Chapter 8

BCH Codes

8.1 Definitions

We defined the least common multiple \( \text{lcm}(f_1(x), f_2(x)) \) of two nonzero polynomials \( f_1(x), f_2(x) \in \mathbb{F}_q[x] \) to be the monic polynomial of the lowest degree which is a multiple of both \( f_1(x) \) and \( f_2(x) \). Suppose we have \( t \) nonzero polynomials \( f_1(x), f_2(x), \ldots, f_t(x) \in \mathbb{F}_q[x] \). The least common multiple of \( f_1(x), \ldots, f_t(x) \) is the monic polynomial of the lowest degree which is a multiple of all of \( f_1(x), \ldots, f_t(x) \), denoted by \( \text{lcm}(f_1(x), \ldots, f_t(x)) \).

It can be proved that the least common multiple of the nonzero polynomials \( f_1(x), f_2(x), f_3(x) \) is the same as \( \text{lcm}(\text{lcm}(f_1(x), f_2(x)), f_3(x)) \) By induction, one can prove that the least common multiple of the polynomials \( f_1(x), f_2(x), \ldots, f_t(x) \) is the same as \( \text{lcm}(\text{lcm}(f_1(x), \ldots, f_{t-1}(x)), f_t(x)) \).

Lemma 8.1. Let \( f(x), f_1(x), f_2(x), \ldots, f_t(x) \) be nonzero polynomials over \( \mathbb{F}_q \). If nonzero polynomial \( f(x) \) is divisible by every polynomial \( f_i(x) \) for \( i = 1, 2, \ldots, t \), then \( f(x) \) is divisible by \( \text{lcm}(f_1(x), f_2(x), \ldots, f_t(x)) \) as well.

Definition 8.2 (BCH codes). Let \( \alpha \) be an element of order \( n \) in a finite field \( \mathbb{F}_{q^m} \). A BCH code of length \( n \) and design distance \( d \) is a cyclic code generated by the least common multiple of minimal polynomials in \( \mathbb{F}_q[x] \) of the elements \( \alpha, \alpha^2, \ldots, \alpha^{d-1} \).

Remark. 1) Since \( n|q^m - 1 \), then we have \( \text{gcd}(n, q) = 1 \).

2) In this course, we focus on the case \( n = q^m - 1 \) then \( \alpha \) is a primitive element of field \( \mathbb{F}_{q^m} \). The resulting BCH code is known as a primitive BCH code.
Example 8.1. Let $\alpha \in F_8$ be a root of $1 + x + x^3 \in F_2[x]$. Then it is a primitive element of $F_8 = F_2[\alpha]$. The polynomials $M^{(1)}(x)$ and $M^{(2)}(x)$ are both equal to $1 + x + x^3$. Hence, a narrow-sense binary BCH code of length 7 generated by $\text{lcm}(M^{(1)}(x), M^{(2)}(x)) = 1 + x + x^3$ is a $[7, 4]$-code. In fact, it is a binary $[7, 4, 3]$-Hamming code.

Lecture 24, April 7, 2011

Remark. For $t \geq 1$, $t$ and $2t$ belong to the same cyclotomic coset of 2 modulo $2^m - 1$. This is equivalent to the fact that $M^{(t)}(x) = M^{(2t)}(x)$. Therefore,

$$\text{lcm}(M^{(1)}(x), \ldots, M^{(2t-1)}(x)) = \text{lcm}(M^{(1)}(x), \ldots, M^{(2t)}(x))$$

i.e., the primitive binary BCH codes of length $2^m - 1$ with designed distance $2t + 1$ are the same as the primitive binary BCH codes of length $2^m - 1$ with designed distance $2t$.

In this course, we focus on primitive BCH codes. Now let’s discuss Parameters of BCH codes. The length of a primitive BCH code is clearly $q^m - 1$. For the rest of this subsection, we study the minimum distance of BCH codes.

Lemma 8.3. Let $C$ be a $q$-ary cyclic code of length $n$ with generator polynomial $g(x)$. Suppose $\alpha_1, \ldots, \alpha_r$ are all the roots of $g(x)$ and the polynomial $g(x)$ has no multiple roots. Then an element $u(x)$ of $R^n_q = F_q[x]/(x^n - 1)$ is a codeword of $C$ if and only if $u(\alpha_i) = 0$ for all $i = 1, \ldots, r$.

