

南昌大学实验报告

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

```
1.#include <set>
2.#include <bitset>
3.#include <cmath>
4.#include <cstdio>
5.#include <cstring>
6.#include <iostream>
7.#include <algorithm>
8.#include <vector>
using namespace std;
10.
11. //5 阶 m 序列
12. //string tar = "10001";
13. int st;//记录初始值
14. set<int>vis;//判重
15. vector<int>v;//存放序列
16. int s2i(string s) {
17.
       int sum = 0;
18.
      for (int i = 0; i < s.size(); i++) {</pre>
```

```
19.
           sum += ((s[s.size() - i - 1] - '0') * pow(2, i));
20.
21.
       return sum;
22.}
23.
24. string i2s(int x) {
25.
       string s = "";
       for (int i = 4; i >= 0; i--) {
26.
27.
           s += (x >> i) % 2 + '0';
28.
29.
       return s;
30.}
31.
32. void work(int x) {
       do {
33.
34.
           vis.insert(x);
35.
           cout << i2s(x) << "\t" << x % 2 << endl;</pre>
36.
           v.push back(x % 2); //末尾入队
           int yhz = (x % 2) ^ ((x >> 3) % 2); //得到异或值
37.
38.
           x >>= 1; //状态转移
           x += (yhz * pow(2, 4)); //状态转移
39.
40.
       } while (x != st && vis.count(x) != 1);
41. }
42.
43. 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
45.
   如: a(6) = a(4) ^ a(1)
46.
       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
47.
   是周期为 31 的 m 序列
           cout << "此时的初始序列为" << bitset<8>(i) << endl;
48.
49.
           vis.clear();
50.
           v.clear();
51.
           //st = s2i(tar);//记录初始状态,用于判断循环终止
52.
           st = i;
           work(st);
53.
54.
55.
           cout << "m 序列为: ";
           for (int i = 0; i < v.size(); i++) {</pre>
56.
57.
               cout << v[i];</pre>
58.
59.
           puts("");
           cout << "序列截断周期为: " << v.size() << endl;
60.
```

```
61. puts("");
62. }
63. return 0;
64. }
```

五、实验数据及处理结果

最后实验数据截图如下:

■ F:\LECTURE\课程文件\大三作业\密码学\现代密码学实验\实验二\5阶m序列.exe

```
10101
11010
11101
01110
10111
11011
01101
00110
00011
       00010 0
00010 0
m序列为: 1000010101110110001111100110100
序列截断周期为: 31
此时的初始序列为00000010

00010 0

00001 1

10000 0

01010 0

01010 0

10101 1

11010 0

10111 1

10011 1

11000 0

11111 1

10011 1

11000 0

11111 1

00111 1

10011 1

10011 1

10011 1

10011 1

10111 1

01111 1

01111 1

01111 1

01111 1

01111 1

01111 1

01111 1

01111 1

01111 1

01111 1

01111 1

01111 1

01111 1

01111 1

01111 1

01111 1

01111 1

01111 1

01111 1

01111 1

01111 1

01110 0

01011 1

10010 0

01011 1

00101 1

10010 0

01011 1

00101 1

00101 1

00100  0

0F列为: 0100001010111011000111110011010

F列截断周期为: 31
```

```
此时的初始序列为00011111
111111
011111
001111
10011
11001
01100
10110
01011
00101
10010
01001
00100
00010
00001
10000
01000
10100
01010
10101
11010
11101
01110
10111
11011
01101
01101
00110
00011
10001
10001 1
11000 0
11100 0
11110 0
瓜字列为: 1111100110100100001010111011000
序列截断周期为: 31
```

```
此时的初始序列为00011110
11110 0
11111 1
00111 1
10011 1
11001 1
11001 0
10110 0
10110 0
01011 1
10010 1
10010 0
00001 1
10000 0
10100 0
01010 0
01010 1
11010 0
11101 1
11010 0
11101 1
11010 0
11111 1
11011 1
11011 1
11010 0
10110 0
10110 0
10110 1
11000 1
11000 1
11001 1
11000 1
11000 1
11001 1
11000 1
11000 1
11000 1
11000 1
11000 1
11000 1
11000 1
11000 1
11000 1
11000 1
11000 1
11000 1
11000 1
11000 1
11000 0
11100 0
11100 0
11100 0
11100 0
11100 0
11100 1
```

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