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：混沌映射置乱的循环阶分析

团队人员：罗俊鹏

2025 年 6 月 7 日

基本信息表

作品题目：混沌映射置乱的循环阶分析

作品内容摘要：

```cpp
CycleAnalysisResult test_cycles(const int* cycletable, int N)
{
    CycleAnalysisResult result;
    result.cycle_counts.resize(N + 1, 0);
    std::vector<bool> visited(N, false);
    result.order = 1;
    for(int i = 0; i < N; i++) {
        if(!visited[i]) {
            int current = i;
            int cycle_length = 0;
            do {
                visited[current] = true;
                cycle_length++;
                for(int j = 0; j < N; j++) {
                    if(cycletable[j] == cycletable[current] && !visited[j]) {
                        current = j;
                        break;
                    }
                }
            } while(current != i && !visited[current]);
            if(cycle_length > 0) {
                result.cycle_counts[cycle_length]++;
                result.order = std::lcm(result.order, cycle_length);
            }
        }
    }
    return result;
```

关键词（五个）：置乱，循环阶，

lojistic 映射，singer 映射，cubic 映射

团队成员（按在作品中的贡献大小排序）：

序号	姓名	学号	任务分工
1	罗俊鹏	PB23331863	所有的工作
2			
3			

1.作品功能与性能说明

作品实现了对三种混沌映射：lojistic 映射，singer 映射，cubic 映射运算后得到的置乱表的置换阶数的统计，并能以折线图的形式展现出三种映射“平均阶-N”的曲线。

