## **第5章 序列密码**

**1．3级线性反馈移位寄存器在*c*3=1时可有4种线性反馈函数，设其初始状态为，求各线性反馈函数的输出序列及周期。**

答案：此时线性反馈函数可表示为

当，时，，

输出序列为101101…， 周期=3

当，时，，

输出序列为10111001011100…， 周期=7

当，时，，

输出序列为10100111010011…， 周期=7

**2．设*n*=4，，初始状态为，求此非线性反馈移位寄存器的输出序列及周期。**

答案：由反馈函数和初始状态得状态输出表为

  （回到初始状态）

所以此反馈序列输出为：11011…周期为5

**3．已知某3级反馈移位寄存器的反馈函数为，，求初始状态决定的反馈移位寄存器序列。**

答案：因为，所以，*a*3=*a*0*a*1+*a*2，由初态可得，序列（11011101…），所以。

**4．已知一个4-LFSR的结构常数为，**

**（1）画出此LFSR的结构图；**

**（2）给出反馈函数；**

**（3）分别求对应初始状态（1000）、（0010）和（1111）的序列，这三个序列有何关系？**

答案：（1）



（2）反馈函数

联接多项式

（3）初态（1000）对应的序列是；

初态（0010）对应的序列是；

初态（1111）对应的序列是；

所对应的状态图和全零状态组成了此LFSR决定的状态图。

**5．某5-LFSR的联接多项式为，求此LFSR的结构常数。**

答案：反馈函数为，结构常数 [1，0，1，1，1]。

**6．设二元域GF(2)上的一个LFSR的结构常数为[1101]，初始状态为1101，试求其输出序列及其周期。**

答案：其反馈函数为，初始状态为1101生成的序列为，周期为7。

**7．若周期序列的有理表示为，求序列的周期。**

答案： ，所以由

的系数得出。

**8．设序列是二元域上的一个长度为6的序列，试利用B-M算法求其线性综合解。**

答案：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  | m |  |
| 0 | 1 | 1 | 0 |  |  |
| 1 | 0 | 1+x | 1 |  |  |
| 2 | 0 | 1+x | 1 |  |  |
| 3 | 1 | 1+x | 1 | 0 | 1 |
| 4 | 1 |  | 3 | 0 | 1 |
| 5 | 1 |  | 3 | 3 | 1+x |
| 6 |  |  | 3 |  |  |

线性综合解为：<,3>

**9．（1）若是一个29级M-序列，求=（ ）；**

**（2）若周期序列的有理表示为，求；**

**（3）在25级M序列的一个周期环上，有（ ）个“0”，有（ ）个长为15的“1−游程”。**

答案：（1）；

（2）；

（3）。