课程报告

混沌密码学

by 1901210540 谢成淋
1901210620 陈夏润
1901210420 李成扬

目录

0. 背景及研究现状

混沌是客观存在于自然界中的一种不规则的、有界的奇异运动形态。是一种具备确定性但又表现出随机特性的非线性动力系统，从某种意义上来看，混沌理论是继量子力学和相对论之后，20 世纪人类在物理学上的又一项重大发现。

迄今为止，各类不同的混沌加密算法陆续提出。

- 基于混沌的序列密码（流密码）：
  直接用混沌伪随机实值序列作为密钥流去加密明文信息。
- 基于混沌的分组密码：
  混沌应用于分组密码中研究较多的是使用混沌系统设计分组密码中的S盒。
- 基于混沌的公开密钥密码：
  利用混沌理论与公钥密码相结合的思想，提出常规密码系统和混沌密码系统相结合的系统方法，提高整个加密算法的抗攻击能力。

1. 混沌是什么

混沌 是 什么

在不同的应用场景下，混沌的定义不同，其一直以来并没有一个明确的定义

1. 混沌是什么

Li-Yorke 定义：设 F 在区间 J 上，$F:J\to J$，若 F 在区间 J 上有 3 周期点，则对于每一个正整数 k，在 J 中有 F 的周期 k 的周期点。

设有一个不包括周期点的不可数集合 $S\subset J$ 且符合下面三个条件，则认为它是混沌的：

1）对集合 S 中有两个不相等的点 p,q 满足

$$\limsup_{n\to\infty}|F^n(p)-F^n(q)|>0$$

?

混沌 是 什么

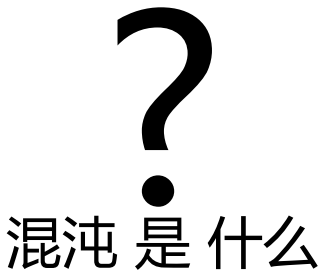
2）对集合 S 中任意两点 p,q 满足

$$\liminf_{n\to\infty}|F^n(p)-F^n(q)|=0$$

3）对任意 $p\in S$ 的和周期点 $q\in J$ 满足

$$\limsup_{n\to\infty}|F^n(p)-F^n(q)|>0$$

1. 混沌是什么



另一个定义是 **Devaney** 提出，其描述如下。

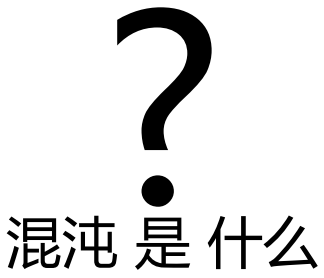
在集合中V，如果映射$f:V \to V$具备下面的前提就称该映射是混沌的：

1）f有对初始条件的敏感依赖性；

2）f是拓扑传递的；

3）状态点在集合V中是稠密的。

1. 混沌是什么



混沌系统本质特征：

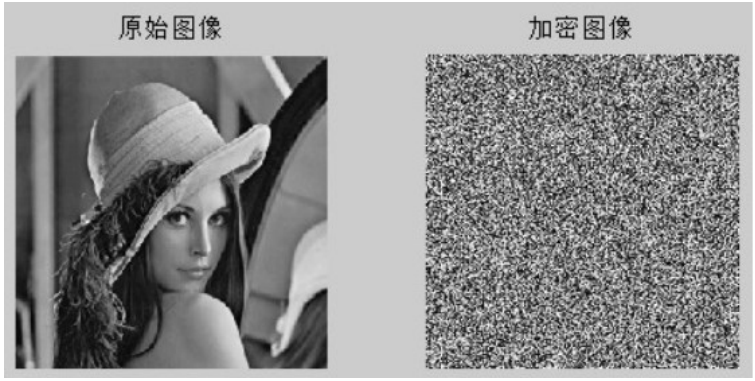
（1）有界

（2）非周期

（3）敏感初条件

2. 混沌实现一瞥

Logistic混沌算法



2. 混沌实现一瞥

Logistic 映射

- 虫口问题
- logistic 映射方程
- 初始密钥

假设有一种昆虫，每年夏季成虫产卵后全部死亡，第二年春天每个虫卵孵化为一个成虫。设第 n 年的虫子数目为x_n，每只成虫平均产卵 a 个。这样的过程年复一年的重复下去，一般规律可以写成 $x_{n+1} = ax_n$，进一步推导可得：

