Theory and Applications of Chaotic Cryptography

廖晓峰 肖 迪
陈 勇 向 涛 著

混沌密码学
原理及其应用

科学出版社
www.sciencep.com

混沌密码学原理及其应用

廖晓峰　肖　迪　陈　勇　向　涛　著

科学出版社

北京

内 容 简 介

混沌密码学是非线性科学与密码学交叉融合的一门新的科学。本书取材新颖，概念清晰，书中不仅介绍了数字混沌学所涉及的基础理论和各种代表性的算法，同时也涵盖了混沌密码学的最新研究成果，以及本学科最新的发展方向。本书全面而详细地介绍了混沌密码学的理论和相关算法。全书共分为6章，包括混沌理论与密码学基础、基于混沌的分组密码、基于混沌的流密码、混沌公钥密码技术、混沌 Hash 函数、混沌密码学的安全应用等内容。

本书可供高等院校数学、计算机、通信、信息安全等专业本科生、研究生、教师和科研人员参考。

图书在版编目(CIP)数据

混沌密码学原理及其应用/廖晓峰等著. —北京：科学出版社，2009
ISBN 978-7-03-024677-6

Ⅰ.混… Ⅱ.廖… Ⅲ.密码术 Ⅳ.TN918.1

中国版本图书馆 CIP 数据核字(2009)第 089005 号

责任编辑：鞠丽娜/责任校对：柏连海
责任印制：吕春珉/封面设计·三函设计

科 学 出 版 社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

双 青 印 刷 厂 印刷

科学出版社发行 各地新华书店经销

*

2009 年 7 月第 一 版 开本：B5(720×1000)
2009 年 7 月第一次印刷 印张：18
印数：1—2 000 字数：359 000

定价：46.00 元

(如有印装质量问题，我社负责调换(双青))
销售部电话 010-62134988 编辑部电话 010-62138978-8002

前　言

1999年10月，我受香港城市大学电子工程系黄国和（K. W. Wong）博士的邀请到香港做为期一年的合作研究。当时我的主要工作集中于时滞神经网络的分岔与混沌现象的研究，还未涉及混沌应用于信息安全领域。但是黄国和博士每周都与他的博士生和硕士生们讨论混沌密码方面的学术问题，由此引起了我对此领域的兴趣。但由于我的工作重心并不在此，加之时间紧迫，也未参加他们的“混沌密码”研究小组的讨论。当时我就打算回到重庆大学后带一批博士生和硕士生从事“混沌密码学”的研究。在我的第一批博士中肖迪（本书的作者之一）和邓绍江是最先从事“混沌密码学”研究的，第二批博士中陈勇（本书的作者之一）和张林华也从事“混沌密码学”的研究。我陆续培养了十余名从事这方面研究工作的博士。我们从2000年9月开始举办的“混沌密码学”讨论班，一直持续到现在，同时我也先后派出了一些博士生到黄国和博士那里进行合作研究，他们分别是向涛（本书的作者之一）、周庆、王永、杨华千和韦鹏程。

随着计算机和网络技术的日益普及，信息安全已成为学术界和企业界所共同关注的研究热点和关键问题。安全功能的复杂性以及攻击手段的层出不穷，迫切需要研究和开发出更多安全、高效、可靠的信息安全技术。学术界正在探讨将一些非传统的新颖方法引入信息安全领域。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课题之一。比如我国的《国家中长期科学和技术发展纲要（2006—2020）》在支持的重点领域及其优先主题“核心数学及其在交叉领域的应用”的主要研究方向就包括“离散问题、随机问题、量子问题以及大量非线性问题中的数学理论和方法等”。我国国家自然科学基金在2003年的重大研究项目“网络与信息安全研究计划”中也将“复杂性理论在信息安全中的应用及密码算法分析研究”列入了计划。

混沌和密码学之间具有天然的联系和结构上的某种相似性，启示着人们把混沌应用于密码学领域。混沌的轨道混合特性（与轨道发散和初始值敏感性直接相联系）对应于传统加密系统的扩散特性；而混沌信号的类随机特性和对系统参数的敏感性对应于传统加密系统的混乱特性。可见，混沌所具有的优异混合特性保证了混沌加密器的扩散和混乱作用可以和传统加密算法一样好。另外，很多混沌系统与密码学常用的Feistel网络结构是非常相似的。通过类比研究混沌理论与密码学，可以彼此借鉴各自的研究成果，促进共同的发展。

