**2024年春密码学导论大作业作品题报告**

作品题目： 混沌置乱的循环阶分析

学号： PB22071430

姓名：刘雨田

2024年 6 月 6 日

|  |
| --- |
| 基本信息表 |
| 作品题目：混沌置乱的循环阶分析 |
| 作品内容摘要：  本作品旨在研究和分析基于混沌映射构造的置乱表的循环特性。我们选取了三种不同类型的混沌映射：Logistic映射、ICMIC映射和Tent映射，作为研究对象。通过设定参数和初始值，迭代生成混沌序列，并基于这些序列构造置乱表。具体步骤如下：   1. 选择混沌映射，并设定适当的参数和初始值。 2. 迭代生成混沌序列，取前1000个迭代结果作为舍去项，继续迭代生成所需长度(10-110)的混沌序列。 3. 将生成的混沌序列排序，以排序后的索引构造置乱表。 4. 评估生成的置乱表的循环情况，包括循环圈长度的种类、每种长度的循环圈数量、总的循环长度（阶）等。 5. 使用不同的初始值（种子）生成多个置乱表，并计算平均的阶，绘制“平均阶-N”的曲线，分析其安全性。   通过这些步骤，我们对三种混沌映射生成的置乱表进行详细分析，比较不同映射在生成置乱表时的性能和安全性。最终，评估不同混沌映射在实际应用中的优劣，为基于混沌映射的置乱方法提供理论支持和实践参考。 |
| 关键词（五个）：  混沌映射、置乱、循环群、阶、安全性 |