Proof. If $u(x)$ is a codeword of $C = \langle g(x) \rangle$, then there exists a polynomial $f(x)$ such that $u(x) = g(x)f(x)$. Thus, we have $u(\alpha_i) = g(\alpha_i)f(\alpha_i) = 0$ for all $i = 1, \ldots, r$.

Conversely, if $u(\alpha_i) = 0$ for all $i = 1, \ldots, r$, then $u(x)$ is divisible by $g(x)$ since $g(x)$ has no multiple roots. This means that $u(x)$ is a codeword of $C$. \qed

Theorem 8.1 (Vandermonde Determinants). For $t \geq 2$ the $t \times t$ Vandermonde matrix

$$G = \begin{bmatrix}
1 & 1 & \cdots & 1 \\
e_1 & e_2 & \cdots & e_t \\
e_1^2 & e_2^2 & \cdots & e_t^2 \\
p & \vdots & \vdots & \vdots \\
_1 & e_2^{t-1} & \cdots & e_t^{t-1}
\end{bmatrix}$$

has determinant $\prod_{1 \leq j < i \leq t} (e_i - e_j)$. 
**Theorem 8.2.** A BCH code with designed distance $d$ has minimum distance at least $d$.

**Proof.** Let $\alpha$ be a primitive element of $F_{p^m}$ and let $C$ be a BCH code generated by $g(x) = \text{lcm}(M^{(1)}(x), \ldots, M^{(d-1)}(x))$. It is clear that the elements $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ are roots of $g(x)$.

Suppose that the minimum distance $r$ of $C$ is less than $d$. Then there exists a nonzero codeword $u(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ such that $\text{wt}(u(x)) = r < d$. By proof of Lemma 8.5, we have $u(\alpha^i) = 0$ for all $i = 1, \ldots, d-1$ i.e.,

$$
\begin{bmatrix}
1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\
1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{n-1} \\
1 & \alpha^3 & (\alpha^3)^2 & \cdots & (\alpha^3)^{n-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \alpha^{d-1} & (\alpha^{d-1})^2 & \cdots & (\alpha^{d-1})^{n-1}
\end{bmatrix}
\begin{bmatrix}
a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1}
\end{bmatrix} = 0.
$$

Let $R = \{i_1, \ldots, i_r\}$ such that $0 \leq i_1 < i_2 < \cdots < i_r \leq n-1$ and $c_j \neq 0$ if and only if $j \in R$. Then we have

$$
\begin{bmatrix}
(\alpha)^{i_1} & (\alpha)^{i_2} & (\alpha)^{i_3} & \cdots & (\alpha)^{i_r} \\
(\alpha^2)^{i_1} & (\alpha^2)^{i_2} & (\alpha^2)^{i_3} & \cdots & (\alpha^2)^{i_r} \\
(\alpha^3)^{i_1} & (\alpha^3)^{i_2} & (\alpha^3)^{i_3} & \cdots & (\alpha^3)^{i_r} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
(\alpha^{d-1})^{i_1} & (\alpha^{d-1})^{i_2} & (\alpha^{d-1})^{i_3} & \cdots & (\alpha^{d-1})^{i_r}
\end{bmatrix}
\begin{bmatrix}
a_{i_1} \\ a_{i_2} \\ a_{i_3} \\ \vdots \\ a_{i_r}
\end{bmatrix} = 0.
$$

Since $r \leq d-1$, we obtain the following system of equations by choosing the first $r$ equations of the above system of equations:

$$
\begin{bmatrix}
(\alpha)^{i_1} & (\alpha)^{i_2} & (\alpha)^{i_3} & \cdots & (\alpha)^{i_r} \\
(\alpha^2)^{i_1} & (\alpha^2)^{i_2} & (\alpha^2)^{i_3} & \cdots & (\alpha^2)^{i_r} \\
(\alpha^3)^{i_1} & (\alpha^3)^{i_2} & (\alpha^3)^{i_3} & \cdots & (\alpha^3)^{i_r} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
(\alpha^{d-1})^{i_1} & (\alpha^{d-1})^{i_2} & (\alpha^{d-1})^{i_3} & \cdots & (\alpha^{d-1})^{i_r}
\end{bmatrix}
\begin{bmatrix}
a_{i_1} \\ a_{i_2} \\ a_{i_3} \\ \vdots \\ a_{i_r}
\end{bmatrix} = 0.
$$