自从1989年第一篇关于“混沌密码”的论文发表以后，混沌密码已得到了

学术界的广泛关注。自此以来的近 20 年的时间已涌现出数目众多的混沌密码学的研究成果，其中还出现了几篇关于混沌密码的综述性文章。然而，目前在国内外还没有一部系统介绍混沌密码学的专著。

本书全面而详细地介绍了混沌密码学的理论和相关算法。全书共分为 6 章，包括混沌理论与密码学基础、基于混沌的分组密码、基于混沌的流密码、混沌公钥密码技术、混沌 Hash 函数和数字混沌密码学的安全应用等内容。通过对国内外大量文献资料进行了精心筛选和重新组织后，本书有相当一部分成果是取自作者及其所带领的“混沌密码学”讨论班成员和所指导的博士研究生、硕士研究生的研究成果。

第 1 章主要对混沌理论的基础和混沌密码进行了介绍。首先简要介绍了混沌的定义和混沌运动的特征；接着收集并归纳总结了混沌研究所需要的判据与准则；然后在介绍密码学基本知识和混沌与密码学关系的基础上，从混沌流密码、混沌分组密码、混沌公钥密码、混沌图像加密、基于混沌公钥的密钥协商和混沌密码学存在的问题及发展前景对混沌密码学的研究现状进行了详细的介绍和总结。

第 2 章对传统的分组密码的工作模式、设计原则和体系结构进行了概述。在此基础之上详细讨论了基于 Feistel 结构的混沌分组密码、基于检索机制的混沌分组密码和基于迭代机制的混沌分组密码。

第 3 章首先简要介绍了流密码的基础知识，并讨论了最新的随机数序列检测标准；然后对当前一些主要基于混沌密码设计的思想进行了讨论，详细介绍和分析了一些具有代表性的基于混沌的流密码算法。

第 4 章在分析传统的公钥密码的基础之上，详细介绍了已有的各种公钥密码算法，如细胞自动机的公钥密码、一种变形的 ElGamal 混沌密码算法、基于分布混沌系统公钥加密和加性混合调制、基于切比雪夫映射的公钥密码算法、基于环面自同构的混沌公钥密码以及多混沌系统的公钥密码算法，同时还分析了已经提出的这些混沌公钥密码算法在计算速度上与传统的公钥密钥尚有一定差距，而其安全性分析还相对较少。

第 5 章首先简要介绍了 Hash 函数的基础知识，然后按照简单混沌映射 Hash 函数构造、复杂或复合混沌映射 Hash 函数构造、混沌神经网络 Hash 函数构造、并行混沌 Hash 函数构造及混沌加密散列组合算法的顺序，对当前一些主要的基于混沌的 Hash 函数构造及函数构造思想进行了讨论，详细介绍和分析了一些具有代表性的基于混沌的 Hash 函数构造算法。

第 6 章首先讨论了空域加密算法、频域加密算法、数字图像置乱算法、图像加密等，讨论了已有混沌图像加密方法，进而也讨论了混沌在数字水印中的应用。当然数字混沌的安全应用还远不止这些，我们这里仅给出图像加密与数字水

印中的应用以做说明。

本书的编写工作得到了国家自然科学基金项目“基于混沌密码学的安全JPEG2000图像编码系统的设计和实现”、“数字混沌技术及其在数字媒体认证中的应用研究”、“混沌密码及其应用于图像保护的关键技术和评测方法研究”，教育部新世纪优秀人才支持计划项目“耦合混沌系统的滞同步与期望同步及其在保密通信中的应用研究”，重庆市自然科学重点基金项目“基于混沌理论的信息安全技术研究”和“数字混沌技术与无线网络环境中数字媒体信息安全研究”，以及重庆市自然科学基金项目“数字混沌在基于图像压缩编码的加密方案中的研究”等的资助，在此表示感谢！

感谢香港城市大学电子工程系黄国和博士多年对我及我的研究小组所给予的大量的支持和帮助！

在本书的完成过程中，我的博士毕业生邓绍江、桑军、唐国坪、张林华、韦军、杨吉云、杨华千、王永、周庆、韦鹏程、胡月等和硕士毕业生陈巧琳、石熙、陈果、米波，王颖学、孙志娟等也做了一些辅助性工作。另外，书中参考了很多国内外专家和同行学者的论文，在此一并向相关作者表示衷心的感谢！