# 1.作品功能与性能说明

通过分析所得置乱表的阶以及各个平均循环阶长度种类个数，分析不同混沌函数的混沌置乱安全性。

# 2.设计与实现方案

## 2.1 实现原理

置乱函数（Logistic\_map、ICMIC\_map、Tent\_map）

置换表函数（generate\_permutation\_table）：根据置乱函数生成置乱表

寻阶函数（find\_cycles）：获得置乱表中各个循环群的阶

分析阶函数（analyze\_cycles）：获得置乱表总的阶，以及表内各个阶及其出现个数

评估函数（evaluate\_map）：对给定参数的置乱函数求出其表的平均阶，平均指根据5000个初始种子所得结果的平均，以及。

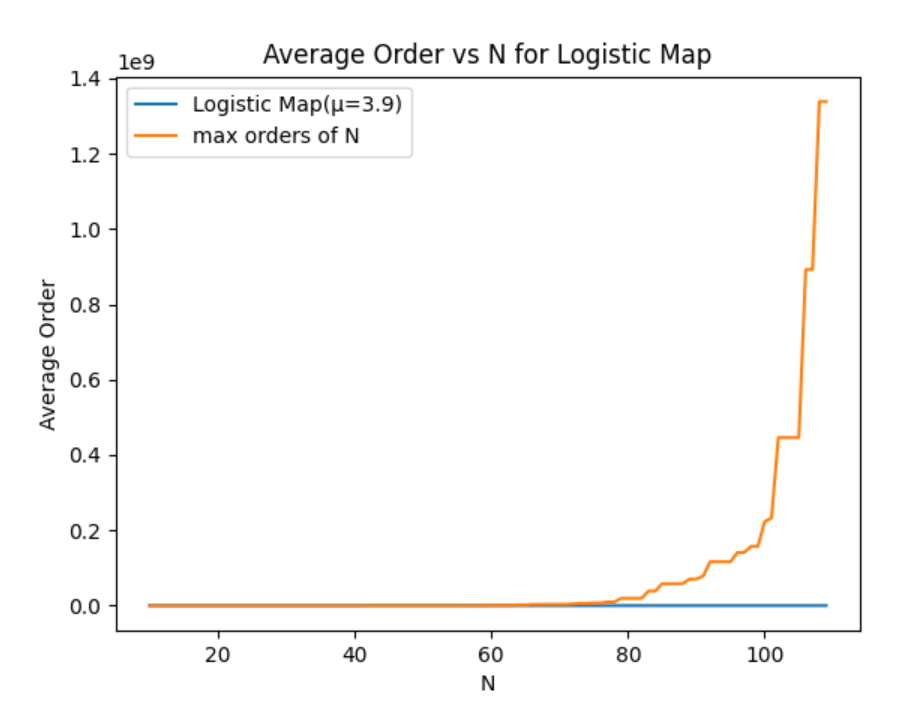
# 3.系统测试与结果

## 3.1测试方案

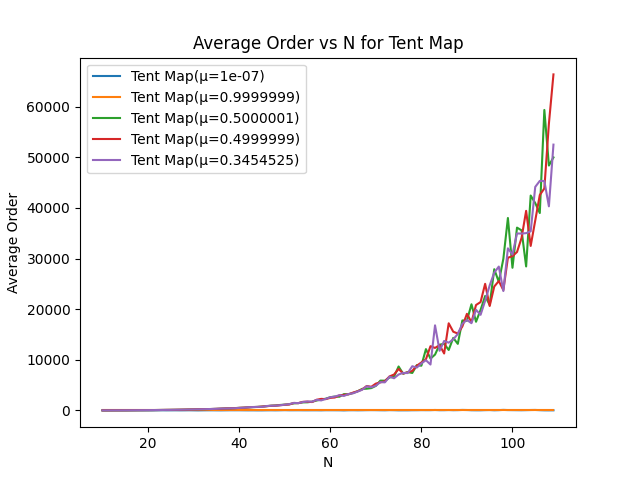
评测各混沌函数各参数的置乱表平均阶-N曲线。

分析平均循环阶长度种类个数-N曲线。

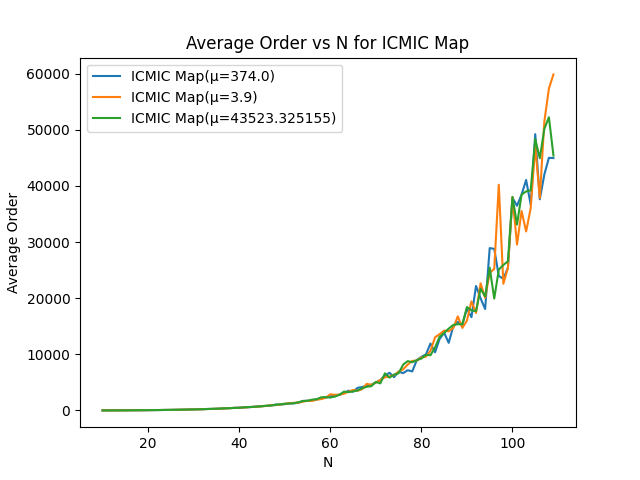
## 3.2 测试数据与结果

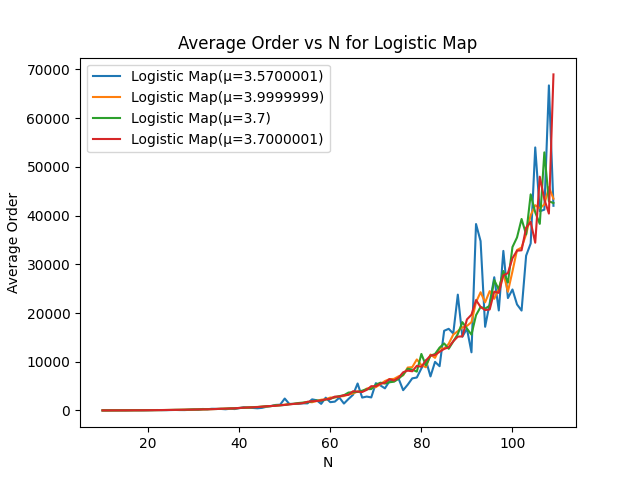


以参数为3.9的Logistic混乱置乱为例，元素个数为N的置乱表的阶与理论上最大的阶相比十分小。实际安全性与理论上的最大安全性相比还有差距。



对Tent置乱，参数范围从0到1，当太靠近边界时，置乱效果很差；当处于中间区域时，置乱效果随参数变化不明显。

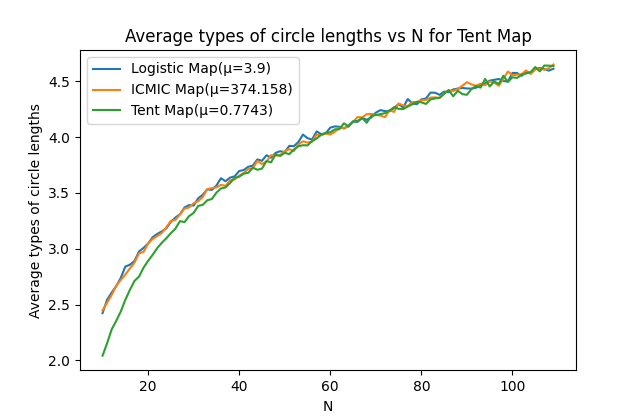


对ICMIC置乱，参数范围为从0到正无穷，乱效果随参数变化不明显。

对Logistic置乱，参数范围为从3.57到4，置乱效果随参数变化不明显。

# 3 map comparision

对三个混沌函数所得置乱表，平均阶相差不大，安全性相当。



对三个混沌函数所得置乱表平均循环阶长度种类个数，N<40时Tent混沌置乱相对较小；其他两个相当N>40时，三个混沌置乱平均循环阶长度种类个数相差不大。

# 5. 结论

各个混沌函数置乱安全性效果相差无几，但与理论上的最大安全性仍有差距。