ECE 3553 Homework #3 Solutions Brad

**Problem 3-3**

A polynomial of degree 3 is primitive if the smallest power of $D$ which it divides evenly is $D^7 + 1$. The smallest power of $D$ which needs to be checked is $D^3$:

$$\begin{array}{r} 1 \\ \hline D^3 + D + 1 \;\big|\; D^3 + 1 \\ \underline{D^3 + D + 1} \\ D \end{array}$$

$$\begin{array}{r} D \\ \hline D^3 + D + 1 \;\big|\; D^4 + 1 \\ \underline{D^4 + D^2 + D} \\ D^2 + D + 1 \end{array}$$

$$\begin{array}{r} D^2 + 1 \\ \hline D^3 + D + 1 \;\big|\; D^5 + 1 \\ \underline{D^5 + D^3 + D^2} \\ D^3 + D^2 + 1 \\ \underline{D^3 + D + 1} \\ D^2 + D \end{array}$$

$$\begin{array}{r} D^3 + D + 1 \\ \hline D^3 + D + 1 \;\big|\; D^6 + 1 \\ \underline{D^6 + D^4 + D^3} \\ D^4 + D^3 + 1 \\ \underline{D^4 + D^2 + D} \\ D^3 + D^2 + D + 1 \\ \underline{D^3 + D + 1} \\ D^2 \end{array}$$

$$
\begin{array}{rl}
 & D^4 + D^2 + D + 1 \\
\hline
D^3 + D + 1 \;\big| & D^7 \qquad\qquad + 1 \\
 & \underline{D^7 + D^5 + D^4 \qquad + 1} \\
 & \quad D^5 + D^4 \\
 & \quad \underline{D^5 + \qquad D^3 + D^2} \\
 & \qquad D^4 + D^3 + D^2 \qquad + 1 \\
 & \qquad \underline{D^4 + \qquad D^2 + D} \\
 & \qquad\quad D^3 \qquad + D + 1 \\
 & \qquad\quad \underline{D^3 + \qquad D + 1} \\
 & \qquad\quad 0
\end{array}
$$

Thus, by exhaustive search we have found that $1 + D + D^3$ is primitive.

## Problem 3-4

Suppose that there are two additive identity elements, 0 and 0'. By definition, the sum of an additive identy element with *any* element of the field is an element. In particular $0 = 0 + 0' = 0'$. Suppose there are two multiplicative identity elements, 1 and 1'. By definition, the product of a multiplicative identity with any non-zero element of the field is the element. In particular, $1 = 1 \cdot 1' = 1'$.

## Problem 3-5

Set $D = 1$ to obtain $g(D) = g(1) = 1 + 1^2 + 1^3 + 1^4 = 0$. Thus $D = 1$ is a root and $D + 1$ is a factor. Divide $g(D)$ by $D + 1$:

$$
\begin{array}{rl}
 & D^3 + D + 1 \\
\hline
D + 1 \;\big| & D^4 + D^3 + D^2 + \quad 1 \\
 & \underline{D^4 + D^3} \\
 & \qquad D^2 + \quad 1 \\
 & \qquad \underline{D^2 + D} \\
 & \qquad\quad D + 1 \\
 & \qquad\quad \underline{D + 1} \\
 & \qquad\quad 0
\end{array}
$$

Thus

$$g(D) = (1 + D)(1 + D + D^3)$$

$$[g(D)]^2 = (1 + D^2 + D^3 + D^4)(1 + D^2 + D^3 + D^4)$$

$$= 1 + D^4 + D^6 + D^8 \text{ (after simplification )}$$

$$[g(D)]^4 = (1 + D^4 + D^6 + D^8)(1 + D^4 + D^6 + D^8)$$

$$= 1 + D^8 + D^{12} + D^{16} \text{ (after simplification )}$$

Observe that $[g(D)]^4 = g(D^4)$. In general, it can be shown that $[g(D)]^{2^i} = g(D^{2^i})$.

