LINEAR ALGEBRA PROBLEMS

(1) By reducing to a row echelon form prove that the following system does not have any solutions modulo 2.

$$\underbrace{\begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix}}_{A} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}}_{a}.$$

(2) By reducing to a row echelon form find all solutions to the system modulo 2.

$$\underbrace{\begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix}} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}}.$$

(3) Let $f(X) = X^n + c_1 X^{n-1} + \ldots + c_n$ and

$$A = \begin{pmatrix} c_1 & 1 & 0 & \ldots & 0 \\ c_2 & 0 & 1 & \ldots & 0 \\ & & & \ldots & \\ c_{n-1} & 0 & 0 & \ldots & 1 \\ c_n & 0 & 0 & \ldots & 0 \end{pmatrix}$$

Let $S_0 = (s_{n-1}, \ldots, s_1, s_0)$ and $S_1 = (s_n, \ldots, s_2, s_1)$ be two consecutive states of an LFSR with the generating polynomial $f(X)$. Prove

(a) $S_1 = S_0 A$

(b) The characteristic polynomial of A is $f(X)$. Hint: by definition(we work modulo 2) the characteristic polynomial of A is the determinant of the matrix $X \cdot I + A$, where I is an $n \times n$ identity matrix. Use the Laplace formula to represent the determinant as a sum.

1)
$$M = \left(\begin{array}{ccccc|c} \boxed{0} & 1 & 1 & 1 & 0 & 1 \\ \boxed{1} & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \to \left(\begin{array}{ccccc|c} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

$$\to \left(\begin{array}{ccccc|c} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & \boxed{1} & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 \end{array}\right) \to \left(\begin{array}{ccccc|c} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & \boxed{1} \end{array}\right)$$

$\neq 0$

$\Rightarrow$ no solutions

(as $0 = 1$)

2) $$M = \begin{array}{c} \begin{matrix} 0 & 1 & 0 & 0 & 0 & \end{matrix} \\ \left(\begin{array}{ccccc|c} 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \end{array}\right) \end{array} \to \left(\begin{array}{ccccc|c} 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{array}\right)$$

$$\to \left(\begin{array}{ccccc|c} 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right) \to \begin{array}{c} \begin{matrix} t_1 & t_2 & t_3 & & & \end{matrix} \\ \left(\begin{array}{ccccc|c} 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \boxed{0} \end{array}\right) \end{array}$$

there are solutions

$r = \text{rank} = 3 \Rightarrow \#\text{ solutions} = 2^{5-3} = 4$

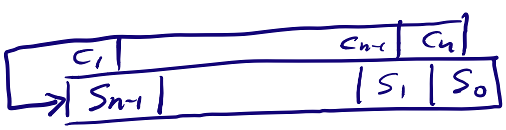
$\underbrace{x_4, x_5}$ any values

$\underbrace{x_1, x_2, x_3}$ are to be computed

$$x_{t_i} = M_{i\,n+1} + \sum_{j=t_i+1}^{n} x_j M_{ij} \qquad (n=5)$$

x_1	x_2	x_3	x_4	x_5
0	1	0	0	0
1	0	0	0	1
0	1	1	1	0
1	0	1	1	1

all solutions to the system.

3) 

$f(x) = X^n + c_1 X^{n-1} + \dots + c_n$

gen. polynomial.

companion matrix to f

$$(s_{n-1} \dots s_1 s_0) \cdot \begin{pmatrix} c_1 & 1 & 0 & & 0 \\ c_2 & 0 & 1 & & 0 \\ \dots & & & & \\ c_{n-1} & 0 & 0 & & 1 \\ c_n & 0 & 0 & & 0 \end{pmatrix} = (s_n s_{n-1} \dots s_2 s_1)$$

current state $\qquad\qquad$ next state.

$$\begin{pmatrix} c_1 & 1 & 0 & & 0 \\ \dots & & & & \\ c_n & 0 & 0 & & 0 \end{pmatrix} = A$$

characteristic polynomial for A

$$\det(\underbrace{x \cdot I}_{n \times n \text{ unity matrix}} + A) = \det \underbrace{\begin{array}{c} \\ \\ i=3 \\ \\ \\ \\ \\ \end{array} \begin{array}{c} j=1 \\ \begin{pmatrix} c_1+x & 1 & 0 & 0 & 0 & 0 & \dots & 0 \\ c_2 & x & 1 & 0 & 0 & 0 & \dots & 0 \\ c_3 & 0 & x & 1 & 0 & 0 & \dots & 0 \\ c_4 & 0 & 0 & x & 1 & 0 & \dots & 0 \\ \dots & & & & & & & x \quad 1 \\ c_{n-1} & 0 & 0 & 0 & 0 & 0 & \dots & 0 \quad x \\ c_n & 0 & 0 & 0 & 0 & 0 & \dots & \end{pmatrix} \end{array}}_{B = (b_{ij})_{1 \le i,j \le n}} =$$

Laplace rule

$$\det B = \sum_{i=1}^{n} b_{ij} \cdot M_{ij} \cdot (-1)^{i+j}$$

$$M_{ij} = \det \left(\begin{array}{c|c} & j \\ i & \end{array} \right)_{n-1 \times n-1}$$

ith row and jth column were removed

$$\det(xI + A) = \left[(c_1 + x) \det \begin{pmatrix} x & 1 & & 0 \\ & x & 1 & \\ & & \ddots & 1 \\ 0 & & & x \end{pmatrix}_{n-1 \times n-1} = (c_1 + x) \cdot x^{n-1} \right]$$

$$+\left[c_2 \cdot \det \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & x & 1 & \cdots & 0 \\ & & x & 1 & \\ 0 & & & & 1 \\ & & & & x \end{pmatrix}_{(n-1)\times(n-1)} = c_2 \cdot x^{n-2} \right]$$

$$+\left[c_3 \cdot \det \begin{pmatrix} \cancel{1} & 0 & 0 & \cdots & 0 \\ \cancel{x} & 1 & 0 & \cdots & 0 \\ 0 & 0 & x & 1 & 0 \\ & & & \ddots & 1 \\ & & & & x \end{pmatrix} = c_3 \cdot \det \begin{pmatrix} 1 & & \\ x & 1 & \\ & \ddots & 1 \\ & & x \end{pmatrix}_{n-2 \times n-2} + c_3 \cdot \det \begin{pmatrix} 0 & \cdots & 0 \\ & x & \end{pmatrix} \right.$$

$$\left. = c_3 \cdot x^{n-3} \right]$$

$$+\left[c_4 \cdot \det \begin{pmatrix} 1 & & & \\ x & 1 & & \\ & x & 1 & \\ & & x & 1 \\ & & & \ddots & 1 \\ & & & & x \end{pmatrix} = c_4 \cdot x^{n-4} \right] + \cdots$$

$$+\left[c_n \cdot \det \begin{pmatrix} 1 & & \\ x & 1 & \\ & x & \ddots \\ & & x \; 1 \end{pmatrix} = c_n \right] =$$

$$= x^n + c_1 \cdot x^{n-1} + c_2 \cdot x^{n-2} + c_3 \cdot x^{n-3} + \cdots + c_n = f(x).$$