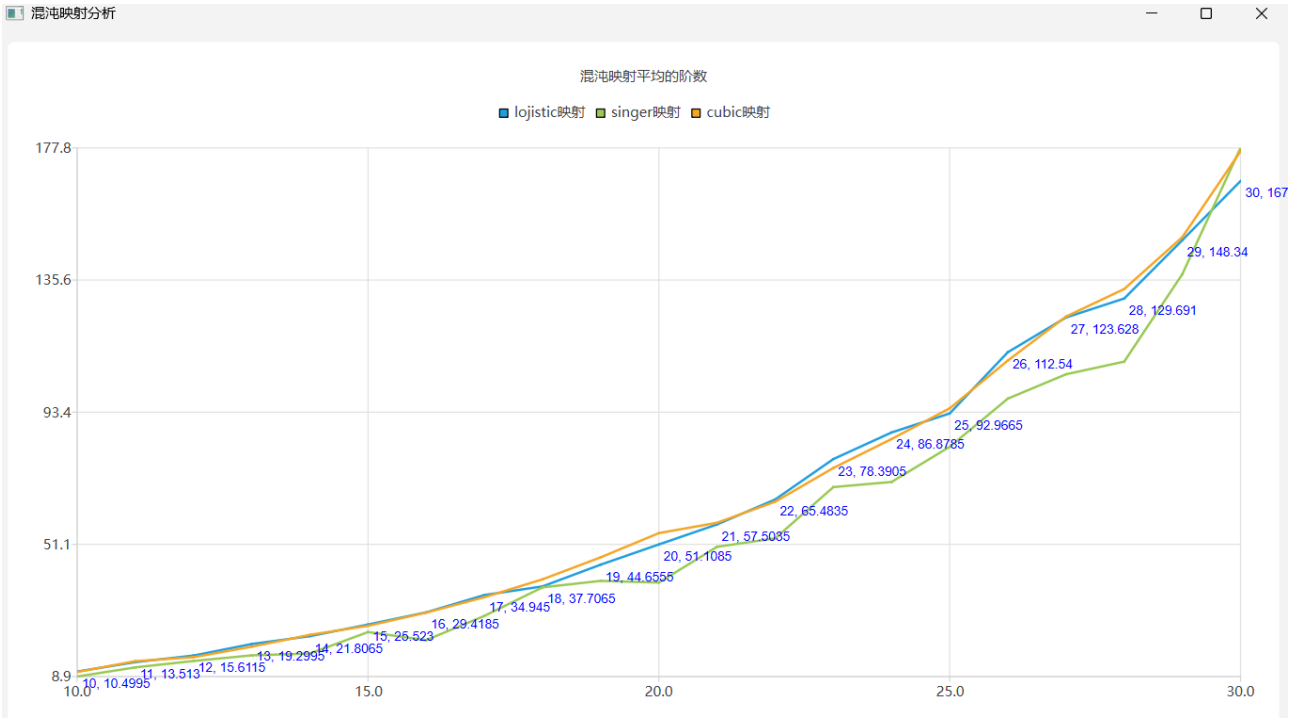
2.设计与实现方案

将置乱表分解为置换的积并计算循环阶，使用随机数生成多个种子计算平均阶

2.1 实现原理

遍历原表，在置乱表中查找当前元素，如果位置不同，则转到元素在置乱表中的位置，并标记，直到再遇到已经标记的元素，并将标记加一。遇到已经标记的元素则转到下一位置。如此便可分解出置换。

2.3 运行结果



2.4 技术指标

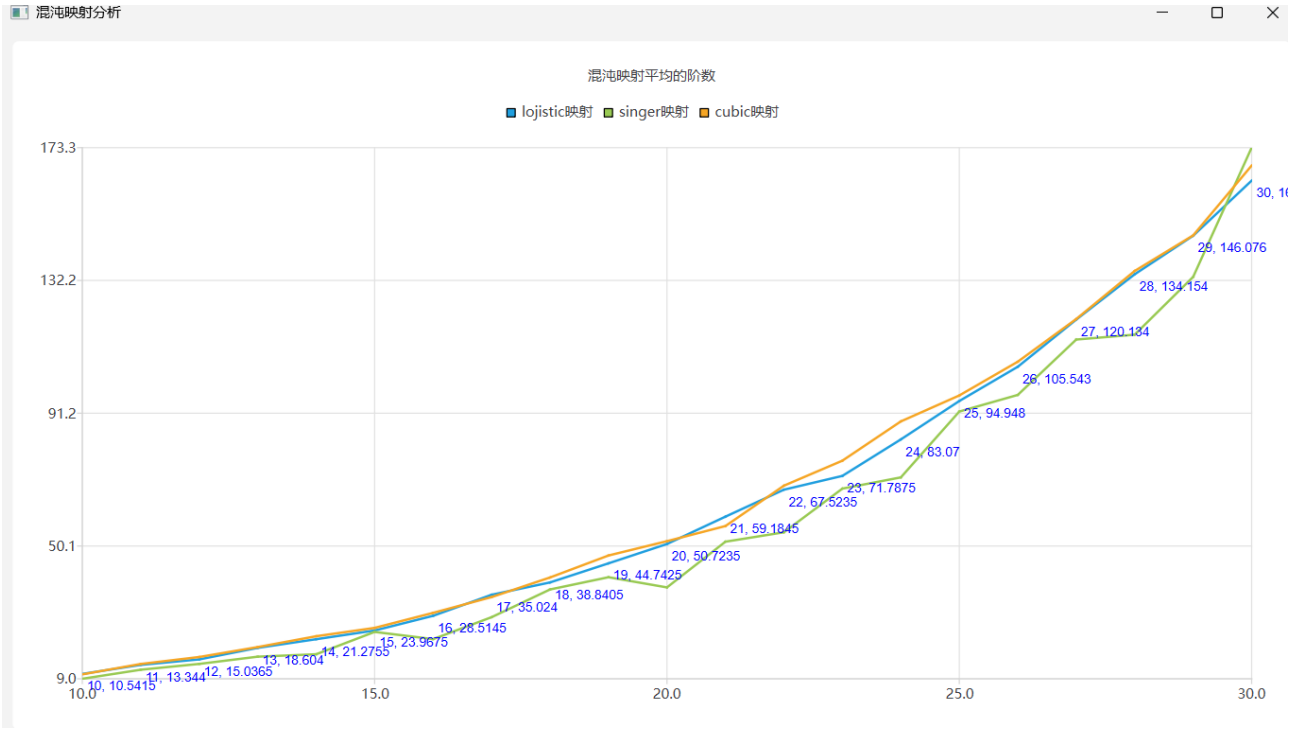
混沌映射的迭代轮数为 1000，置乱表的长度为 10~30，计算平均阶使用的种子为 1000 个

