第二章作业参考答案

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$(a_1,a_2,a_3)=(1,0,1)$，求各线性反馈函数的输出序列及周期。

解：此时线性反馈函数可表示为 $f(a_1,a_2,a_3)=a_1\oplus c_2a_2\oplus c_1a_3$

当 $c_1=0$，$c_2=0$ 时，$f(a_1,a_2,a_3)=a_1\oplus c_2a_2\oplus c_1a_3=a_1$，

输出序列为 101101…，　　周期＝3

当 $c_1=0$，$c_2=1$ 时，$f(a_1,a_2,a_3)=a_1\oplus c_2a_2\oplus c_1a_3=a_1\oplus a_2$，

输出序列为 10111001011100…，周期＝7

当 $c_1=1$，$c_2=0$ 时，$f(a_1,a_2,a_3)=a_1\oplus c_2a_2\oplus c_1a_3=a_1\oplus a_3$，

输出序列为 10100111010011…，周期＝7

当 $c_1=1$，$c_2=1$ 时，$f(a_1,a_2,a_3)=a_1\oplus c_2a_2\oplus c_1a_3=a_1\oplus a_2\oplus a_3$，

有输出序列为 1010…，　　周期＝2

2．设 n 级线性反馈移位寄存器的特征多项式为 $p(x)$，初始状态为$(a_1,a_2,\ldots,a_{n-1},a_n)=(00\ldots01)$，证明输出序列的周期等于 $p(x)$的阶

证：设 $p(x)$的阶为 p，由定理 2-3，由 $r|p$，所以 $r\le p$

设 $A(x)$为序列$\{a_i\}$的生成函数，并设序列$\{a_i\}$的周期为 r，则显然有 $A(x)p(x)=\phi(x)$

又 $A(x)=a_1+a_2x+\ldots+a_rx^{r-1}+x^r(a_1+a_2x+\ldots+a_rx^{r-1})+(x^r)^2(a_1+a_2x+\ldots+a_rx^{r-1})+\cdots$

$=a_1+a_2x+\ldots+a_rx^{r-1}/(1-x^r)=a_1+a_2x+\ldots+a_rx^{r-1}/(x^r-1)$

于是 $A(x)=(a_1+a_2x+\ldots+a_rx^{r-1})/(x^r-1)=\phi(x)/p(x)$

又$(a_1,a_2,\ldots,a_{n-1},a_n)=(00\ldots01)$

所以 $p(x)(a_nx^{n-1}+\ldots+a_rx^{r-1})=\phi(x)(x^r-1)$　即 $p(x)x^{n-1}(a_n+\ldots+a_rx^{r-n})=\phi(x)(x^r-1)$

由于 x^{n-1} 不能整除 x^r-1，所以必有 $x^{n-1}|\phi(x)$，而$\phi(x)$的次数小于 n，所以必有$\phi(x)=x^{n-1}$

所以必有 $p(x)|(x^r-1)$，由 $p(x)$的阶的定义知，阶 $p\le r$

综上所述：$p=r$　#

3．设 n＝4，$f(a_1,a_2,a_3,a_4)=a_1\oplus a_4\oplus 1\oplus a_2a_3$，初始状态为$(a_1,a_2,a_3,a_4)=(1,1,0,1)$，求此非线性反馈移位寄存器的输出序列及周期。

解：由反馈函数和初始状态得状态输出表为

$(a_4\ a_3\ a_2\ a_1)$	输出	$(a_4\ a_3\ a_2\ a_1)$	输出
1 0 1 1	1	1 1 1 1	1
1 1 0 1	1	0 1 1 1	1
1 1 1 0	0	1 0 1 1	1（回到初始状态）

所以此反馈序列输出为：11011…周期为 5

4．设密钥流是由 $m=2s$ 级 LFSR 产生，其前 m+2 个比特是$(01)^{s+1}$，即 s＋1 个 01。问第 m+3 个比特有无可能是 1，为什么？

解：不能是 1。

可通过状态考察的方法证明以上结论。

首先 m 级 LFSR 的状态是一个 m 维的向量，则前 m 个比特构成一个状态 S_0，可表示为$(01)^s$，

第 m＋1 个比特是 0，所以 S_0 的下一个状态是 $S_1=(10)^s$，

第 m＋2 个比特是 1，所以 S_1 的下一个状态是 $S_2=(01)^s=S_0$，回到状态 S_0，

所以下一个状态应是 $S_3=S_1=(10)^s$，也即第 m+3 个比特应该为 0。

5．设密钥流是由 n 级 LFSR 产生，其周期为 2^n-1，i 是任一正整数，在密钥流中考虑以下比特对

$$(S_i, S_{i+1}), (S_{i+1}, S_{i+2}), \ldots, (S_{i+2^n-3}, S_{i+2^n-2}), (S_{i+2^n-2}, S_{i+2^n-1}),$$

问有多少形如$(S_j, S_{j+1})=(1,1)$的比特对？证明你的结论。

答：共有 $2^{(n-2)}$

证明：

证明方法一：由于产生的密钥流周期为 2^n-1，且 LFSR 的级数为 n，所以是 m 序列

以上比特对刚好是 1 个周期上，两两相邻的所有比特对，其中等于(1,1)的比特对包含在所有大于等于 2 的 1 游程中。由 m 序列的性质，所有长为 i 的 1 游程($1\le i\le n-2$)有 $2^{n-i-1}/2$ 个，没有长为 n－1 的 1 游程，有 1 个长为 n 的 1 游程。

