7.6.9

If F is a field and $f(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_1 x - a_0$ is a polynomial in $F[x]$. Define the *companion matrix* by the formula

$$C_f(x) = \begin{bmatrix} 0 & 0 & \cdots & a_0 \\ 1 & 0 & \cdots & a_1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{n-1} \end{bmatrix}$$

Prove the following:

a) $\det(C_f - xI) = (-1)^{n-1} f(x)$

b) $\det(xC_f - I) = (-1)^n f^*(x)$, where $f^*(x)$ denotes the reciprocal polynomial.

Solution:

a) We prove this by induction. The base case of degree 1 is clear. To see the induction step we expand the determinant along the top row. With this expansion we find that $\det(C_f - xI) = -x\det(M) + (-1)^{n-1}a_0 \det N$, where $M = C_{f'} - I$, for $C_{f'}$ the companion matrix of the polynomial $x^{n-1} - a_{n-1}x^{n-2} - a_1$, and N is the matrix

$$N = \begin{bmatrix} 1 & -x & 0 & \cdots & 0 & & & \\ 0 & 1 & -x & \cdots & 0 & & & \\ \vdots & \vdots & \ddots & \vdots 0 & 0 & \cdots & 1 \end{bmatrix}$$

By the induction hypothesis $\det(M) = (-1)^{n-2}(x^{n-1} - a_{n-1}x^{n-2} - a_1)$ and it is straightforward to argue that $\det(N) = 1$ (for example by induction). Putting these facts together gives the formula.

b) We do another induction argument. Again the degree 1 case is obvious, and the induction step begins with expanding the determinant along the top row. We find that $\det(xC_f - I) = -1\det(M) + xa_0 \det(N)$. The matrix $M = xC_{f'} - I$ for $C_{f'}$ the companion matrix of the polynomial $x^{n-1} - a_{n-1}x^{n-2} - a_1$, and N is the matrix

$$N = \begin{bmatrix} x & -1 & 0 & \cdots & 0 & & & \\ 0 & x & -1 & \cdots & 0 & & & \\ \vdots & \vdots & \ddots & \vdots 0 & 0 & \cdots & x \end{bmatrix}$$

By induction $\det(M) = (-1)^n f^*(x)$ and a simple induction argument proves that $\det(N) = x^{n-1}$. Putting these facts together gives the result.

7.6.10

See textbook for problem statement

Solution:

Multiplying by C_f is exactly the same computation as iterating the corresponding feedback shift register.

7.6.11

Given that $x^3 + 2x + 1$ is a primitive polynomial over $\mathbb{F}_3$, compute the table of powers of a root θ using the companion matrix method.

Solution:

The companion matrix is:

$$C_f = \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

The vector corresponding to θ is $(0, 1, 0)$. By multiplying this vector with C_f we obtain the other powers of θ.

$$\begin{array}{c|c}
\theta^0 & (1,0,0) = 1 \\
\theta^1 & (0,1,0) = \theta \\
\theta^2 & (0,0,1) = \theta^2 \\
\theta^3 & (-1,1,0) = -1 + \theta \\
\theta^4 & (0,-1,1) = -\theta + \theta^2 \\
\theta^5 & (-1,1,-1) = -1 + \theta - \theta^2 \\
\theta^6 & (1,1,-1) \\
\theta^7 & (-1,-1,1) \\
\theta^8 & (-1,0,-1) \\
\theta^9 & (1,1,0) \\
\theta^{10} & (0,1,1) \\
\theta^{11} & (-1,1,1) \\
\theta^{12} & (-1,0,1) \\
\theta^{13} & (-1,0,0) \\
\theta^{14} & (0,-1,0) \\
\theta^{15} & (0,0,-1) \\
\theta^{16} & (1,-1,0) \\
\theta^{17} & (0,1,-1) \\
\theta^{18} & (1,-1,1) \\
\theta^{19} & (-1,-1,1) \\
\theta^{20} & (1,1,-1) \\
\theta^{21} & (1,0,1) \\
\theta^{22} & (-1,-1,0) \\
\theta^{23} & (0,-1,-1) \\
\theta^{24} & (1,-1,-1) \\
\theta^{25} & (1,0,-1) \\
\theta^{26} & (1,0,0)
\end{array}$$