**Problem 3-6**

(a) The Galois field for this problem is the same field used in Ex. 3-5(a): $D^{10} \cdot D^{12} = D^{22}$. We know that $D^{15} = 1$. Thus, $D^{22} = D^{15} \cdot D^7 = D^7 = 1 + D + D^3$. Alternatively,

$$D^{10} \cdot D^{12} = (1 + D + D^2)(1 + D + D^2 + D^3)$$

$$= 1 \quad + D^2 + D^3 \quad + D^5$$

Divide $D^4$ by the primitive polynomial:

$$\begin{array}{r|l} & 1 \\ D^4 + D + 1 & D^4 \\ & \underline{D^4 + D + 1} \\ & D + 1 \end{array}$$

and $D^4 = D^3 \cdot D = D + 1$. Multiply both sides by $D$ to obtain $D^5 = D + D^2$ and

$$D^{10} \cdot D^{12} = 1 + D^2 + D^3 + D + D^2$$

$$= 1 + D + D^3$$

(b)

$$D^{10} + D^{12} = 1 + D + D^2 + 1 + D + D^2 + D^3$$

$$= (1 + 1) + (1 + 1)D + (1 + 1)D^2 + (1 + 0)D^3$$

$$= D^3$$

(c)

$$\frac{D^{10}}{D^{12}} = D^{10}(D^{-12})$$

where $(D^{-12})$ is the multiplicative inverse of $D^{12}$. Since $D^{15} = 1$, $(D^{-12}) = D^3$. Thus

$$D^{10}(D^{-12}) = D^{10} \cdot D^3 = D^{13} = 1 + D^2 + D^3$$

(d) Addition and subtraction are identical on GF(2) so that

$$D^{10} - D^{12} = D^{10} + D^{12} = D^3$$

## Problem 3-7

The shift register configuration is derived from Figure 3-3. The result is $a(D) = 1 + D + D^2 + D^3$. The output of the circuit is calculated using normal polynomial multiplication and division:

$$a(D)g(D) = (1 + D + D^2)(1 + D + D^2 + D^3)$$

$$= 1 + D^2 + D^3 + D^5$$

The output by division:

$$\begin{array}{r} 1 + D + D^3 + D^7 + D^8 + D^9 + D^{10} + D^{12} + D^{12} + D^{14} + D^{15} + D^{18} + D^{22} \\ 1 + D + D^4 \;\big|\; 1 + D^2 + D^3 + D^5 \\ \underline{1 + D \qquad + D^4} \\ D + D^2 + D^3 + D^4 + D^5 \\ \underline{D + D^2 \qquad\qquad D^5} \\ D^3 + D^4 \\ \underline{D^3 + D^4 \quad + D^7} \\ D^7 \\ \underline{D^7 + D^8 + \quad D^{11}} \\ D^8 + \quad D^{11} \\ \underline{D^8 + D^9 + \qquad D^{12}} \\ D^9 + \quad D^{11} + D^{12} \\ \underline{D^9 + D^{10} + \qquad D^{13}} \\ D^{10} + D^{11} + D^{12} + D^{13} \\ \underline{D^{10} + D^{11} + \qquad D^{14}} \\ D^{12} + D^{13} + D^{14} \end{array}$$

Observe that after the fourth clock interval, the output is periodic with period 15 and pattern 000111101011001. With proper selection of $g(D)$ and $a(D)$ this circuit can be used to perform the division of Problem 8-6.

**Problem 3-8**

Refer to Fig. 3-3. The feedback connections are defined by the polynomial $g(D) = 1 + D^2 + D^3 + D^5 + D^6$. The initial condition can be established using the circuit of Fig. 3-3 with $h(D) = D^6$ and input $a(D) = 1 + D + D^2 + D^3$. The output (including time used for loading) is

$$b(D) = \frac{D^6(1 + D + D^2 + D^3)}{1 + D^2 + D^3 + D^5 + D^6}$$

The output is obtained by polynomial log division with the result (see the solution to Prob. 3-7 for an example)

$$y(D) = D^6 + D^7 + D^9 + D^{10} + D^{14} + D^{17} + D^{22} + D^{23} + D^{24} + D^{30} + D^{32} + D^{33} + D^{34} + D^{35} + \cdots$$