The determinant $D$ of the coefficient matrix of the above equation is equal to

$$
\prod_{j=1}^{r} \alpha^{i_j} \det \begin{bmatrix}
1 & 1 & 1 & \cdots & 1 \\
(\alpha)^{i_1} & (\alpha)^{i_2} & (\alpha)^{i_3} & \cdots & (\alpha)^{i_r} \\
(\alpha^2)^{i_1} & (\alpha^2)^{i_2} & (\alpha^2)^{i_3} & \cdots & (\alpha^2)^{i_r} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
(\alpha^{d-1})^{i_1} & (\alpha^{d-1})^{i_2} & (\alpha^{d-1})^{i_3} & \cdots & (\alpha^{d-1})^{i_r}
\end{bmatrix} = \prod_{j=1}^{r} \alpha^{i_j} \prod_{1 \leq i < k \leq r} (\alpha^k - \alpha^i) \neq 0.
$$

Combining these, we obtain $(a_{i_1}, a_{i_2}, a_{i_3}, \ldots, a_{i_r}) = 0$. This is a contradiction. \qed
**Example 8.2.** Let $\alpha$ be a root of $1 + x + x^4 \in F_2[x]$. Then $\alpha$ is a primitive element of $F_{16}$. Consider the primitive binary BCH code of length 15 with designed distance 7. Then the generator polynomial is

$$g(x) = \text{lcm}(M^{(1)}(x), \ldots, M^{(6)}(x)) = M^{(1)}(x)M^{(3)}(x)M^{(5)}(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}.$$  

Therefore, $d(C) \leq \text{wt}(g(x)) = 7$. On the other hand, we have, by Theorem 8.3, that $d(C) \geq 7$. Hence, $d(C) = 7$.

### 8.2 Decoding of BCH codes

Suppose $\alpha$ is a primitive element of field $F_{q^m}$. Let $C$ be a primitive $q$-ary BCH code of length $n = q^m - 1$ and design distance $d$. Set

$$H = \begin{bmatrix}
1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1}
1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{n-1}
1 & \alpha^3 & (\alpha^3)^2 & \cdots & (\alpha^3)^{n-1}
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \alpha^{d-1} & (\alpha^{d-1})^2 & \cdots & (\alpha^{d-1})^{n-1}
\end{bmatrix}$$

Then

$$u(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in C \subset R_q^n \iff H \begin{bmatrix} a_0 \\
a_1 \\
a_2 \\
\vdots \\
a_{n-1} \end{bmatrix} = \begin{bmatrix} u(\alpha) \\
u(\alpha^2) \\
u(\alpha^3) \\
\vdots \\
u(\alpha^{d-1}) \end{bmatrix} = 0.$$

In decoding rule of BCH codes, for any word $u = (a_0, a_1, \ldots, a_{n-1}) \in F_q^n$ we define the syndrome $S(u)$ of $u$ as $S(u) = H u^t$.

The decoding procedure for $C$ is now as follows: Suppose a vector $f$ is received, which we think of as a polynomial of degree $< n$. We assume that $d = 2t + 1$ is odd. We need to compute the error vector $e$.

1). **Compute the syndromes:** $S_1 = f(\alpha), S_2 = f(\alpha^2), \ldots, S_{d-1} = f(\alpha^{d-1})$. These are elements of $F_{q^m}$.
2). If all of the $S_i$ are zero, $f$ is a codeword. Otherwise, for $k = 1, 2, 3, \ldots, t$ consider

$$M_k = \begin{bmatrix}
S_1 & S_2 & \cdots & S_k \\
S_2 & S_3 & \cdots & S_{k+1} \\
\vdots & \vdots & \ddots & \vdots \\
S_k & S_{k+1} & \cdots & S_{2k-1}
\end{bmatrix}$$

This is a $k \times k$ matrix with entries in $F_{q^m}$.

