Assignment #8 Due 4-12-05

For $F = GF(2^5) = \mathbb{Z}_2(x)/x^5+x^2+1$

$\alpha = x$

Find generator polynomial g, check polynomial f and generator matrix for $BCH(5,3)$

1. Compute $m_\alpha(x)$, $m_{\alpha^3}(x)$, $m_{\alpha^5}(x)$

✓ α^5	α^4	α^3	✓ α^2	α	✓ 1
0	x^4	0	0	0	0
0	0	x^3	0	0	0
x^2	0	0	x^2	0	0
0	0	0	0	x	0
1	0	0	0	0	1

$\alpha^5 + \alpha^2 + 1 = 0$

$m_\alpha(x) = x^5 + x^2 + 1$

✓ $(\alpha^3)^5$	✓ $(\alpha^3)^4$	✓ $(\alpha^3)^3$	✓ $(\alpha^3)^2$	$(\alpha^3)^1$	✓ 1
x^4	0	x^4	0	0	0
x^3	x^3	x^3	x^3	x^3	0
x^2	x^2	0	0	0	0
x	x	x	x	0	0
1	0	0	0	0	1

$(\alpha^3)^5 + (\alpha^3)^4 + (\alpha^3)^3 + (\alpha^3)^2 + 1 = 0$

$m_{\alpha^3}(x) = x^5 + x^4 + x^3 + x^2 + 1$

✓ $(\alpha^5)^5$	✓ $(\alpha^5)^4$	$(\alpha^5)^3$	✓ $(\alpha^5)^2$	✓ $(\alpha^5)^1$	✓ 1
x^4	0	x^4	x^4	0	0
x^3	x^3	x^3	0	0	0
0	x^2	x^2	0	x^2	0
0	0	x	0	0	0
1	0	1	1	1	1

$(\alpha^5)^5 + (\alpha^5)^4 + (\alpha^5)^2 + (\alpha^5)^1 + 1 = 0$

$m_{\alpha^5}(x) = x^5 + x^4 + x^2 + x + 1$

To check $m_{\alpha^i}(x)$ irreducible, need to see: 0 not a root (not divisible by x), 1 not a root (not divisible by $x+1$), not divisible by x^2+x+1. For 3rd check:

$$x^5+x^2+1 = (x^3+x^2)(x^2+x+1)+1$$
$$x^5+x^4+x^3+x^2+1 = (x^3+1)(x^2+x+1)+x$$
$$x^5+x^4+x^2+x+1 = (x^3+x)(x^2+x+1)+1$$

2. $g =$ common multiple of distinct m_{α^i} $i = 1, 3, 5$

$$g = (x^5+x^2+1)(x^5+x^4+x^3+x^2+1)(x^5+x^4+x^2+x+1)$$
$$= x^{15}+x^{11}+x^{10}+x^9+x^8+x^7+x^5+x^3+x^2+x+1$$

3. $f =$ result of dividing $x^{31}-1$ by g

$$= x^{16}+x^{12}+x^{4}+x^{10}+x^9+x^8+x^4+x+1$$

(see next page)

4. Rank $= (n-1)-(\deg g) = 31-15=16$

G is 31×16 matrix with columns

$x^{15}g \quad x^{14}g \quad --- \quad x^2g \quad xg \quad g$

(see last page)

The other irreducible polynomials of degree 5 are

$$x^5 + x^3 + x^2 + x + 1$$
$$x^5 + x^4 + x^2 + x + 1$$
$$x^5 + x^3 + 1$$

Since these are also factors of $x^{31} - 1$, and so is $x+1$,

$$f = (x^5 + x^3 + x^2 + x + 1)(x^5 + x^4 + x^2 + x + 1) \cdot (x^5 + x^3 + 1)(x+1)$$

$$= x^{16} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^4 + x + 1$$

31 x 16

$$
\begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0\\
1&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0\\
1&1&1&1&1&0&0&0&1&0&0&0&0&0&0&0\\
0&1&1&1&1&1&0&0&0&1&0&0&0&0&0&0\\
1&0&1&1&1&1&1&0&0&0&1&0&0&0&0&0\\
0&1&0&1&1&1&1&1&0&0&0&1&0&0&0&0\\
1&0&1&0&1&1&1&1&1&0&0&0&1&0&0&0\\
1&1&0&1&0&1&1&1&1&1&0&0&0&1&0&0\\
1&1&1&0&1&0&1&1&1&1&1&0&0&0&1&0\\
1&1&1&1&0&1&0&1&1&1&1&1&0&0&0&1\\
0&1&1&1&1&0&1&0&1&1&1&1&1&0&0&0\\
0&0&1&1&1&1&0&1&0&1&1&1&1&1&0&0\\
0&0&0&1&1&1&1&0&1&0&1&1&1&1&1&0\\
0&0&0&0&1&1&1&1&0&1&0&1&1&1&1&1\\
0&0&0&0&0&1&1&1&1&0&1&0&1&1&1&1\\
0&0&0&0&0&0&1&1&1&1&0&1&0&1&1&1\\
0&0&0&0&0&0&0&1&1&1&1&0&1&0&1&1\\
0&0&0&0&0&0&0&0&1&1&1&1&0&1&0&1\\
0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&0\\
0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&1\\
0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1
\end{bmatrix}
$$