**Problem 3-9**

The feedback connections are described by the polynomial $g(D) = 1 + D^2 + D^3 + D^5 + D^6$. The shift register output can be found by finding the equivalent initial fill $a'(D)$ for the shift register configuration of Fig. 3-5. This is accomplished by using (3-41) and equating coefficients on each side of the equation:

$$(1 + D + D^2 + D^3)(1 + D^2 + D^3 + D^5 + D^6) + e(D) = a_0 + a_1D + a_2D^2 + a_3^3 + a_4D^4 + a_5D^5$$

$e(D)$ contains no power of $D$ less than 6 and can be ignored. Equating coefficients gives:

$a_0 = 1$ $\qquad$ $a_3 = 1 + 1 + 1 = 1$

$a_1 = 1$ $\qquad$ $a_4 = 1 + 1 = 0$

$a_2 = 1 + 1 = 0$ $\qquad$ $a_5 = 1 + 1 + 1 = 1$

Thus $a(D) = 1 + D + D^3 + D^5$. The output is now calculated using polynomial long division. The result is

$$y(D) = 1 + D + D^2 + D^3 + D^6 + D^8 + D^{10} + D^{14} + \cdots$$

| $N$ | $P_0$ | $m_0$ | $P_1$ | $10 \log_{10}(P_0/P_1)$ |
|---|---|---|---|---|
| 3 | 0.111 | 0 | 0 | - |
| 7 | 0.184 | 0 | 0 | - |
| 15 | 0.218 | 1 | 0.0354 | 7.9 dB |
| 63 | 0.242 | 6 | 0.0482 | 7.01 dB |
| 255 | 0.248 | 24 | 0.0471 | 7.21 dB |

For $N$ very large, $P_0 \rightarrow 0.25$ and the summation for $P_1$ approaches an integral. Let $1/N = \Delta$ and $m\Delta = x$. Then

$$P_1 = 0.25 \int_{x_0}^{x_0} \text{sinc}^2(x/2)\,dx \approx 0.05$$

and $10 \log_{10}(P_0/P_1) = 6.99$ dB. Observe that increasing $N$ does not significantly affect the code self noise component.

**Problem 3-18**

The period of the code is $2^{10} - 1 = 1023$ symbols for 10.23 μs. The propagation delay of 0.15 μs is equivalent to 15 clock cycles. The shift register generator has 10 stages and cycles through the nonzero elements of GF($2^{10}$) in reverse order. Let the initial condition of the transmitter be $a(D) = 1$. Then the initial condition in the receiver is the remainder when $D^{15}a(D) = D^{15}$ is divided by $g(D) = 1 + D^3 + D^{10}$ which is $R(D) = D^8 + D^6 = a'(D)$. Thus the transmitter and receiver initial loads are

0000000001 (Transmitter )
0100100000 (Receiver )

This result can be checked by calculation of the two output sequences by polynomial long division. When this is done, note that, beginning with the 15th clock cycle, the receiver begins to reproduce the sequence which started with the first clock cycle in the transmitter.

**Problem 3-19**

Using the same procedure as in Example 3-20, the delay polynomial $S(D)$ is the remainder when dividing $D^{15}$ by $g(D) = 1 + D^3 + D^{10}$. The result is

$$S(D) = D^5 + D^8$$

Thus, the modulo-2 sum of a 5 unit delay and an 8 unit delay will produce the desired 15

(b) The inverse of **G** is

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

and

$$[G^{-1}]^5 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

Therefore the state five clock cycles before $\mathbf{S}_0$ is

$$S_{-5} = [G^{-1}]^5 \times S_0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

These results may be verified by manual calculation of the shift register states.

**Problem 3-25**

The shift register of a maximal length sequence generator passes through all states except the all zero state exactly once. The sequence generator has exactly two cycles. The first is the maximal-length cycle and the second is the cycle consisting only of the all zeros state. Consider an arbitrary Fibonacci feedback generator with an odd number of taps. Suppose this sequence generator is in the all-ones state. Since there are an odd number of taps, the modulo-2 sum of the odd number of "ones' in the shift register equals "one". Thus, the shift register input is a "one" and the shift register will remain in the all-ones state forever. Thus, the sequence generator has at least three cycles and cannot be maximal length.

**Problem 3-26**

The Fibonacci feedback shift register for this generator polynomial is