Find the maximum value $k$ such that $\det M_k \neq 0$. We think of $k$ as the number of errors that occurred. It is potentially possible that $\det M_k = 0$ for all $k$ but some $S_i$ are nonzero nevertheless. In this case more than $t$ errors occurred, and we have to seek retransmission.

We assume that $k$ is the number of errors that actually occurred.

3). Solve the following system of linear equations (over $F_{q^m}$):

$$M_k b = -S$$

with indeterminate $b$ and coefficient matrix $S$

$$b = \begin{bmatrix}
b_k \\
b_{k-1} \\
\vdots \\
b_1
\end{bmatrix}, \quad S = \begin{bmatrix}
S_{k+1} \\
S_{k+2} \\
\vdots \\
S_{2k}
\end{bmatrix}$$

The solution to this system gives us the **error locator polynomial**

$$\sigma(x) = b_k x^k + b_{k-1} x^{k-1} + \cdots + b_1 x + 1.$$ 

The coefficients $b_i$ of $\sigma(x)$ are elements of $F_{q^m}$ in general, and need not be elements of $F_q$.

4). **Find the roots of the error locator polynomial.** $\sigma(x)$ must have precisely $k$ distinct roots $\beta_1, \beta_2, \ldots, \beta_k$ unless more than $k$ errors occurred. Again, the roots are in $F_{q^m}$. If the roots do not exist, then we have to seek retransmission.

5). **Compute the error locations:** First compute $\alpha_i = \beta_i^{-1}$. Now find $l_1, l_2, \ldots, l_k$ such that $\alpha_i = \alpha^{l_i}$. Notice that the $l_i$ are unique as long as we require $0 \leq l_i < n = q^m - 1$.

We now have worked our way to an **error vector** of the form

$$e(x) = e_1 x^{l_1} + e_2 x^{l_2} + \cdots + e_k x^{l_k}$$

We therefore conjecture the error locations to be $l_1, l_2, \ldots, l_k$. 
6). **Determine the values of** \( e_1, e_2, \ldots, e_k \). Solve the equations

\[
S_i = e_1(\alpha^i) + e_2(\alpha^{i^2}) + \cdots + e_k(\alpha^{i^k}) \quad (i = 1, 2, \ldots, 2k)
\]

for the \( e_j \) in \( F_q \). (Notice that often not all \( 2^k \) equations are needed to determine the \( e_i \) because each single equation corresponds to multiple linear equations over \( F_q \), but you still need to check all \( 2^k \) equations hold).

It could potentially happen that the \( e_i \) computed in this manner are not elements of \( F_q \) but are in \( F_{q^m} \) rather. In this case, decoding is not possible, because of course our error vector must have coefficients in \( F_q \).

7). **Check for consistency.** Check that \( S_i = e(\alpha^i) \) for \( i = 2k + 1, 2k + 2, \ldots, 2t = d - 1 \). If this fails for any \( i \), more than \( t \) errors occurred, and decoding is not possible.

8). **Celebrate.** We are done. The decoded codeword is now \( u = f - e \).

**Lecture 25, April 12, 2011**

We focus on primitive BCH codes:

Let \( \alpha \) be a primitive element of \( F_{q^m} \). A BCH code \( C \) of length \( n = q^m - 1 \) and design distance \( d \) is a cyclic code generated by the least common multiple of minimal polynomials in \( F_q[x] \) of the elements \( \alpha, \alpha^2, \ldots, \alpha^{d-1} \).

\[
C = \langle g(x) \rangle, \quad \text{where} \quad g(x) = \text{lcm}(M^{(1)}(x), \ldots, M^{(d-1)}(x)).
\]

**Fact.** Let \( \alpha \) be a primitive element of \( F_{q^m} \) and \( C \) be a \( q \)-ary primitive BCH code of length \( n = q^m - 1 \) with design distance \( d \). Then we have

\[
C = \{ u(x) \in R_q^n = F_q[x]/(x^n - 1) \mid u(\alpha^i) = 0 \text{ for all } i = 1, 2, \ldots, d - 1 \}.\]