由于作者水平有限，书中不足之处在所难免，敬请读者批评指正。

廖晓峰

2008.12.13

于重庆

目　录

第 1 章　混沌理论与密码学基础

1.1　混沌理论基础

20 世纪下半叶，非线性科学得到了蓬勃发展。其中，对混沌现象的研究占了极大的份额。半个世纪以来，人们对混沌运动的规律及其在自然科学各个领域的表现有了十分丰富的认识[1~8]。一般而言，混沌现象隶属于确定性系统而难以预测（基于其动力学形态对于初始条件的高度灵敏性），隐含于复杂系统但又不可分解（基于其具有稠密轨道的拓扑特征），以及呈现多种“混乱无序却有规则”的图像（如具有稠密的周期点）。

1.1.1　混沌理论的历史回顾

在现实世界中，非线性现象远比线性现象广泛。混沌现象是指在确定性系统中出现的一种貌似无规则、类似随机的现象，是自然界普遍存在的复杂运动形式。人们在日常生活中早已习以为常的种种现象，如钟摆的摆动、山石的滚动、奔腾的小溪、岸边海浪的破碎、股市的涨跌、漂浮的云彩、闪电的路径、血管的微观网络、大气和海洋的异常变化、宇宙中的星团乃至经济的波动和人口的增长……在它们看似杂乱无章的表面现象下却蕴涵着惊人的运动规律[1~3]。最早对混沌进行研究的是法国的庞加莱（H. Poincare）。1913 年，他在研究能否从数学上证明太阳系的稳定性问题时，把动力学系统和拓扑学有机地结合起来，并提出三体问题在一定范围内，其解是随机的。实际上，这是一种保守系统中的混沌。1927 年，丹麦电气工程师 B. Van der Pol 在研究氖灯张弛振荡器的过程中，发现了一种重要的现象并将它解释为“不规则的噪声”，即所谓 B. Van der Pol 噪声[9]。二战期间，英国科学家重复了这一实验并开始提出质疑。后来的研究发现，B. Van der Pol 观察到的不是“噪声”，而是一种混沌现象。1954 年，前苏联概率论大师 A. N. Kolmogorov[10] 在探索概率起源的过程中，提出了 KAM 定理的雏形，为早期明确不仅耗散系统有混沌现象而且保守系统也有混沌现象的理论铺平了道路。1963 年，麻省理工学院的气象学家洛伦兹（E. N. Lorenz）[11] 在研究大气环流模型的过程中，提出“决定论非周期流”的观点，讨论了天气预报的困难和大气湍流现象，给出了著名的洛伦兹方程。这是第一个在耗散系统中由一个确定的方程导出混沌解的实例。从此以后，关于混沌理论的研究正式揭开了序幕。1964 年，法国天文学家 M. Henon 发现[12]，一个自由度为 2 的不可积的

保守的哈密顿系统，当能量渐高时其运动轨道在相空间中的分布越来越无规律，给出了 Henon 映射。1971 年，法国物理学家 D. Ruelle 和荷兰数学家 F. Takens 首次用混沌来解释湍流发生的机理，并为耗散系统引入了“奇怪吸引子”的概念[13]。1975 年，美籍华人学者李天岩（T. Y. Li）和他的导师美国数学家 J. A. Yorke 发表《周期 3 意味着混沌》一文[14]，首次使用“混沌”这个名词，并为后来的学者所接受。1976 年，美国数学生态学家 R. May 在文章《具有极复杂动力学的简单数学模型》中详细描述了 Logistic 映射 $x_{n+1} = \mu x_n(1 - x_n)$ 的混沌行为[15]，并指出生态学中一些非常简单的数学模型，可能具有非常复杂的动力学行为。1978 年，M. J. Feigenbaum 通过对 Logistic 模型的深入研究[16]，发现倍周期分岔的参数值呈几何级数收敛，从而提出了 M. J. Feigenbaum 收敛常数 δ 和标度常数 α，它们是和 π 一样的自然界的普适性常数。但是，M. J. Feigenbaum 的上述突破性进展开始并未立即被接受，其论文直到三年后才公开发表。M. J. Feigenbaum 的卓越贡献在于他看到并指出了普适性，真正地用标度变换进行计算，使混沌学的研究从此进入了蓬勃发展的阶段。进入 20 世纪 80 年代，人们着重研究了系统如何以有序到新的混沌以及混沌的性质和特点，并进入了混沌理论的应用阶段。90 年代以来，随着非线性科学及混沌理论的发展，混沌科学与其他应用学科相互交错、相互渗透、相互促进、综合发展，其在电子学、信息科学、图像处理等领域都有了广泛的应用，混沌密码学就是其中之一[17~19]。