长为 i (i>1)的 1 游程可以产生 i-1 个(1,1)比特对，

所以共有(1,1)比特对的数目 $N=2^{n-2-2}\times(2-1)+2^{n-3-2}\times(3-1)+\ldots+2^{n-i-2}\times(i-1)+\ldots+2^{n-(n-2)-2}\times(n-2-1)+n-1=\sum_{i=2}^{n-2}2^{n-i-2}(i-1)+n-1=2^{(n-2)}$

证明方法 2：考察形如 11*…*的状态的数目，共有 $2^{(n-2)}$个

6．已知流密码得密文串为 1010110110 和相应明文串 0100010001，而且还已知密钥流是使用 3 级线性反馈移位寄存器产生的，试破译该密码系统。

解：由二元加法流密码的加密算法可知，将密文串和相应的明文串对应位模 2 加可得连续的密钥流比特为 1110100111

设该三级线性反馈移位寄存器的反馈函数为 $f(a_1,a_2,a_3)=c_3a_1\oplus c_2a_2\oplus c_1a_3$

取其前 6 比特可建立如下方程

$$(a_4a_5a_6)=(c_3,c_2,c_1)\begin{bmatrix}a_1&a_2&a_3\\a_2&a_3&a_4\\a_3&a_4&a_5\end{bmatrix},$$

$$\text{即}(c_3,c_2,c_1)=(a_4a_5a_6)\begin{bmatrix}a_1&a_2&a_3\\a_2&a_3&a_4\\a_3&a_4&a_5\end{bmatrix}^{-1}=(0\ 1\ 0)\begin{bmatrix}1&1&1\\1&1&0\\1&0&1\end{bmatrix}^{-1}=(0\ 1\ 0)\begin{bmatrix}1&1&1\\1&0&1\\1&1&0\end{bmatrix}=(1\ 0\ 1)$$

所以 $f(a_1,a_2,a_3)=a_1\oplus a_3$，即流密码的递推关系式为 $a_{i+3}=a_{i+2}\oplus a_i$

7．若 GF(2)上的二元加法流密码的密钥生成器是 n 级线性反馈移位寄存器，产生的密钥是 m 序列。2.5 节已知，敌手若知道一段长为 2n 的明密文对就可破译密钥流生成器。如果敌手仅知道长为 2n－2 的明密文对，问如何破译密钥流生成器。

解：破译 n－LFSR 所产生的 m 序列，需要 2n 个连续比特，现在仅有 2n－2 个连续的密钥比特(由长为 2n－2 的明密文对逐位异或得到)，因此需要猜测后两个比特。这有 00，01，10，11 四种情况，对这些情况按下式逐一试破译

$$(a_{n+1}a_{n+2}..a_{2n})=(c_nc_{n-1}..c_1)\begin{pmatrix}a_1&a_2&\cdots&a_n\\a_2&a_3&\cdots&a_{n+1}\\\vdots&&&\\a_n&a_{n+1}&\cdots&a_{2n-1}\end{pmatrix}=(c_nc_{n-1}..c_1)\boldsymbol{X}$$

首先验证矩阵 $\boldsymbol{X}$ 的可逆性，如果不可逆则可直接排除此情况

其次对于可逆的情况，求解出$(c_nc_{n-1}..c_1)$，然后验证多项式 $p(x)=1+c_1x+\ldots+c_nx^n$ 是否是本原多项式，如果是，则是一解。

结果可能会多余 1 个。

8.设 J-K 触发器中$\{a_k\}$和$\{b_k\}$分别为 3 级和 4 级 m 序列，且

$\{a_k\}$＝11101001110100…

$\{b_k\}$＝001011011011000 001011011011000…

求输出序列$\{c_k\}$及周期。

解：由于 gcd(3，4)=1 且 $a_0+b_0=1$ 所以序列$\{c_k\}$的周期为$(2^3-1)(2^4-1)=105$

又由 J-K 触发器序列的递推式 $c_k=(a_k+b_k+1)c_{k-1}+a_k$，令 $c_{-1}=0$ 可得输出序列为：

$\{c_k\}$=11001001…

9．设基本钟控序列产生器中$\{a_k\}$和$\{b_k\}$分别为 2 级和 3 级 m 序列，且

$\{a_k\}$＝101101…

$\{b_k\}$＝10011011001101…

求输出序列$\{c_k\}$及周期。

解：序列$\{a_k\}$的周期 $p_1=2^2-1=3$，序列$\{b_k\}$的周期 $p_2=2^3-1=7$，$w_1=a_0+a_1+a_2=2$

而 gcd(w_1, p_2)=1。所以序列$\{c_k\}$的周期 $p=p_1p_2=3\times7=21$

记 LFSR2(产生序列$\{b_k\}$)的状态向量为σ_k，则σ_0＝(100)，在 LFSR1(产生序列$\{a_k\}$)的控制下，状态转移为：

$\{a_k\}$ 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1

(100),(001),(001),(011),(110),(110),(101),(011),(011),(110),(100),(100),(001),(011),(011),(110)

1 0 0 0 1 1 1 0 0 1 1 1 0 0 0 1

$\{a_k\}$ 1 0 1 1 0 1 1 0 1

(101),(101),(011),(110),(110),(100),(001), (001),(011)

1 1 0 1 1 1 0 0 0

所以输出序列为 100011100111000111011 1000…