**Theorem 8.1.** A BCH code with designed distance \( d \) has minimum distance at least \( d \). \( \square \)

**Example 8.3.** Let \( \alpha \) be a root of \( 1 + x + x^3 \in F_2[x] \) and \( C \) be the binary primitive BCH code of length 7 with designed distance \( 3 = 2 \times 1 + 1 \). Note \( \alpha \) is a primitive element \( F_8 = F_2[x]/(1 + x + x^3) \). Indeed all elements in \( F_2[\alpha] \) can be expressed as powers of \( \alpha \):

\[
F_8 = \{ 0, 1, \alpha, \alpha^2, \alpha^3 = \alpha + 1, \alpha^4 = \alpha^2 + \alpha, \alpha^5 = \alpha^2 + \alpha + 1, \alpha^6 = \alpha^2 + 1 \}.
\]

Suppose a vector \( u = (1, 0, 0, 1, 1, 0, 0) \) is received, then the corresponding polynomial is \( u(x) = 1 + x^3 + x^4 \).
1). **Compute the syndromes:**

\[ S_1 = u(\alpha) = 1 + \alpha^3 + \alpha^4 = 1 + \alpha + 1 + \alpha^2 + \alpha = \alpha^2, \]
\[ S_2 = u(\alpha^2) = 1 + \alpha^6 + \alpha^8 = 1 + \alpha^2 + 1 + \alpha = \alpha + \alpha^2. \]

2). Notice that \( t = 1 \) and \( \det M_1 = S_1 = \alpha^2 \neq 0 \). We assume that 1 error occurred.

3). Solve the following system of linear equations (over \( F_{q^m} \)):

\[ M_k b = -S, \text{ i.e., } S_1 b_1 = -S_2. \]

We get \( b_1 = \alpha^{-2}(\alpha^2 + \alpha) = \alpha^5(\alpha^2 + \alpha) = 1 + \alpha^6 = 1 + \alpha^2 + 1 = \alpha^2. \) Thus the error locator polynomial is

\[ \sigma(x) = b_k x^k + b_{k-1} x^{k-1} + \cdots + b_1 x + 1 = b_1 x + 1 = \alpha^2 x + 1. \]

4). **Find the roots of the error locator polynomial:** Obviously \( \sigma(x) \) has just one root, namely, \(-\alpha^{-2} = \alpha^5\). Thus \( \beta_1 = \alpha^5 \).

5). **Compute the error locations:** \( \alpha_1 = \beta^{-1} = \alpha^2. \) Hence we have \( l_1 = 2 \) such that \( \alpha_1 = \alpha^{l_1} \).

6). **Determine the values of** \( e_1, e_2, \ldots, e_k \): The error vector \( e(x) = e_1 x^2 \). we need to compute \( e_1 \). Solve the equations

\[ S_1 = e_1 \alpha^2 \text{ and } S_2 = e_1(\alpha^2)^2 = e_1 \alpha^4 = e_1(\alpha^2 + \alpha). \]

We get \( e_1 = 1 \).

7). **Check for consistency:** Since \( t = k \) so we do not need to check.

8). **Celebrate:** We are done. The decoded codeword is now \( u(x) - e(x) = 1 + x^2 + x^3 + x^4 = (1 + x)(1 + x + x^3) \in C. \)

**Example 8.4.** Let \( \alpha \) be a root of \( 2 + x + x^2 \in F_3[x] \) and \( C \) be the ternary primitive BCH code of length 8 with designed distance \( d = 5 = 2 \times 2 + 1 \). So here \( m = 2, q = 3 \) and \( t = 2 \). Note \( \alpha \) is a primitive element \( F_9 = F_3[x]/(2 + x + x^2) \). Indeed all elements in \( F_3[\alpha] \) can be expressed as powers of \( \alpha \):

\[ F_9 = \{0, 1, \alpha, \alpha^2 = 1 + 2\alpha, \alpha^3 = 2\alpha + 2, \alpha^4 = 2, \alpha^5 = 2\alpha, \alpha^6 = 2 + \alpha, \alpha^7 = \alpha + 1\}. \quad (8.1) \]

