1. Put $\beta = \alpha$ where $\alpha$ is a primitive element of $GF(16)$ as defined in the table for $GF(16)$ in the notes. Consider the binary BCH-code of length 15 with generator polynomial

$$\text{lcm}(m_\beta(x), m_\beta^2(x), m_\beta^3(x), m_\beta^4(x))$$

(a) What is the dimension of this code?
(b) What is the designed distance of this code?
(c) Use the Peterson-Gorenstein-Zierler decoding algorithm to decode the following word:

$$y = 111000000000000$$

**Solution** : (a)(b) Careful: the code is a BINARY code so $q = 2$. This is not a Reed-Solomon code!

The cyclotomic cosets depending on $n = 15$ and $q = 2$ are

$$\{0\}, \ {1, 2, 4, 8}, \ {3, 6, 12, 9}, \ {5, 10} \ \text{and} \ {7, 14, 13, 11}$$

From the cyclotomic cosets, we get that

$$g_0(x) := m_\beta^0(x) = x - \beta^0$$
$$g_1(x) := m_\beta^1(x) = m_\beta(x) = m_\beta(x) = (x - \beta_1)(x - \beta_2)(x - \beta_4)(x - \beta_8)$$
$$g_2(x) := m_\beta^2(x) = m_\beta^0(x) = m_\beta^2(x) = m_\beta^2(x) = (x - \beta_2)(x - \beta_6)(x - \beta_2^2)(x - \beta_2^6)$$
$$g_3(x) := m_\beta^3(x) = m_\beta^2(x) = m_\beta^3(x) = m_\beta^3(x) = m_\beta^3(x) = (x - \beta_3)(x - \beta_9)(x - \beta_3^2)(x - \beta_3^6)$$
$$g_4(x) := m_\beta^4(x) = m_\beta^3(x) = m_\beta^2(x) = m_\beta^3(x) = m_\beta^4(x) = m_\beta^4(x) = (x - \beta_4)(x - \beta_8^2)(x - \beta_8^8)$$

From the given generator polynomial, we get that $b = 1$ and $\delta = 4 + 1 = 5$.

So

$$g(x) = \text{lcm}(m_\beta(x), m_\beta^2(x), m_\beta^3(x), m_\beta^4(x)) = \text{lcm}(g_1(x), g_1(x), g_2(x), g_1(x)) = g_1(x)g_2(x)$$

Hence

$$\deg(g(x)) = \deg(g_1(x)g_2(x)) = \deg(g_1(x)) + \deg(g_2(x)) = 4 + 4 = 8$$

Thus

$$\dim(C) = n - \deg(g(x)) = 15 - 8 = 7$$

(c) We have that

$$y(x) = 1 + x + x^2$$

First, we calculate $\delta - 1 = 4$ syndromes. We get

$$S_1 = y(\beta) = y(\alpha) = 1 + \alpha + \alpha^2 = 0001 + 0010 + 0100 = 0111 = \alpha^7$$
$$S_2 = y(\beta^2) = y(\alpha^2) = 1 + \alpha^2 + \alpha^4 = 0001 + 0100 + 1001 = 1100 = \alpha^{14}$$
$$S_3 = y(\beta^3) = y(\alpha^3) = 1 + \alpha^3 + \alpha^6 = 0001 + 1000 + 1111 = 0110 = \alpha^{13}$$
$$S_4 = y(\beta^4) = y(\alpha^4) = 1 + \alpha^4 + \alpha^8 = 0001 + 1001 + 1110 = 0110 = \alpha^{13}$$

Next, we calculate $k$, the number of errors that occurred. Since $\delta = 5$, we have that $t = 2$. We get

$$\begin{vmatrix} \alpha^7 & \alpha^{14} \\ \alpha^{14} & \alpha^{13} \end{vmatrix} = \alpha^7\alpha^{13} + \alpha^{14}\alpha^{14} = \alpha^{20} + \alpha^{28} = \alpha^5 + \alpha^{13} = 1011 + 0110 = 1101 = \alpha^{11} \neq 0$$

Hence we assume that $k = 2$ : two errors occurred.
Next, we find the error-locating polynomial. So we have to solve
\[
\begin{bmatrix}
\alpha^7 & \alpha^{14} \\
\alpha^{14} & \alpha^{13}
\end{bmatrix}
\begin{bmatrix}
s_2 \\
s_1
\end{bmatrix}
= \begin{bmatrix}
\alpha^{13} \\
\alpha^{13}
\end{bmatrix}
\]

We use Cramer’s Rule.

