中国科学技术大学 University of Science and Technology of China | 网络空间安全学院 School of Cyber Science and Technology

作品类别： □软件设计 □硬件制作 □工程实践

# 《密码学导论》课程大作业作品设计报告

作品题目：混沌置乱的循环阶分析

姓名：宋重林

学号：PB22071371

2024 年 6 月 8 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：

针对混沌映射构造置乱的一种常用方法:选定一个混沌映射,参数 μ 和初始值迭代 M 轮,继续迭代计算 N 次,将这 N 个数排序，以每个数的位置为置乱索引，设计了一个评测程序，分析了置乱表的循环情况，循环圈长度，个数，总循环次数。同时选择固定 N 使用不同种子生成多个置乱表，计算平均的阶；绘制“平均阶-N”的曲线；分析其安全性。

关键词（五个）：

混沌置乱,循环阶,置乱,Logistic 映射,安全性

开发人员：

宋重林

# 1.作品功能与性能说明

对常见的混沌映射，使用图像的方法，分析平均阶与 N 的关系，判断安全性。

# 2. 设计与实现方案

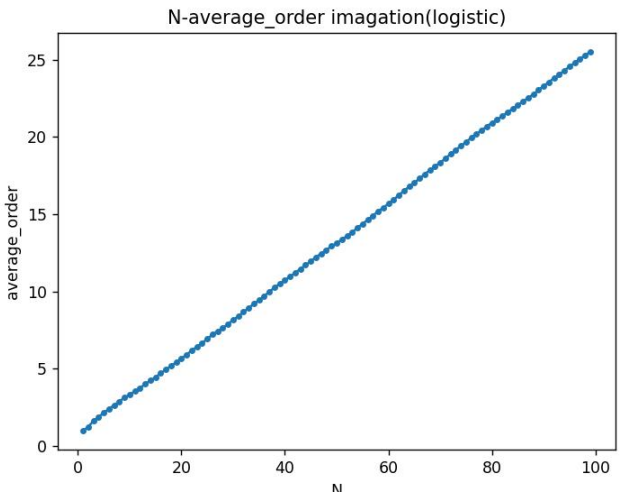
## 2.1 实现原理

先通过混沌映射获得一个置乱表，然后对自然排序表重复置乱，得到所有的循环圈，它们的最小公倍数即为总体的循环圈的阶。
然后对一个具体的混沌映射测评：先设定 N 变化的范围，在设定种子数，对每个 N 的若干次映射得到的平均阶，与 N 本省作为参数作图，绘出曲线，分析安全性。

## 2.2 参考文献

改进策略：21 种混沌映射方法-混沌初始化（附 matlab 代码） 如何使用混沌映射生成初始种群-CSDN 博客

## 2.3 运行结果



以 logistic 映射为例作图。

## 2.4 技术指标

以 logistic 映射为例，取 N 为 0-100，种子数为 100，M 取 1000，运行时间为 6.22s

```
运行时间:6.622412443161011s
```

