南昌大学实验报告

学生姓名：丁俊　　学　　号：8003119100　专业班级：信息安全 193 班
实验类型：☑验证 □ 综合 □ 设计 □ 创新　实验日期：2021.10.2　实验成绩：

一、实验项目名称

编码打印 5 阶 m 序列

二、实验目的

了解一些常用的本原多项式
能根据本原多项式和给定的初始状态求出 m 序列

三、实验基本原理

实验基于线性反馈移位寄存器的一些理论基础，并且应用 c/c++相关技术实验 m 序列的求解

四、实验步骤

1、给定一个本原多项式
2、给定初始状态
3、编码实现

具体实现见代码：

//5 阶 m 序列.cpp

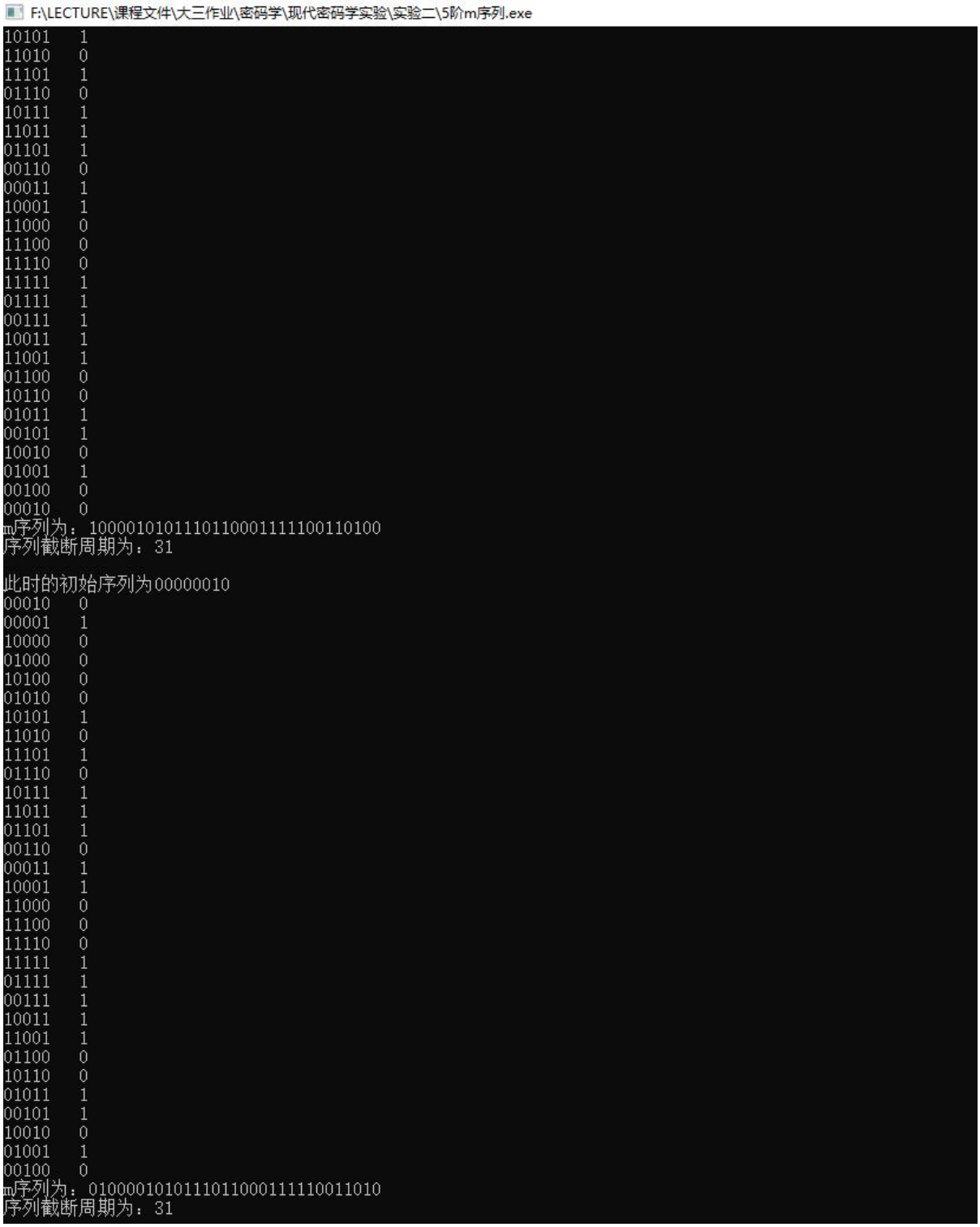
```cpp
#include <set>
#include <bitset>
#include <cmath>
#include <cstdio>
#include <cstring>
#include <iostream>
#include <algorithm>
#include <vector>
using namespace std;

//5 阶 m 序列
//string tar = "10001";
int st;//记录初始值
set<int>vis;//判重
vector<int>v;//存放序列
int s2i(string s) {
    int sum = 0;
    for (int i = 0; i < s.size(); i++) {
```

```
        sum += ((s[s.size() - i - 1] - '0') * pow(2, i));
    }
    return sum;
}

string i2s(int x) {
    string s = "";
    for (int i = 4; i >= 0; i--) {
        s += (x >> i) % 2 + '0';
    }
    return s;
}

void work(int x) {
    do {
        vis.insert(x);
        cout << i2s(x) << "\t" << x % 2 << endl;
        v.push_back(x % 2); //末尾入队
        int yhz = (x % 2) ^ ((x >> 3) % 2); //得到异或值
        x >>= 1;  //状态转移
        x += (yhz * pow(2, 4)); //状态转移
    } while (x != st && vis.count(x) != 1);
}

int main() {
    //1、搜索资料得 5 阶本原多项式 为 :  x^5 + x^2 + 1
