1 设 4 级线性移位寄存器的反馈函数为 $f(b_4,b_3,b_2,b_1)=b_4\oplus b_1$ 初始状态 $(b_4b_3b_2b_1)=(1000)$ ，计算这个线性移位寄存器的状态转换图，并给出该移位寄存器的输出及周期。

2 设 $n=4$， $f(b_4,b_3,b_2,b_1)=b_4\oplus b_2b_3\oplus b_1\oplus 1$，初态为 $(b_4b_3b_2b_1)=(1011)$，计算这个非线性移位寄存器的状态转换图，并给出此非线性移位寄存器的输出序列及周期。

3 已知序列密码的密文串 1010110110 和相应的明文串 0100010001，且已知密钥流是使用了 3 级线性反馈移位寄存器产生的，试破译该密码系统。

4 构造一个输出小 m 序列的 5 级 LFSR。

5 调研 ZUC 算法，概述其三层结构并详细说明 ZUC 算法中线性移位寄存器的特色及优势。