应用密码学第四次作业解答

1. 设二元域$GF(2)$上线性移位寄存器的特征多项式为$f(x) = 1 + x + x^3 + x^4$，试画出其所对应的线性移位寄存器图。进一步，假设初始状态为1101，试求其输出序列及其周期，以及生成该序列的最短线性移位寄存器。

解： 输出序列为110 110 110 110 ...，周期为3. (反馈结构图略)

为了求生成该序列的最短移位寄存器，设其极小多项式为$g(x)$，我们知道必有$g(x) \mid f(x)$。容易给出$f(x)$的分解

$$f(x) = (x+1)^2(x^2+x+1) = (x^2+1)(x^2+x+1)$$

（这个分解可以这样得到：$x = 1$显然是$f(x)$的根，所以可以从$f(x)$中去除掉$x-1$这个因子。注意：x^2+x+1是$\mathbb{F}_2$上唯一的二次不可约多项式）
验证发现x^2+x+1能生成上述序列，而$x+1$和$(x+1)^2$都不可以。

2. 假设密码分析者得到密文串1010110110 和相应的明文串0100010001。假定攻击者也知道密钥流是使用3 级线性移位寄存器产生的，试破译该密码系统。

解： 容易得到密钥流序列为1110100111 。设产生该序列的三级线性移位寄存器的特征多项式为$f(x) = x^3 + c_1x^2 + c_2x + c_3$，利用密钥流序列的前6比特可以得到关系式

$$c_1 + c_2 + c_3 = 0;\ \ c_2 + c_3 = 1;\ \ c_1 + c_3 = 0.$$

通过解此线性方程组（在有限域$\mathbb{F}_2$上）可以得到

$$c_1 = 1,\ c_2 = 0,\ c_3 = 1.$$

从而该移位寄存器的特征多项式为$f(x) = x^3 + x^2 + 1$.

3. 试用Berlekamp-Massey 算法求产生序列：10011011000111010100 的最短线性移位寄存器，并画出结构图。

n	d_{n-1}	f_n	l_n
0		1	0
1	1	1+x	1
2	1	1	1
3	0	1	1
4	1	$1+x^3$	3
5	1	$1+x+x^3$	3
6	1	$1+x+x^2+x^3$	3
7	1	$1+x+x^2$	4
8	0	$1+x+x^2$	4
9	0	$1+x+x^2$	4
10	1	$1+x+x^2+x^3+x^4+x^5+x^6$	6
11	1	$1+x^4+x^5+x^6$	6
12	1	$1+x^2+x^3+x^5+x^6$	6
13	1	$1+x^2+x^4+x^6$	6
14	1	$1+x+x^2+x^3+x^7$	7
15	0	$1+x+x^2+x^3+x^7$	7
16	1	$1+x+x^2+x^5+x^6+x^7+x^8+x^9$	9
17	1	$1+x^3+x^4+x^5+x^6+x^7+x^9$	9
18	0	$1+x^3+x^4+x^5+x^6+x^7+x^9$	9
19	1	$1+x^3+x^9+x^{11}$	11

解： 生成该序列的最短移位寄存器的连接多项式为$1+x^3+x^9+x^{11}$. 计算过程中每步的结果如上表。

反馈关系图略。

对这条序列，$n_0=0$，我们自然地让$f_0(x)=1,\ l_0=0$即可。在计算开始时可以算出$f_1=1+x,\ f_2=f_3=1, l_1=l_2=l_3=1;\ f_4=1+x^2+x^3, l_4=$

3，这实际上说明序列的前3比特可以由退化的2级寄存器生成，到第4比特才由3级移位寄存器生成。（退化的意思是指连接多项式本来应该写成$f_2(x) = f_3(x) = 1 + 0 \cdot x$）。

在利用BM算法计算时为避免出错，可以每算出一个$f_i(x)$，都去检验一下它能否正确地产生第i比特前面所有的比特。否则一步错后面的计算就全都错了。