    //2、递推关系可得为 :   a(k) = a(k-2) ^ a(k-5), k>5 例如:  a(6) = a(4) ^ a(1)

    for (int i = 1; i <= 31; i++) { //遍历所有 5 位二进制数的状态，发现最后结论都是周期为 31 的 m 序列
        cout << "此时的初始序列为" << bitset<8>(i) << endl;
        vis.clear();
        v.clear();
        //st = s2i(tar);//记录初始状态，用于判断循环终止
        st = i;
        work(st);

        cout << "m 序列为: ";
        for (int i = 0; i < v.size(); i++) {
            cout << v[i];
        }
        puts("");
        cout << "序列截断周期为: " << v.size() << endl;
```

```
        puts("");
    }
    return 0;
}
```

五、实验数据及处理结果

最后实验数据截图如下：




此时的初始序列为00011111
11111 1
01111 1
00111 1
10011 1
11001 1
01100 0
10110 0
01011 1
00101 1
10010 0
01001 1
00100 0
00010 0
00001 1
10000 0
01000 0
10100 0
01010 0
10101 1
11010 0
11101 1
01110 0
10111 1
11011 1
01101 1
00110 0
00011 1
10001 1
11000 0
11100 0
11110 0
m序列为：11111001101001000010101110110000
序列截断周期为：31
无论初始序列为多少，最终的
序列周期都是31，m序列


此时的初始序列为00011110
11110 0
11111 1
01111 1
00111 1
10011 1
11001 1
01100 0
10110 0
01011 1
00101 1
10010 0
01001 1
00100 0
00010 0
00001 1
10000 0
01000 0
10100 0
01010 0
10101 1
11010 0
11101 1
01110 0
10111 1
11011 1
01101 1
00110 0
00011 1
10001 1
11000 0
11100 0
m序列为：01111100110100100001010111011000
序列截断周期为：31
序列周期始终为31

六、思考讨论题或体会或对改进实验的建议

无

七、参考资料

现代密码学教材