得人们对混沌的研究不再局限于欧氏空间。近年来，有研究者将“返回扩张不动点”与同宿轨道或异宿轨道结合起来判定混沌[14]。

目前，混沌已被广泛应用于数学、物理、化学、医学、心理学、气象学、经济学以及信息科学等许多领域。混沌也是第一个将众多的学科和领域紧紧联系在一起的概念。混沌倡导者之一的 Shlesinger 说过：“相对论、量子力学和混沌是 20 世纪科学永远铭记的三件事。”因此，混沌可算得上是 20 世纪物理学上的第三次革命了。

1.1 混沌的基本概念

一般认为，混沌是一种在确定性系统中产生的类随机行为。这种随机的产生并不是由外部随机输入引发的，而是由系统本身引起的。与以往了解的确定性轨道有所不同，混沌系统的轨道在长期内是不可预测的。虽然从表面上看，混沌系统是无序的，然而其内部却有着有序的层次结构，是一种新型的非线性系统。一般地，动力系统可分为连续动力系统和时间离散动力系统，它们本质上都属于相空间连续系统。

混沌是自然界中一种普遍存在的现象，已受到人们的广泛关注。然而迄今为止，混沌还没有一个统一的定义。现有的定义都是从某个特定的角度来描述混沌的某种特性，其中应用最广泛的有三类：一是 Li - Yorke 混沌定义，它是从系统轨道角度阐述的；二是 Devaney 混沌定义，它是从拓扑角度阐述的；三是 Smale 马蹄混沌，它是从几何角度阐述的。

1975 年,李天岩和他的导师约克(Yorke)给出了混沌的第一个数学定义,即

Li – Yorke 定义[1] 设 $I\subset\mathbf{R}$,$f:I\to I$ 的连续映射,若其满足

(1)对任意的 $k=1,2,\cdots$ f 有 k 周期点;

(2)存在不可数子集 $S\subset[a,b]$,S 中无周期点,且满足

(a)对任意 $x,y\in S$,有 $\liminf\limits_{n\to\infty}|f^n(x)-f^n(y)|=0$;

(b)对任意 $x,y\in S$,$x\neq y$,有 $\limsup\limits_{n\to\infty}|f^n(x)-f^n(y)|>0$;

(c)对任意的 $x\in S$ 和 f 的任意周期点 $y\in I$,有 $\limsup\limits_{n\to\infty}|f^n(x)-f^n(y)|>0$。

上述定义表明,一个确定的混沌映射的轨道受初值条件不同的影响会表现出两种不同的性态:在某些区域,具有任意周期;在另一些不规则区域,只具有非周期轨道。任意两条不同的非周期轨道会任意接近,但又必须分离,即混沌不仅具有遍历性而且具有发散特性。任意的非周期轨道不能用周期轨道去逼近,即该区域内不存在渐近周期点。李天岩等人把该不规则区域称作映射 f 的混沌区域。

当 f 具有周期为 3 的点时,上述定理显然成立。这就是著名的“周期三意味着混沌”。从而可直接得出这样一个结论,只要一区间上的映射有周期为 3 的点,那么它就有任意周期点,即有如下结论:

定理 1.1[1] 设 $I\subset\mathbf{R}$,$f:I\to I$ 的连续映射,若存在点 $a\in I$,令 $b=f(a)$,$c=f^2(a)$,$d=f^3(a)$,满足如下条件:

$$d\leqslant a<b<c\ (d\geqslant a>b>c)$$

则定义在 I 上的变换 f 是 Li – Yorke 定义下的混沌系统。

事实上,早在 1964 年,苏联数学家 Sharkovskii 就给出了一个周期蕴含另一周期的更一般性的结论[2]。

定义 1.1[2] 定义自然数的一个优先次序“$\triangleright$”如下:

$$3\triangleright5\triangleright7\triangleright\cdots\triangleright2\cdot3\triangleright2\cdot5\triangleright\cdots\triangleright2^2\cdot3\triangleright2^2\cdot5\triangleright\cdots2^3\cdot3\triangleright2^3\cdot5\triangleright\cdots\triangleright\cdots2^3\triangleright2^2\triangleright2\triangleright1$$

可知,此序列首先列出了所有的奇数,然后是奇数的 2 倍,接着是奇数的 2^2 倍,再然后是奇数的 2^3 倍……这个过程能列完所有的自然数,除了最后列出的 2 的幂次,则有如下结论:

定理 1.2[2] 设 $f:\mathbf{R}\to\mathbf{R}$ 连续,f 具有 k 周期点,若在上面定义的序列中有 $k\triangleright l$,则 f 具有周期为 l 的点。

