1. 填空题
2. 有无记忆性
3. 2^n -1
4. 101 110 1011101110111...周期为4
5. 设{ai}∈G(p(x)),{ai}为m序列的充 要条件是p(x)为本原多项式
6. 2^5-1 = 31
7. 1和 -1/7（当0<=i<=2^n-2）
8. 2
9. 49 21
10. 2
11. 2^(n-i-2) 1 0
12. 2n
13. 256B
14. 2
16. 选择

4.3. 已知一有限状态自动机的状态转移图如图所示，则当初始状态为*s*1，且输入字符序列为*A*1(1)*A*2(1)*A*1(1)*A*3(1)*A*3(1)*A*1(1)时，输出的状态序列和输出符号序列分别是什么？



解：根据有限状态机转移图有

1. 输出的状态序列 *s*1, *s*2, s2, s3, s2, s1, s2
2. 输出的符号序列 *A*1(2) *A*1(2) *A*2(2)  *A*1(2) *A*3(2) *A*1(2)

5.3 n次不可约多项式*p*(*x*)的周期为*r*，试证*A*(*x*)=1/*p*(*x*)的充要条件是0的n－1游程出现在一个周期的最后n-1bit

证：由于*p*(*x*)是不可约多项式，则由*p*(*x*)生成的非0序列的周期等于*p*(*x*)的周期*r*

由*A*(*x*)＝*a*1+*a*2*x*+…+*arxr*-1+*xr*(*a*1+*a*2*x*+…+*arxr*-1)+(*xr*)2(*a*1+*a*2*x*+…+*arxr*-1)+…

＝*a*1+*a*2*x*+…+*arxr*-1/(1-*xr*)＝*a*1+*a*2*x*+…+*arxr*-1/(*xr*-1)

于是*A*(*x*)=(*a*1+*a*2*x*+…+*arxr*-1)/(*xr*-1)＝1/*p*(*x*)

所以*p*(*x*) (*a*1+*a*2*x*+…+*arxr*-1)= *xr*+1

由于*p*(*x*)的次数为n，所以(*a*1+*a*2*x*+…+*arxr*-1)的最大次数为*r*-1-*n*，也就是说从*xr*-1-*n*+1开始系数都为0

即从*xr*-*n*到*xr*-1共n-1个系数都为0，由0的最大游程长度是n-1，所以0的n-1游程出现在一个周期的最后n-1bit

必要性：

如果0的n-1游程出现在最后n-1bit，我们考察*p*(*x*) (*a*1+*a*2*x*+…+*arxr*-1)＝*φ*(*x*) (*xr*-1)，其中*φ*(*x*)满足*A*(*x*)*p*(*x*)＝*φ*(*x*)，由于*p*(*x*)次数为n，而根据0的n-1游程出现在最后n-1bit 知(*a*1+*a*2*x*+…+*arxr*-1)的最大次数是

*r*-1-(*n*-1)，所以方程左边*p*(*x*) (*a*1+*a*2*x*+…+*arxr*-1)的次数为*n*+ *r*-1-(*n*-1)=r，所以方程右边*φ*(*x*)=1，即*A*(*x*)=1/*p*(*x*) #

6.2 已知一序列的前10比特为**0010001111**

(1) 试用B-M算法求出产生该序列极小多项式和线性复杂度

(2) 给出产生该序列的LFSR的递推式、结构图和周期

(3) 破译该序列最少需要知道多少连续的密钥流比特

解：(1) 产生该序列的极小多项式和线性复杂度分别是1+*x*+*x*4和4

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **n** | **a10** | ***dn*** | ***fn*(*x*)** | ***ln*** | **m** | ***fm*(*x*)** |
| **0** | 0 | 0 | 1 | 0 |  |  |
| **1** | 0 | 0 | 1 | 0 |  |  |
| **2** | 1 | 1 | 1 | 0 | 2 | 1 |
| **3** | 0 | 0 | 1-*d*2*x*2+1=1+*x*3 | 2+1=3 |  |  |
| **4** | 0 | 0 | 1+*x*3 | 3 |  |  |
| **5** | 0 | 1 | 1+*x*3 | 3 |  |  |
| **6** | 1 | 1 | (1+*x*3)+*x*5-2(1)=1 | 3 | 6 | 1 |
| **7** | 1 | 1 | 1+ *x*6-2(1)=1+*x*4 | 4 |  |  |
| **8** | 1 | 0 | 1+*x*4+*x*7-6(1)=1+*x*+*x*4 | 4 |  |  |
| **9** | 1 | 0 | 1+*x*+*x*4 | 4 |  |  |
| **10** |  |  | 1+*x*+*x*4 | 4 |  |  |

(2)结构图、递推式和周期



递推式 *ak*+4=*ak*+3⊕*ak*

周期：由于是本原多项式，所以周期为24-1=15

1. 需要知道至少2x4=8个连续的密钥流比特