Suppose a vector \( u = (2, 0, 1, 1, 1, 1, 0, 0) \) is received, then the corresponding polynomial is \( u(x) = 2 + x^2 + x^3 + x^4 + x^5 \). Then
1). \( S_1 = u(\alpha) = 2 + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 = 2 + 1 + 2\alpha + 2\alpha + 2 + 2 + 2\alpha = 1, \)
\( S_2 = u(\alpha^2) = 2 + \alpha^4 + \alpha^6 + \alpha^8 + \alpha^{10} = 2 + 2 + 2 + \alpha + 1 + 1 + 2\alpha = 2, \)
\( S_3 = u(\alpha^3) = 2 + \alpha^6 + \alpha^9 + \alpha^{12} + \alpha^{15} = 2 + 2 + \alpha + \alpha + 2 + \alpha + 1 = 1, \)
\( S_4 = u(\alpha^4) = 2 + \alpha^8 + \alpha^{12} + \alpha^{16} + \alpha^{20} = 2 + 1 + 2 + 1 + 2 = 2. \)
(Note: it is an accident that all syndromes are in \( F_q = \mathbb{Z}_3 \) rather than in \( F_9 \).)

2). Notice that
\[
M_2 = \begin{bmatrix}
1 & 2 \\
2 & 1
\end{bmatrix}
\]
and \( \det(M_2) = 1 - 4 = 0. \) Now we know that either 1 or more than 2 errors occurred. \( M_1 = [1] \), so \( \det M_1 = 1 \neq 0. \) We assume that 1 error occurred.

3). The syndrome equations now take the form \( M_1 b_1 = -S_2 \), or \( b_1 = -2 = 1. \) Thus the error locator polynomial \( \sigma(x) = x + 1. \)

4). \( \sigma(x) \) has just one root \(-1 = 2. \) Thus \( \beta_1 = 2. \)

5). Compute the error locations: \( \alpha_1 = \beta_1^{-1} = 2^{-1} = 2. \) Moreover, we have \( 2 = \alpha^4, \) i.e., \( l_1 = 4. \)

6). The error vector \( e(x) = e_1 x^4. \) we need to compute \( e_1. \) Solve the equations
\[
S_1 = e_1 \alpha^4 = 2e_1 \text{ and } S_2 = e_1 (\alpha^4)^2 = e_1.
\]
We get \( e_1 = 2. \)

7). We need to check \( S_3 = e(\alpha^3) \) and \( S_4 = e(\alpha^4). \) Now the first one follows because \( e(\alpha^3) = 2\alpha^{12} = 2 \times 2 = 1 = S_3. \) The second \( e(\alpha^4) = 2 \times 1 = 2 = S_4. \)

8). Celebrate: We are done. The decoded codeword is now \( u(x) - e(x) = 2 + x^2 + x^3 + 2x^4 + x^5 \in C. \)

**Example 8.5 (k = 2).** Let \( C \) be the same code as above, but this time suppose we receive \( u(x) = x + x^3 + 2x^4 + 2x^5 + x^6. \) Then

1). \( S_1 = u(\alpha) = \alpha + \alpha^3 + 2\alpha^4 + 2\alpha^5 + \alpha^6 = \alpha + 2\alpha + 2 + 1 + \alpha + 2 + \alpha = 2 + 2\alpha = \alpha^3, \)
\( S_2 = u(\alpha^2) = \alpha^2 + \alpha^6 + 2\alpha^8 + 2\alpha^{10} + \alpha^{12} = 1 + 2\alpha + 2 + \alpha + 2 + 2 + \alpha + 2 = \alpha, \)
\( S_3 = u(\alpha^3) = \alpha^3 + \alpha^9 + 2\alpha^{12} + 2\alpha^{15} + \alpha^{18} = 2\alpha + 2 + \alpha + 1 + 2\alpha + 2 + 2\alpha + 1 = \alpha, \)
\( S_4 = u(\alpha^4) = \alpha^4 + \alpha^{12} + 2\alpha^{16} + 2\alpha^{20} + \alpha^{24} = 2 + 2 + 2 + 1 + 1 = 2. \)
2). Notice that
\[ M_2 = \begin{bmatrix} \alpha^3 & \alpha \\ \alpha & \alpha \end{bmatrix} \]
and \( \text{det}(M_2) = \alpha^4 - \alpha^2 = 2 - 2\alpha - 1 = \alpha + 1 = \alpha^7 \neq 0 \). Now we conclude that 2 or more errors occurred. We assume that 2 errors occurred.

