EEC269A Homework 6 Solution

1. Problem 1

$GF(2^5)$ is constructed by a primitive polynomial $p(X) = 1 + X^2 + X^5$.
Due to $t = 3$,

$$g(x) = LCM\phi_1(X), \phi_3(X), \phi_5(X).$$

Then,

$$\phi_1(X) = p(X) = 1 + X^2 + X^5,$$
$$\phi_3(X) = (X + \alpha^3)(X + \alpha^6)(X + \alpha^{12})(X + \alpha^{24})(X + \alpha^{17}) = X^5 + X^4 + X^3 + X^2 + 1,$$
$$\phi_5(X) = (X + \alpha^5)(X + \alpha^{10})(X + \alpha^{20})(X + \alpha^9)(X + \alpha^{18}) = X^5 + X^4 + X^2 + X + 1.$$

$\phi_1(X)$ is a primitive polynomial. $\phi_3(X)$ and $\phi_5(X)$ are irreducible polynomials, so

$$g(X) = \phi_1(X) \cdot \phi_3(X) \cdot \phi_5(X) = X^{15} + X^{11} + X^{10} + X^9 + X^7 + X^6 + X^3 + X^2 + 1$$

Then the degree of $g(X)$ is 15, $n = 2^5 - 1 = 31$, so $k = 16$.

2. Problem 2

The minimal polynomial of $\beta = \alpha^7$ is $X^4 + X^3 + 1$.
The minimal polynomial of $\beta = \alpha^{14}$ is $X^4 + X^3 + 1$.
The minimal polynomial of $\beta = \alpha^6$ is $X^4 + X^3 + X^2 + X + 1$.
The minimal polynomial of $\beta = \alpha^{13}$ is $X^4 + X^3 + 1$.

$$g(X) = LCM\{X^4 + X^3 + 1, X^4 + X^3 + 1, X^4 + X^3 + X^2 + X + 1, X^4 + X^3 + 1\}$$
$$= (X^4 + X^3 + 1)(X^4 + X^3 + X^2 + X + 1)$$
$$= X^8 + X^4 + X^2 + X + 1.$$
3. Problem 3

\[ r = (010000111011000), \]
\[ r \cdot H^T = (0101, 0101). \]
Then \( S_1 = \alpha^9, S_2 = (S_1)^2 = \alpha^3, S_3 = \alpha^9, S_4 = (S_2)^2 = \alpha^6 \)

4. Problem 4 \( r = (010000000001000). \)

Then \( r(X) = X + X^{11} \).
\( S_1 = r(\alpha) = \alpha + \alpha^{11} = \alpha^6, \)
\( S_2 = (S_1)^2 = \alpha^{12}, \)
\( S_3 = r(\alpha^3) = \alpha^3 + \alpha^3 = 0, \)
\( S_4 = (S_2)^2 = \alpha^9, \)
\( S_5 = r(\alpha) = \alpha^5 + \alpha^{10} = 1, \)
\( S_6 = (S_3)^2 = 0, \)

\[
\begin{array}{|c|c|c|c|c|}
\hline
\mu & & d_\mu & l_\mu & \mu - l_\mu \\
\hline
-1 & 1 & 1 & 0 & -1 \\
0 & 1 & 0 & 0 & \\
1 & 1 + \alpha^6X & 0 & 1 & 0 \\
2 & 1 + \alpha^6X & \alpha^3 & 1 & 1 \\
3 & 1 + \alpha^6X + \alpha^{12}X^2 & 0 & 2 & 1 \\
4 & 1 + \alpha^6X + \alpha^{12}X^2 & 0 & 2 & 2 \\
5 & 1 + \alpha^6X + \alpha^{12}X^2 & 0 & 2 & 3 \\
6 & 1 + \alpha^6X + \alpha^{12}X^2 & & & \\
\hline
\end{array}
\]

\( d_1 = S_2 + \sigma_1^{(1)}(X) S_1 = \alpha^{12} + \alpha^6 \cdot \alpha^6 = 0 \)
\( d_2 = S_3 + \sigma_1^{(2)}(X) S_2 = 0 + \alpha^6 \cdot \alpha^{12} = \alpha^3, \)
\( d_3 = S_4 + \sigma_1^{(3)}(X) S_3 + \sigma_2^{(3)} S_2 = \alpha^9 + \alpha^6 \cdot 0 + \alpha^{12} \cdot \alpha^{12} = 0 \)
\( d_4 = S_5 + \sigma_1^{(4)}(X) S_4 + \sigma_2^{(4)} S_3 = 1 + \alpha^6 \cdot \alpha^9 + \alpha^{12} \cdot 0 = 0 \)
\( d_5 = S_6 + \sigma_1^{(5)}(X) S_5 + \sigma_2^{(5)} S_4 = 0 + \alpha^6 \cdot 1 + \alpha^{12} \cdot \alpha^9 = 0 \)

\( \sigma(X) = 1 + \alpha^6X + \alpha^{12}X^2. \) The roots are \( \alpha^4 \) and \( \alpha^{14} \), so \( \beta_1 = \alpha^{11} \) and \( \beta_2 = \alpha. \)

Then,
\[
\sigma(X) = 1 + \alpha^6X + \alpha^{12}X^2
\]
\[
e(X) = X + X^{11}
\]
\[
v(X) = r(X) + e(X) = 0 = (00000000000000)
\]