1.1.2 混沌的定义

“混沌”一词最早出现在中国和希腊的神话故事中，本是“杂乱无章、混乱无序”之意。几千年来，混沌的词义在不同的地域文化背景和学科领域有着不同的内涵，混沌的概念也在经历不断的演化。迄今为止，非线性动力学对混沌进行的研究是最为深入的。在非线性动力学中提出了一些可供理论判定的定义和实际测量的标度，尽管它偏重从数学和物理学的角度对混沌下定义，但是却为混沌学的建立和发展打下了一个坚实的基础，给混沌在不同学科间的交流和渗透提供了方便。

由于混沌系统的奇异性和复杂性至今尚未被人们彻底了解，因此至今混沌还没有一个统一的定义。一般认为，混沌就是指确定性系统中出现的一种貌似无规则的、类似随机的现象。对于确定性的非线性系统出现的具有内在随机性的解，就称为混沌解。这种解在短期内可以预测而在长期内却不可预测，因此与确定解和随机解都不同（随机解在短期内也是不可预测的）。混沌不是简单的无序而是没有明显的周期和对称，但却是具有丰富的内部层次的有序结构，是非线性系统中的一种新的存在形式。但是迄今为止，对混沌概念还没有公认的严格的定义。我们认为，对混沌概念的界定应从混沌现象的本质特征入手，从数学和物理两个

层次上考察，才有可能得出正确的完整的结论。目前已有的定义是从不同的侧面反映了混沌运动的性质，虽然定义的方式不同，彼此在逻辑上也不一定等价，但它们在本质上是一致的[1,20,21]。1975 年，李天岩和 J. A. Yorke 给出了混沌的一个数学定义，这也是第一次赋予混沌这个词以严格的科学意义[14]。除此之外，还有几类从几何和拓扑的角度对混沌进行的定义。

1. Li-Yorke 的混沌定义

区间 I 上的连续自映射 $f(x)$，如果满足下列条件，便可确定它有混沌现象。

1) f 的周期点的周期无上界。

2) 闭区间 I 上存在不可数子集 S，满足：

a. $\forall x,y \in S, x \neq y$ 时，$\limsup\limits_{n\to\infty} |f^n(x) - f^n(y)| > 0$；

b. $\forall x,y \in S, \liminf\limits_{n\to\infty} |f^n(x) - f^n(y)| = 0$；

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

2. Melnikov 的混沌定义

如果存在稳定流形和不稳定流形且这两种流形横截相交，则必存在混沌。

3. Devaney 的混沌定义

在拓扑意义下，混沌定义为：设 V 是一度量空间，映射 $f: V \to V$，如果满足下面 3 个条件，则称 f 在 V 上是混沌的。

1) 对初值的敏感依赖性：存在 $\delta > 0$，对于任意的 $\varepsilon > 0$ 和任意 $x \in V$，在 x 的 ε 邻域内存在 y 和自然数 n，使得 $d(f^n(x), f^n(y)) > \delta$。

2) 拓扑传递性：对于 V 上的任意一对开集 $Z, Y \in V$，存在 $k > 0$，使 $f^k(Z) \cap Y \neq \varnothing$。

3) f 的周期点集在 V 中稠密。

从稳定性角度考虑，混沌轨道是局部不稳定的，“敏感初条件”就是对混沌轨道的这种不稳定性的描述。对于初值的敏感依赖性，意味着无论 x,y 离得多么近，在 f 的作用下，两者的轨道都可能分开较大的距离，而且在每个点 x 附近都可以找到离它很近而在 f 的作用下最终分道扬镳的点 y。对这样的 f，如果用计算机计算它的轨道，任何微小的初始误差，经过若干次迭代以后都将导致计算结果的失效。

拓扑传递性意味着任一点的邻域在 f 的作用之下将“遍历”整个度量空间 V，这说明 f 不可能细分或不能分解为两个在 f 下不相互影响的子系统。

上述两条一般说来是随机系统的特征，但第三条——周期点集的稠密性，却

又表明系统具有很强的确定性和规律性，绝非一片混乱，而是形似紊乱实则有序，这也正是混沌能够和其他应用学科相结合走向实际应用的前提。

1.1.3 混沌运动的特征

混沌运动具有通常确定性运动所没有的本质特征，其体现在几何和统计方面有：局部不稳定而整体稳定、无限相似、连续的功率谱、奇怪吸引子、分维、正的 Lyapunov 指数、正的测度熵等。为了与其他复杂现象区别，一般认为混沌应具有以下几个方面的特征，且它们之间有着密不可分的内在联系[1,2,5]。