Since
\[
\begin{vmatrix}
\alpha^{13} & \alpha^{14} \\
\alpha^{13} & \alpha^{13}
\end{vmatrix} = \alpha^{13}\alpha^{15} + \alpha^{13}\alpha^{14} = \alpha^{26} + \alpha^{27} = \alpha^{11} + \alpha^{12} = 1101 + 0011 = 1110 = \alpha^8
\]
we get that
\[
s_2 = \frac{\alpha^8}{\alpha^{11}} = \alpha^{-3} = \alpha^{12}
\]

Since
\[
\begin{vmatrix}
\alpha^7 & \alpha^{13} \\
\alpha^{14} & \alpha^{13}
\end{vmatrix} = \alpha^7\alpha^{13} + \alpha^{14}\alpha^{13} = \alpha^{20} + \alpha^{27} = \alpha^5 + \alpha^{12} = 1011 + 0011 = 1000 = \alpha^3
\]
we get that
\[
s_1 = \frac{\alpha^3}{\alpha^{11}} = \alpha^{-8} = \alpha^7
\]

So the error-locating polynomial is
\[
s(x) = 1 + s_1 x + s_2 x = 1 + \alpha^7 x + \alpha^{12} x^2
\]

Next, we need to find the roots of \(s(x)\). We should find two roots and they should be powers of \(\beta\). Since we really want the reciprocals of the roots, we start
\[
s(\beta^0) = s(1) = 1 + \alpha^7 + \alpha^{12} = 0001 + 0111 + 0011 = 0101 \neq 0
\]
\[
s(\beta^{-1}) = s(\alpha^{-1}) = 1 + \alpha^7\alpha^{-1} + \alpha^{12}\alpha^{-2} = 1 + \alpha^6 + \alpha^{10} = 0001 + 1111 + 1010 = 0100 \neq 0
\]
\[
s(\beta^{-2}) = s(\alpha^{-2}) = 1 + \alpha^7\alpha^{-2} + \alpha^{12}\alpha^{-4} = 1 + \alpha^5 + \alpha^8 = 0001 + 1011 + 1110 = 0100 \neq 0
\]
\[
s(\beta^{-3}) = s(\alpha^{-3}) = 1 + \alpha^7\alpha^{-3} + \alpha^{12}\alpha^{-6} = 1 + \alpha^4 + \alpha^6 = 0001 + 1001 + 1111 = 0111 \neq 0
\]
\[
s(\beta^{-4}) = s(\alpha^{-4}) = 1 + \alpha^7\alpha^{-4} + \alpha^{12}\alpha^{-8} = 1 + \alpha^3 + \alpha^4 = 0001 + 1001 + 1000 = 0000 = 0
\]

So \(\alpha^{-4}\) is a root of \(s(x)\). Since the product of the roots is \(\alpha^{-12}\), we get that \(\alpha^{-8}\) is the other root of \(s(x)\).

Hence
\[
X_1 = \alpha^4 = \beta^4 \quad \text{and} \quad X_2 = \alpha^8 = \beta^8
\]

That means that the first error occurred in the fourth position while the second error occurred in the eight position (recall that we start numbering the position from zero).

Finally, we find the error-sizes \(Y_1\) and \(Y_2\). Since we are working binary, we should find \(Y_1 = Y_2 = 1\). We have to solve
\[
\begin{bmatrix}
\alpha^4 & \alpha^8 \\
\alpha^8 & \alpha^{16} \\
\alpha^{12} & \alpha^{24} \\
\alpha^{16} & \alpha^{32}
\end{bmatrix}
\begin{bmatrix}
Y_1 \\
Y_2
\end{bmatrix}
= \begin{bmatrix}
\alpha^7 \\
\alpha^{14} \\
\alpha^{13} \\
\alpha^{13}
\end{bmatrix}
\]
or
\[
\begin{bmatrix}
\alpha^4 & \alpha^8 \\
\alpha^8 & \alpha \\
\alpha^{12} & \alpha^9 \\
\alpha & \alpha^2
\end{bmatrix}
\begin{bmatrix}
Y_1 \\
Y_2
\end{bmatrix}
= \begin{bmatrix}
\alpha^7 \\
\alpha^{14} \\
\alpha^{14} \\
\alpha^{13}
\end{bmatrix}
\]

A quick check does indeed show that \(Y_1 = Y_2 = 1\):
\[
\alpha^4 + \alpha^8 = 1001 + 1110 = 0111 = \alpha^7
\]
\[
\alpha^8 + \alpha = 1110 + 0010 = 1100 = \alpha^{14}
\]
\[
\alpha^{12} + \alpha^9 = 0011 + 0101 = 0110 = \alpha^{13}
\]
\[
\alpha + \alpha^2 = 0010 + 0100 = 0110 = \alpha^{13}
\]
So the error vector is 

\[ e = 000010001000000 \]

Hence we decode \( y \) as 

\[ y - e = 0 = 111010001000000 \]

2. Put \( \beta = \alpha \) where \( \alpha \) is a primitive element of \( GF(8) \) as defined in the table for \( GF(8) \) in the notes. Consider the binary BCH-code of length 7 with generator polynomial \( \text{lcm}(m_\beta(x), m_{\beta^2}(x)) \). Use the Peterson-Gorenstein-Zierler decoding algorithm to decode the following words:

(a) 1000110
(b) 1000001

**Solution**: Note that \( \delta = 2 + 1 = 3 \) and \( b = 1 \).

(a) Put \( y = 1000110 \). Then \( y(x) = 1 + x^4 + x^5 \).