$$x_{n+1} = a^n x_0$$

，其中 x_0 是起始年度的虫子数量

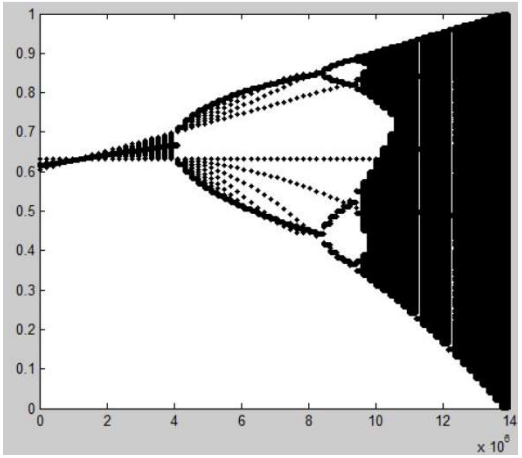
但考虑到种群数量上升后的内部竞争和资源的有限性，一定会存在对于种群数量的负相关的作用。因为 x_n 只虫子配对的事件总数是 $\frac{1}{2}x_n(x_n-1)$。当$x_n >> 1$ 时，基本上是 x_n的平方。因而虫口模型可以用公式表达为：

$$x_{n+1} = ax_n - bx_n^2$$

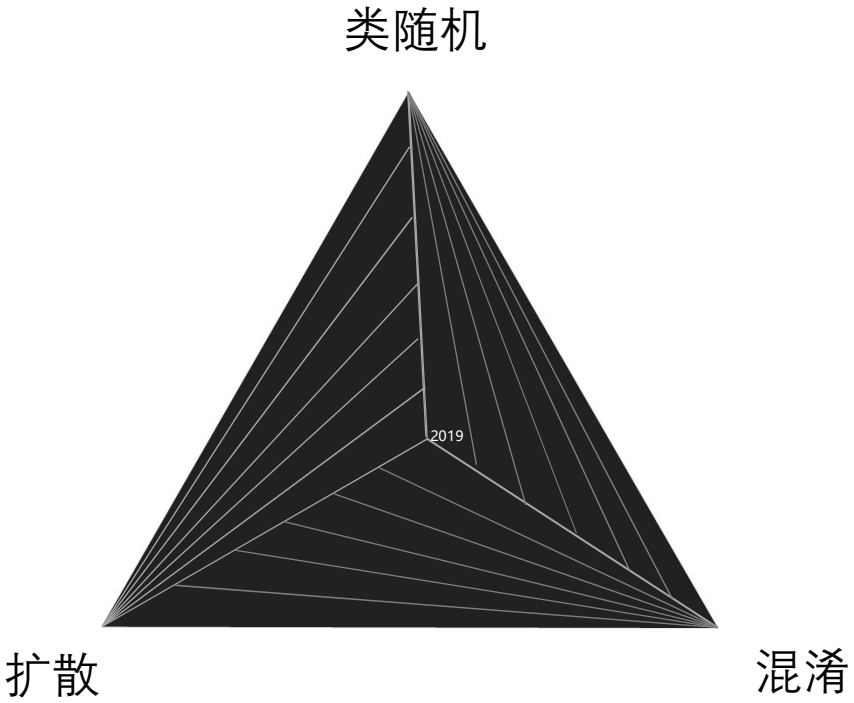
进一步简化，

1. 设环境能承受的最大虫口数为 M，第 n 代虫口数为 n，我们用x_n表示第 n 代相对虫口数，于是有 x_n=n/M，相对虫口数不会大于 1，即 $x_n \in [0, 1]$
2. 令 a＝b＝ μ，为了满足x_n 的取值要求， μ ∈（0，4）
3. 可得公式为：

$$x_{n+1} = ux_n(1-x_n), \quad x_n \in [0, 1], \quad \mu \in (0, 4)$$



3. 混沌和密码的相遇



3.混沌和密码的相遇

1. 对图像数据来说，相邻像素之间存在强相关性。
2. 可以使用多维超混沌系统提供伪随机混沌序列，结合普通图像用分组密码来计算其初始值用于代替或置换，或者基于流密码体系，利用混沌序列作为密钥进行加密。

一、流密码使用方法:

1. 生成序列流
2. 异或加密
3. 异或解密

二、分组密码使用方法:

引入代替或置换过程

3.混沌和密码的相遇

conclusion

1. 混沌是什么
2. 混沌实现一瞥
3. 混沌和密码的相遇

推荐资料

(1).Kocarev L. Chaos-based cryptography: a brief overview[J]. IEEE Circuits and Systems Magazine, 2001, 1(3): 6-21.
(2).混沌密码算法及相关进展


Thanks