3). The syndrome equations is
\[ \begin{bmatrix} \alpha^3 & \alpha \\ \alpha & \alpha \end{bmatrix} \begin{bmatrix} b_2 \\ b_1 \end{bmatrix} = -\begin{bmatrix} \alpha \\ 2 \end{bmatrix} \]
We have
\[ M_2^{-1} = \frac{1}{\alpha^7} \begin{bmatrix} \alpha & -\alpha \\ -\alpha & \alpha^3 \end{bmatrix} = \begin{bmatrix} \alpha^2 & -\alpha^2 \\ -\alpha^2 & \alpha^4 \end{bmatrix} \]
Hence
\[ \begin{bmatrix} b_2 \\ b_1 \end{bmatrix} = -M_2^{-1} \begin{bmatrix} \alpha \\ 2 \end{bmatrix} = -\begin{bmatrix} \alpha^2 & -\alpha^2 \\ -\alpha^2 & \alpha^4 \end{bmatrix} \begin{bmatrix} \alpha \\ 2 \end{bmatrix} = -\begin{bmatrix} \alpha^3 - 2\alpha^2 \\ 1 - \alpha^3 \end{bmatrix} = \begin{bmatrix} 2\alpha \\ 2\alpha + 1 \end{bmatrix} = \begin{bmatrix} \alpha^5 \\ \alpha^2 \end{bmatrix} \]
Thus the error locator polynomial \( \sigma(x) = \alpha^5x^2 + \alpha^2x + 1 \).

4). Find the roots of \( \sigma(x) \): \( \sigma(x) = 0 \), i.e.,
\[ 0 = x^2 + \alpha^5x + \alpha^3 = x^2 + (2\alpha)x + \alpha^3 = (x - \alpha^4)(x - \alpha^7) \]
We conclude that the two roots are \( \beta_1 = \alpha^4 = 2 \) and \( \beta_2 = \alpha^7 \). You can also run through all 9 elements of \( F_9 \) to find out the roots or try the quadratic formula for roots:
\[ \beta_{1,2} = -\frac{-\alpha^5 \pm \sqrt{\alpha^{10} - 4\alpha^3}}{2} = 2^{-1}(\alpha\pm\sqrt{1 + 2\alpha - (2\alpha + 2)}) = 2(\alpha\pm\sqrt{\alpha^4}) = 2(\alpha\pm\alpha^2), \]
i.e., \( \beta_{1,2} = 2\alpha \pm (\alpha + 2) = 2, \alpha + 1 \).

5). Compute the error locations: Now we have \( \alpha_1 = 2^{-1} = 2 = \alpha^4 \) and \( \alpha_2 = (\alpha^7)^{-1} = \alpha \). The supposed error locations are therefore \( l_1 = 4 \) and \( l_2 = 1 \).

6). The error vector \( e(x) = e_1x^4 + e_2x \). we need to compute \( e_1 \) and \( e_2 \). Solve the equations
\[ \alpha^3 = S_1 = e(\alpha) = 2e_1 + \alpha e_2 \]
and
\[ \alpha = S_2 = e(\alpha^2) = e_1 + \alpha^2 e_2 \]
We have
\[ e_1 = \frac{\alpha^4 - \alpha}{2\alpha - 1} = \frac{2 + 2\alpha}{2\alpha + 2} = 1 \]
and
\[ e_2 = \alpha^{-1}(\alpha^3 - 2) = \alpha^{-1}(2\alpha + 2 - 2) = 2. \]
We conclude that \( e(x) = x^4 + 2x \). We also need to check
\[ e(\alpha^3) = \alpha^{12} + 2\alpha^3 = 2 + \alpha + 1 = \alpha = S_3 \]
and
\[ e(\alpha^4) = \alpha^{16} + 2\alpha^4 = 1 + 4 = 2 = S_4. \]

7). We do not have to do any consistency checks, because \( k = t = 2 \).

8). **Celebrate:** We are done. The decoded codeword is now \( u(x) - e(x) = x + x^3 + 2x^4 + 2x^5 + x^6 - (2x + x^4) = 2x + x^3 + x^4 + 2x^5 + x^6 \in C \).

**Note:** always use (8.1) in Example 8.4 to do the computations.