ANSWER TO HOMEWORK 7 PROBLEM 1 OF CMSC 653
SPRING SEMESTER 2001

SAMUEL J. LOMONACO, JR.

Here are the answers to Problem 1 of Homework 7. I haven't checked my calculations. So use at your own risk!

The roots of $m_1(x)$, $m_3(x)$, and $m_5(x)$ are

Polynomial	**Roots**
$m_1(x)$	α, α^2,α^4, α^8
$m_3(x)$	α^3, α^6,α^{12}, α^9
$m_5(x)$	α^5, α^{10}

Hence the roots of the generator polynomial are:

$$\underbrace{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6}_{\text{Run of 6}}, \underbrace{\alpha^8, \alpha^9, \alpha^{10}}_{\text{Run of 3}}, \alpha^{12}$$

It follows that the desiged distance of this BCH code is $\delta = 6 + 1$, and that this is a 3 error-correcting BCH code.

We now compute the power-sum symmetric functions:

$$\begin{cases} S_1 &= & r(\alpha) &= & \alpha^5 \\ S_2 &= & S_1^2 &= & \alpha^{10} \\ S_3 &= & r(\alpha^3) &= & \alpha^9 \\ S_4 &= & S_2^2 &= & \alpha^5 \\ S_5 &= & r(\alpha^5) &= & \alpha^5 \\ S_6 &= & S_3^2 &= & \alpha^3 \end{cases}$$

We need to solve over $GF(2^4)$ the system of equations

$$\begin{cases} S_1\sigma_3 + S_2\sigma_2 + S_3\sigma_1 &= & S_4 \\ S_2\sigma_3 + S_3\sigma_2 + S_4\sigma_1 &= & S_5 \\ S_3\sigma_3 + S_4\sigma_2 + S_5\sigma_1 &= & S_6 \end{cases}$$

which in this case is:

$$\begin{cases} \alpha^5\sigma_3 + \alpha^{10}\sigma_2 + \alpha^9\sigma_1 & = & \alpha^5 \\ \alpha^{10}\sigma_3 + \alpha^9\sigma_2 + \alpha^5\sigma_1 & = & \alpha^5 \\ \alpha^9\sigma_3 + \alpha^5\sigma_2 + \alpha^5\sigma_1 & = & \alpha^3 \end{cases}$$

The corresponding matrix of this linear system of equations over $GF(2^4)$ is:

$$\left(\begin{array}{ccc|c} \alpha^5 & \alpha^{10} & \alpha^9 & \alpha^5 \\ \alpha^{10} & \alpha^9 & \alpha^5 & \alpha^5 \\ \alpha^9 & \alpha^5 & \alpha^5 & \alpha^3 \end{array}\right)$$

After applying Guassian elimination, this becomes (if I haven't made a mistake)

$$\left(\begin{array}{ccc|c} 1 & \alpha^5 & \alpha^4 & 1 \\ 0 & 1 & \alpha^5 & \alpha^8 \\ 0 & 0 & 1 & \alpha^5 \end{array}\right)$$

Hence,

$$\begin{cases} \sigma_3 + \alpha^{15}\sigma_2 + \alpha^4\sigma_1 & = & 1 \\ \sigma_2 + \alpha^5\sigma_1 & = & \alpha^8 \\ \sigma_1 & = & \alpha^5 \end{cases}$$

Thus, after back substitution, we have

$$\begin{cases} \sigma_1 = \alpha^5 \\ \sigma_2 = \alpha \\ \sigma_3 = \alpha^{10} \end{cases}$$

It follows that the error locator polynomial is:

$$\pi(X) = X^3 + \alpha^5 X^2 + \alpha X + \alpha^{10}$$

The roots of this polynomial are the error locators.