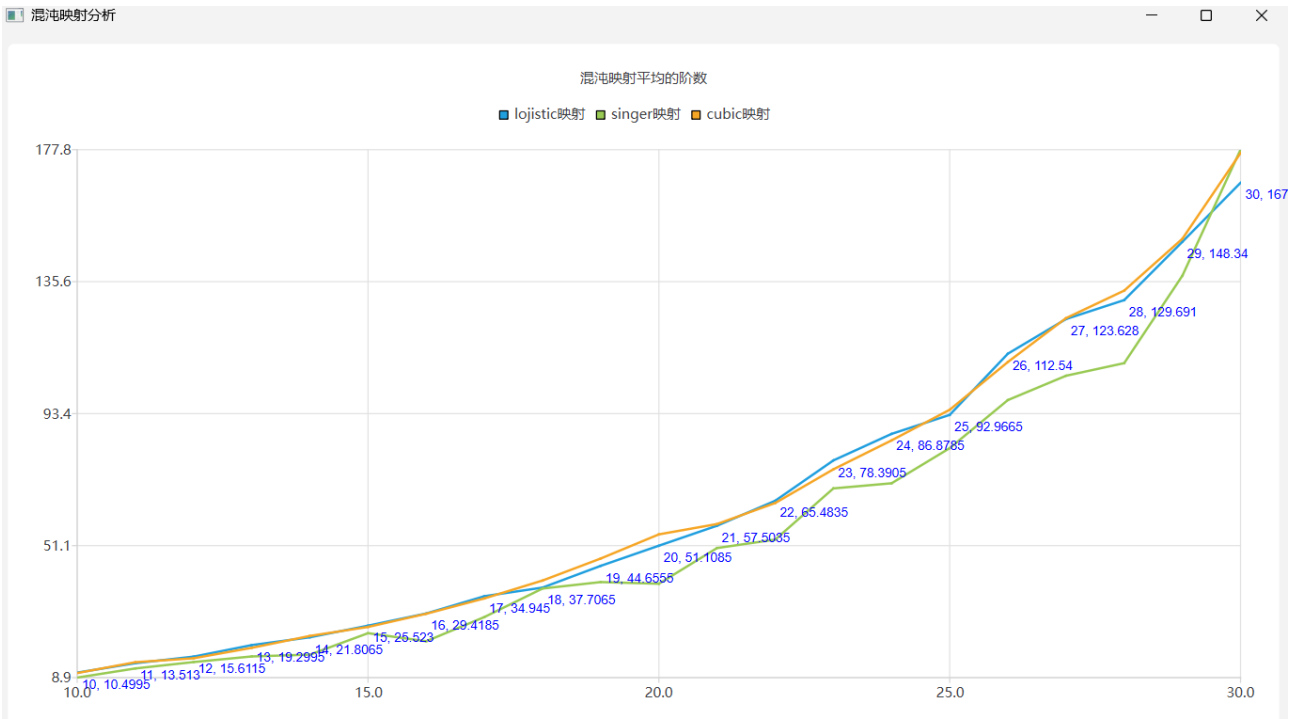
3.系统测试与结果

3.1 测试方案

通过多次测试来检验平均阶是否稳定以及比较映射的性能

3.2 测试数据与结果





平均阶基本稳定且 singer 映射的阶比较小，其他两个相似。

4.结论

混沌映射对初值敏感，且阶数与 N 呈现指数关系。

5.应用前景

无

项目地址： https://github.com/gamonojo/ljp-Crypthomework