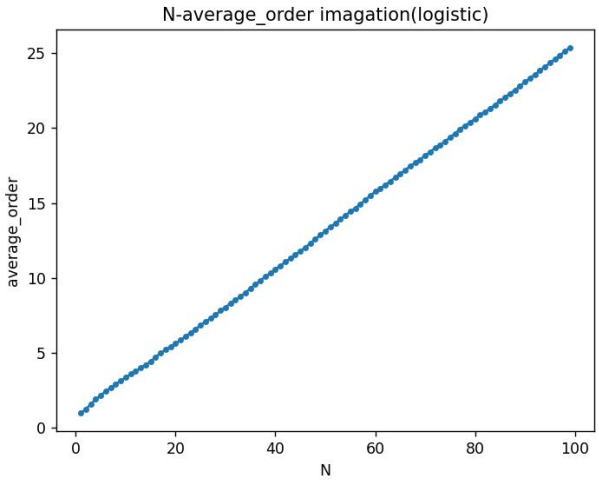
# 3.系统测试与结果

## 3.1 测试方案

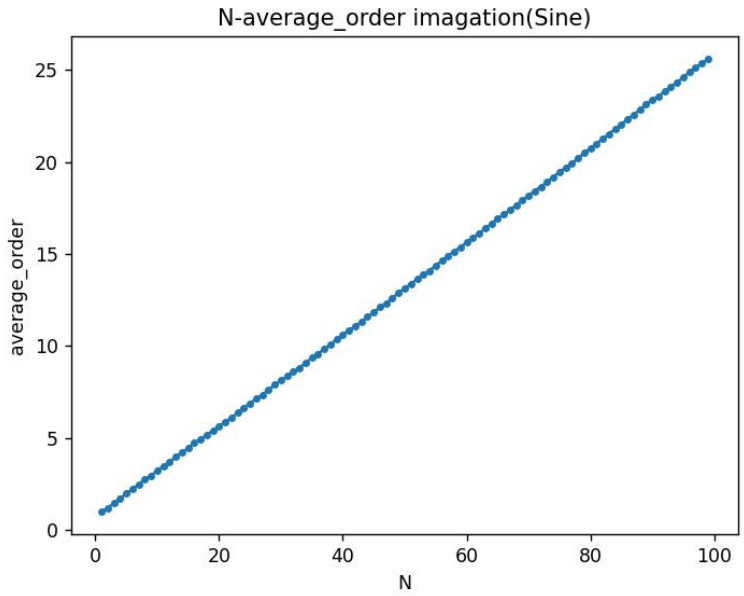
选取 3 个混沌映射：logistic 映射，Sine 映射，Cubic 映射进行测试

## 3.2 功能测试

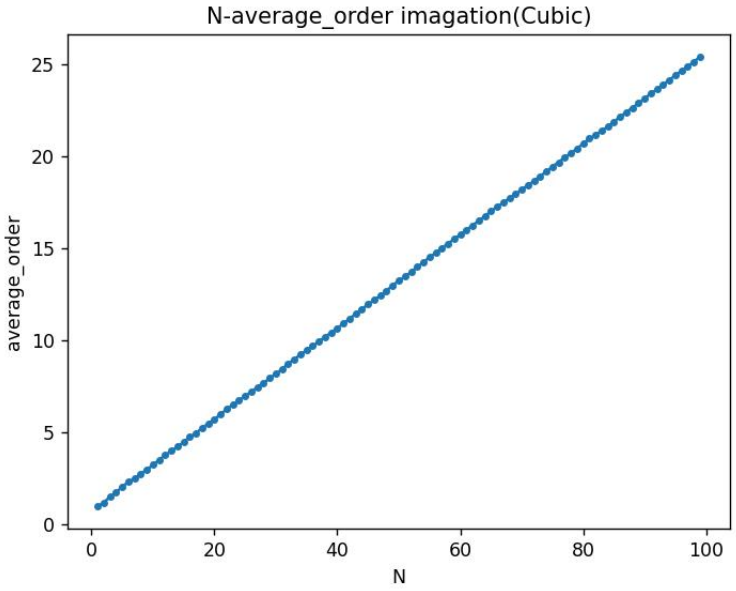
logistic 映射：



Sine 映射：




Cubic 映射：




## 3.3 性能测试

运行时间如下：

```
logistic运行时间:5.554654359817505s,Sine运行时间:6.133698225021362s,Cubic运行时间:5.0347206592559814s,总运行时间:16.72307324409485s
```

## 3.4 测试结果

三个映射混沌性较好，同时运行较快

## 4.应用前景

### 可用于测试各种混沌映射的浑沌性

## 5.结论

通过对混沌置乱的循环阶分析，可以有效地帮助分析混沌映射的混沌性，对常用的 3 个混沌映射检测，可以认定它们的混沌性较大，运算较快。