First, we calculate \( \delta - 1 = 2 \) syndromes. We get

\[ S_1 = y(\beta) = y(\alpha) = 1 + \alpha^4 + \alpha^5 = 001 + 110 + 111 = 000 = 0 \]
\[ S_2 = y(\beta^2) = y(\alpha^2) = 1 + \alpha^8 + \alpha^{10} = 1 + \alpha + \alpha^3 = 001 + 010 + 011 = 000 = 0 \]

Hence \( y \) is a codeword and we decode as \( y \).

(b) Put \( y = 1000001 \). Then \( y(x) = 1 + x^6 \).

First, we calculate \( \delta - 1 = 2 \) syndromes. We get

\[ S_1 = y(\beta) = y(\alpha) = 1 + \alpha^6 = 001 + 101 = 100 = \alpha^2 \]
\[ S_2 = y(\beta^2) = y(\alpha^2) = 1 + \alpha^{12} = 1 + \alpha^5 = 001 + 111 = 110 = \alpha^4 \]

Next, we calculate \( k \), the number of errors that occurred. Since \( \delta = 3 \), we have that \( t = 1 \). So we ‘calculate’

\[ |\alpha^2| = \alpha^2 \neq 0 \]

Hence we assume that \( k = 1 \) : one error occurred.

Next, we find the error-locating polynomial. So we have to solve

\[ \alpha^2 s_1 = \alpha^4 \]

Hence

\[ s_1 = \frac{\alpha^4}{\alpha^2} = \alpha^2 \]

So the error-locating polynomial is

\[ s(x) = 1 + s_1 x = 1 + \alpha^2 x \]

Next, we need to find the roots of \( s(x) \). We easily get that

\[ x = \frac{1}{\alpha^2} = \alpha^{-2} \]

So

\[ X_1 = \alpha^2 = \beta^2 \]

That means that the error occurred in the second position (recall that we start numbering the position from zero).
Finally, we find the error-size $Y_1$. We have to solve

$$\begin{bmatrix} \alpha^2 \\ \alpha^4 \end{bmatrix} \begin{bmatrix} Y_1 \end{bmatrix} = \begin{bmatrix} \alpha^2 \\ \alpha^4 \end{bmatrix}$$

We easily get that

$$Y_1 = \frac{\alpha^2}{\alpha^2} = \frac{\alpha^4}{\alpha^4} = 1$$

So the error vector is

$$\mathbf{e} = 0010000$$

Hence we decode $\mathbf{y}$ as

$$\mathbf{y} - \mathbf{e} = 1010001$$

3. Put $\beta = \alpha^3$ where $\alpha$ is a primitive element of $GF(16)$ as defined in the table for $GF(16)$ in the notes. Then $GF(4) = \{0, 1, \alpha^5, \alpha^{10}\}$ is a subfield of $GF(16)$. Consider the BCH-code of length 5 over $GF(4)$ with generator polynomial lcm($m_{\beta^2}(x), m_{\beta^3}(x)$). So $b = 2$.

(a) What is the dimension of this code?

(b) What is the designed distance of this code?

(c) Use the Peterson-Gorenstein-Zierler decoding algorithm to decode the word $\mathbf{y} = 1\alpha^5100$

Solution: (a) The cyclotomic cosets depending on $n = 5$ and $q = 4$ are

$$\{0\}, \{1, 4\} \text{ and } \{2, 3\}$$

Hence

$$m_{\beta^2}(x) = m_{\beta^3}(x) = (x - \beta^2)(x - \beta^3)$$

and

$$g(x) = \text{lcm}(m_{\beta^2}(x), m_{\beta^3}(x)) = (x - \beta^2)(x - \beta^3)$$

So $\deg(g(x)) = 2$ and thus

$$\dim(C) = n - \deg(g(x)) = 5 - 2 = 3$$

(b) Since $g(x) = \text{lcm}(m_{\beta^2}(x), m_{\beta^3}(x))$, we have that $\delta = 2 + 1 = 3$.

(c) Note that $y(x) = 1 + \alpha^5x + x^2$.