显然,定理 1.1 中的周期结论是定理 1.2 的一个推论。

受 Li – Yorke 工作的启发,1978 年,Marotto 将 Li – Yorke 定义下的混沌推广到 n 维情形。考察如下 n 维离散系统

$$x_{k+1}=f(x_k),x_k\in\mathbf{R}^n,k=0,1,2,\cdots \tag{1.1}$$

式中,f 是关于 x 的连续可微函数,记 $B_r^0(x)$ 为圆心在点 x 处半径为 r 的开球,$B_r(x)$ 为其闭包,则有如下 Marotto 定理。

Marotto **定理**[5] 如果 f 有一个返回扩张不动点,即满足如下两个条件的点 x^*:

(1)f 在 $B_r(x^*)$ 内连续可微,如果 $f(x^*)=x^*$ 且对于所有 $x\in B_r(x^*)$,$Df(x)$ 所有特征值的模均大于 1;

(2)存在 $x^0\in B_r(x^*)$,$x^0\neq x^*$,使得对某个正整数 m,有 $f^m(x^0)=x^*$ 且 $|Df^m(x^0)|\neq0$。

则系统(1.1)是 Li－Yorke 意义下的混沌。亦即,

(1)存在正整数 $\mathbf{N}$,使得对于任意整数 $p \geqslant \mathbf{N}$,f 有 p 周期点;

(2)存在一不规则集 S(不可数且不包含周期点),使得:

(a)$f(S) \subset S$;

(b)对任意 $x, y \in S, x \neq y$,有 $\limsup_{n\to\infty} \| f^n(x) - f^n(y) \| > 0$;

(c)对任意的 $x \in S$ 和 f 的任意周期点 y,有 $\limsup_{n\to\infty} \| f^n(x) - f^n(y) \| > 0$。

(3)存在不可数子集 $S_0 \subset S$,使得对于任意 $x, y \in S$,有 $\liminf_{n\to\infty} \| f^n(x) - f^n(y) \| = 0$。

此外,Marotto 在文献[5]中证明了一维情形下 f 的返回扩张不动点是 f^n 的周期为 3 的点。

Devaney 于 1989 年从系统轨道的不可预测性、不可分解性及具有规律性的行为这三大性质出发给出了一种适用于离散系统且较易验证的混沌定义。

Devaney 定义[7]　设 S 为一集合,S 上的连续变换 f 称为在 S 上是混沌的,如果

(1)f 有初值敏感性,即存在 $\varepsilon > 0$,对任意 x 及其邻域 U,均存在 $y \in U, n \in \mathbf{Z}^+$ 使得

$$|f^n(x) - f^n(y)| > \varepsilon;$$

(2)f 是拓扑传递的,即对于任意两开集 $U, V \subset \boldsymbol{S}$,存在 $k \in \mathbf{Z}^+$,使得 $f^k(U) \cap V \neq \emptyset$;

(3)周期点在 V 中稠密。

初值敏感性是指相近的两个点 x, y,经过 f 的作用在一定时间后会产生较大的分离。这就意味着混沌轨道在长时间内是不可预测的。值得注意的是,并非 x 附近所有的点都必须在迭代下与 x 分离,但至少要存在一个这样的点。

拓扑传递性是指任意一个集合中的任意一个点在 f 的作用下都能转移到任意另一个集合中,即不能将 f 分解为两个互不相关的子系统。

周期点集稠密意味着混沌不是完全无序的,而是在看似混乱之中隐藏着规律。

初值敏感性和拓扑传递性表明混沌具有随机性的特征,周期点集稠密则表明了系统具有规律性的特征。

已有的研究结果表明,在一定条件下,初值敏感性可由其他两条性质推导出来[15],还有研究者对周期点的稠密性是混沌的本质属性这一点表示怀疑。为此,Wiggins 对 Devaney 定义进行了如下修改:

定义 1.2[16]　紧集 S 上一变换 f 是混沌的当且仅当:

(1)f 对初值有敏感性;

(2)f 有拓扑传递性。

显然,Wiggins 定义比 Devaney 定义映射条件要弱些,由 Devaney 混沌定义可推出 Wiggins 混沌定义,反之,则不成立。Martelli 等人通过一个反例说明,在 Wiggins 意义下混沌映射并不一定是 Devaney 意义下的混沌[17]。

已有研究结果表明,一般情况下,Devaney 意义下混沌不能推出 Li－Yorke 意义下的混沌,但在某些条件下,Devaney 和 Wiggins 意义下混沌可推出 Li－Yorke 意义下的混沌[18]。

要想理解为什么简单的确定性系统会导致系统的长期行为对初值具有敏感依赖性,关键要理解混沌的几何特性,即系统内在的非线性作用在系统演化过程中形成的“拉伸”与“折叠”变换。美国拓扑学家 Smale 对此作出了重要贡献。