1）遍历性：混沌运动轨道局限于一个确定的区域——混沌吸引域，混沌轨道经过混沌区域内每一个状态点。

2）整体稳定局部不稳定：混沌态与有序态的不同之处在于，它不仅具有整体稳定性，还具有局部不稳定性。稳定性是指系统受到微小的扰动后系统保持原来状态的属性和能力，一个系统的存在是以结构与性能的相对稳定为前提的。但是，一个系统要演化，要达到一个新的演化状态又不能稳定性绝对化，而应在整体稳定的前提下允许局部不稳定，这种局部不稳定或失稳正是演化的基础。在混沌运动中这一点表现得十分明显。所谓的局部不稳定是指系统运动的某些方面（如某些维度、熵）的行为强烈地依赖于初始条件。

3）对初始条件的敏感依赖性：关于这一点，洛伦兹在一次演讲中生动地指出：一只蝴蝶在巴西扇动翅膀，就有可能在美国的得克萨斯州引起一场风暴。这句话具有深刻的科学内涵和迷人的哲学魅力，它形象地反映了混沌运动的一个重要特征：系统的长期（“长期”的具体含义对不同系统而言可能有较大差别）行为对初始条件的敏感依赖性。初始条件的任何微小变化，经过混沌系统的不断放大，都有可能对其未来的状态造成极其巨大的差别。正所谓“失之毫厘，差以千里”。所以，人们常用“蝴蝶效应”来指代混沌系统对初始条件的敏感依赖特性。

4）轨道不稳定性及分岔：长时间动力运动的类型在某个参数或某组参数发生变化时也发生变化。这个参数值（或这组参数值）称为分岔点，在分岔点处参数的微小变化会产生不同定性性质的动力学特性，所以系统在分岔点处是结构不稳定的。

5）长期不可预测性：由于混沌系统所具有的轨道的不稳定性和对初始条件的敏感性的特征，因此不可能长期预测将来某一时刻的动力学特性。

6）分形结构：耗散系统的有效体积在演化过程中将不断收缩至有限分维内，耗散是一种整体稳定性因素，而轨道又是不稳定的，这就使它在相空间的形状发生拉伸、扭曲和折叠，形成精细的无穷嵌套的自相似结构。“自相似性”就是说每个局部都是整体的一个缩影，即使取无穷小的部分，还是和整体相似。分维则打破了体系的维数只能取整数的观念，认为体系的维数也可以取分数。混沌状态

表现为无限层次的自相似结构。

7）普适性：在混沌的转变中出现某种标度不变性，代替通常的空间或时间周期性。所谓普适性，是指在趋向混沌时所表现出来的共同特性，它不依具体的系数以及系统的运动方程而变。普适有两种，即结构的普适性和测度的普适性。前者是指趋向混沌的过程中轨线的分岔情况与定量特性不依赖于该过程的具体内容，而只与它的数学结构有关；后者指同一映像或迭代在不同测度层次之间嵌套结构相同，结构的形态只依赖于非线性函数展开的幂次。

1.1.4　混沌研究的判据与准则

混沌来自于系统的非线性性质，但是非线性只是产生混沌的必要条件而非充分条件。如何判断给定的一个系统是否具有混沌运动，以及如何用数学语言来说明混沌运动并对它进行定量刻画，是混沌学所研究的重要课题。目前，多采用数值实验来识别动力系统是否存在混沌运动，然后再通过工程实验加以验证。本节归纳并阐述从定量角度刻画混沌运动特征的一些判据与准则[1~7]。

1. Lyapunov 指数

Lyapunov 指数 λ 可以表征系统运动的特征，它沿某一方向取值的正负和大小，表示长时间系统在吸引子中相邻轨道沿该方向平均发散（$\lambda_i > 0$）或收敛（$\lambda_i < 0$）的快慢程度。因此，最大 Lyapunov 指数 λ_{max} 决定轨道覆盖整个吸引子的快慢，最小 Lyapunov 指数 λ_{min} 则决定轨道收敛的快慢，而所有 Lyapunov 指数 λ 之和 $\sum\lambda_i$ 可以认为是大体上表征轨道平均发散的快慢。任何吸引子必定有一个 Lyapunov 指数 λ 是负的；而对于混沌，必定有一个 Lyapunov 指数 λ 是正的。因此，人们只要在计算中得知吸引子中有一个正的 Lyapunov 指数，即使不知道它的具体大小，也可以马上判定它是奇怪吸引子，而运动是混沌的。