First, we calculate $\delta - 1 = 2$ syndromes. We get

$$S_1 = y(\beta^2) = y(\alpha^6) = 1 + \alpha^{11} + \alpha^{12} = 0001 + 1101 + 0011 = 1111 = \alpha^6$$

$$S_2 = y(\beta^3) = y(\alpha^9) = 1 + \alpha^{14} + \alpha^{18} = 1 + \alpha^{14} + \alpha^3 = 0001 + 1100 + 1000 = 0101 = \alpha^9$$

Next, we calculate $k$, the number of errors that occurred. Since $\delta = 3$, we have that $t = 1$. So we ‘calculate’

$$|\alpha^6| = \alpha^6 \neq 0$$

Hence we assume that $k = 1$ : one errors occurred.

Next, we find the error-locating polynomial. So we have to solve

$$\alpha^6 s_1 = \alpha^9$$
Hence

\[ s_1 = \frac{\alpha^9}{\alpha^5} = \alpha^3 \]

So the error-locating polynomial is

\[ s(x) = 1 + s_1x = 1 + \alpha^3x \]

Next, we need to find the roots of \( s(x) \). We easily get that

\[ x = \frac{1}{\alpha^3} = \alpha^{-3} \]

So

\[ X_1 = \alpha^3 = \beta^1 \]

That means that the error occurred in the first position (recall that we start numbering the position from zero).

Finally, we find the error-size \( Y_1 \). We have to solve

\[
\begin{bmatrix}
\alpha^6 \\
\alpha^9
\end{bmatrix} \begin{bmatrix} Y_1 \end{bmatrix} = \begin{bmatrix} \alpha^6 \\
\alpha^9
\end{bmatrix}
\]

We easily get that

\[ Y_1 = \frac{\alpha^6}{\alpha^5} = \frac{\alpha^9}{\alpha^5} = 1 \]

So the error vector is

\[ e = 01000 \]

Hence we decode \( y \) as

\[ y - e = 1\alpha^5100 - 01000 = 1\alpha^{16}100 \]

since \( \alpha^5 - 1 = 1011 + 0001 = 1010 = \alpha^{10} \).

4. Let \( \alpha \) be a primitive element of \( GF(32) \) as defined in the table for \( GF(32) \) in the notes.

Find polynomials \( u(x), v(x) \in GF(32)[x] \) such that \( \gcd(x^7 + \alpha, x^5 + \alpha^2) = u(x)(x^7 + \alpha) + v(x)(x^5 + \alpha^2) \).

**Solution**: We use the Euclidean Algorithm. We get

\[
\begin{array}{ccc}
1 & 0 & x^7 + \alpha \\
0 & 1 & x^5 + \alpha^2 \\
1 & x^2 & \alpha^{29}x^3 + \alpha^{28}x \\
\alpha^{29}x^5 + \alpha^{28}x^3 + 1 & \alpha^2x^2 + \alpha & \alpha^{29}x + \alpha^2 \\
\alpha^2x^4 + \alpha^6x^3 + \alpha x^2 + \alpha^5x + 1 & \alpha^2x^6 + \alpha^6x^5 + \alpha x^4 + \alpha^5x^3 + x^2 + \alpha^4x + \alpha^8 & \alpha^{17}
\end{array}
\]

because

(1) \( x^7 + \alpha = (x^5 + \alpha^2)x^2 + (\alpha^2x^2 + \alpha) \)

(2) \( x^5 + \alpha^2 = (\alpha^2x^2 + \alpha)(\alpha^{29}x + \alpha^2) + (\alpha^{29}x + \alpha^2) \)

(3) \( \alpha^{29}x^2 + \alpha = (\alpha^{29}x + \alpha^2)(\alpha^4x + \alpha^8) + \alpha^{17} \)

(4) \( \alpha^{29}x + \alpha^2 = \alpha^{17}(\alpha^{12}x + \alpha^{16}) + 0 \)

Hence we get that

\[ \alpha^{17} = (\alpha^2x^4 + \alpha^6x^3 + \alpha x^2 + \alpha^5x + 1)(x^7 + \alpha) + (\alpha^2x^6 + \alpha^6x^5 + \alpha x^4 + \alpha^5x^3 + x^2 + \alpha^4x + \alpha^8)(x^5 + \alpha^2) \]

Since the greatest common divisor of polynomials is monic, we divide both sides by \( \alpha^{17} \) to get

\[
\gcd(x^7 + \alpha, x^5 + \alpha^2) = 1 = \frac{1}{\alpha^{17}}(\alpha^{10}x^4 + \alpha^{20}x^3 + \alpha^{15}x^2 + \alpha^{19}x + \alpha^{14})(x^7 + \alpha) + \\
\frac{1}{\alpha^{17}}(\alpha^{10}x^6 + \alpha^{20}x^5 + \alpha^{15}x^4 + \alpha^{19}x^3 + \alpha^{14}x^2 + \alpha^{18}x + \alpha^{22})(x^5 + \alpha^2)
\]