对于混沌动力系统，λ 的大小与系统的混沌程度有关，假设系统从相空间中某半径足够小的超球开始演变，则第 i 个 Lyapunov 指数定义为

$$\lambda_i = \lim_{t\to\infty}\ln(r_i(t)/r_i(0)) \tag{1.1}$$

式中，$r_i(t)$ 为 t 时刻按长度排在第 i 位的椭圆轴的长度；$r_i(0)$ 为初始球的半径，换言之，在平均的意义下，随时间的演变，小球的半径会作出如下的改变：

$$r(t) \propto r_i(0)e^{\lambda_i t} \tag{1.2}$$

下面具体介绍一维混沌系统、差分方程组和微分方程组计算 Lyapunov 指数的方法。

（1）一维混沌系统计算 Lyapunov 指数

考虑一维映射 $x_{n+1} = F(x_n)$。假设 x_n 有偏差 $\mathrm{d}x_n$，并导致 x_{n+1} 偏差 $\mathrm{d}x_{n+1}$，则

$x_{n+1}+\mathrm{d}x_{n+1}=F(x_n+\mathrm{d}x_n)\approx F(x_n)+\mathrm{d}x_nF'(x_n)$，即 $\mathrm{d}x_{n+1}=\mathrm{d}x_nF'(x_n)$

设轨道按指数规律分离，即

$$|\mathrm{d}x_{n+1}|=|\mathrm{d}x_n|\mathrm{e}^{\lambda} \tag{1.3}$$

式中，λ 为 Lyapunov 指数。

为了得到稳定的值，通常要取足够的迭代次数，即

$$\mathrm{d}x_n=\mathrm{d}x_{n-1}F'(x_{n-1})=\mathrm{d}x_{n-2}F'(x_{n-2})F'(x_{n-1})=\cdots=\mathrm{d}x_0\prod_{i=0}^{n-1}F'(x_i)$$

因此

$$\lambda=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln|F'(x_i)| \tag{1.4}$$

(2) 差分方程组计算 Lyapunov 指数

设 R^n 空间上的差分方程 $x_{i+1}=f(x_i)$，f 为 R^n 上的连续可微映射。设 $f'(x)$ 表示 f 的 Jacobi 矩阵，即

$$f'(x)=\frac{\partial f}{\partial x}=\begin{bmatrix}\dfrac{\partial f_1}{\partial x_1}, & \cdots, & \dfrac{\partial f_1}{\partial x_n}\\ \vdots & & \vdots\\ \dfrac{\partial f_n}{\partial x_1}, & \cdots, & \dfrac{\partial f_n}{\partial x_n}\end{bmatrix}$$

令

$$J_i=f'(x_0)f'(x_1)\cdots f'(x_{i-1}) \tag{1.5}$$

将 J_i 的 n 个复特征根取模后，依从大到小的顺序排列为

$$|\lambda_1^{(i)}|\geqslant|\lambda_2^{(i)}|\geqslant\cdots\geqslant|\lambda_n^{(i)}|$$

那么，f 的 Lyapunov 指数定义为

$$\lambda_k=\lim_{i\to\infty}\frac{1}{i}\ln|\lambda_k^{(i)}|,\quad k=1,\cdots,n \tag{1.6}$$

该定义是计算差分方程组的最大 Lyapunov 指数 λ_1 的理论基础，本书的二维映射都是采用这种方法来计算最大 Lyapunov 指数 λ_1 的。

(3) 微分方程组计算最大的 Lyapunov 指数

设在由给定微分方程组所确定的相空间中，选取两条相轨迹起点差距为 d_0，经过时间 τ 后，呈指数分离，差距为 d_t，即

$$d_\tau=d_0\mathrm{e}^{\tau\lambda} \tag{1.7}$$

则

$$\lambda=\frac{1}{\tau}\ln\frac{d_\tau}{d_0} \tag{1.8}$$

定义为 Lyapunov 指数。

数值计算时，从一条参考轨迹上找一个起点，计算出相邻相轨的 d_0、d_τ，若