BCH CODES

Mehmet Dagli

November, 2004

Department of Mathematics, Iowa State University,
Ames, Iowa 50011-2064
email: mdagli@iastate.edu
Abstract

How do we modify a Hamming code to correct two errors? In other words, how can we increase its minimum distance from 3 to 5? We will either have to lengthen the code words or eliminate some of them from our code. Correcting two errors in a long word may not be much better than correcting one error in a short one. So we will try to produce a double error correcting subcode of the Hamming code by removing some code words to make a new code. BCH codes is a generalization of Hamming codes for multiple error correction. Binary BCH codes were first discovered by A. Hocquenghem in 1959 and independently by R.C. Bose and D.K. Ray-Chaudhuri in 1960.
Overlook

1. BCH Codes as Subcodes of Hamming Codes
2. BCH Codes as Polynomial Codes
3. BCH Error Correction
1 BCH Codes as Subcodes of Hamming Codes

Recall: Encoder $E$ for a linear binary $(n, m)$-code $C$ is a linear map from $B^m$ to $B^n$.

Definition 1.1 Let $C$ be a linear $(n, m)$-code with encoder $E$. Choose $n \times m$ matrix $G$ so that $E(x) = Gx^T$ for any word $x$ of length $m$. Then $G$ is called a generator matrix of the code $C$.

Definition 1.2 A check matrix for a linear code $C$ over a field $F$ is a $k \times n$ matrix $H$ with the property that for any word $v$ in $F^n$, $Hv^T = 0$ iff $v \in C$. The number $k$ is arbitrary here, but the smallest possible value for $k$ is $n - m$. In terms of linear algebra, $C$ is the null space of $H$. 
**Question**: How do we reduce the set of word of a Hamming code?

“*Introduce further checks, i.e. add new rows to the Hamming check matrix $H$*”.

**Problem**:

i. Additional checks may be a linear combination of the ones that we have. In that case, the set of code words will not be changed.

ii. Although the set of code words may be reduced, the minimum distance may not be increased.

**Trick**: Gather bits together in groups of $k$ and consider the groups to represent the elements of the field $GF(2^k)$.
Example 1.3 Consider the columns of the Hamming check matrix $H_4$ as representing the nonzero elements of $GF(2^4) = B[x]/(x^4 + x^3 + 1)$.

Choose columns of $H_4$ in a decreasing powers of the primitive element 2, then check matrix $H_4$ has the following form:

$$(12 \ 6 \ 3 \ 13 \ 10 \ 5 \ 14 \ 7 \ 15 \ 11 \ 9 \ 8 \ 4 \ 2 \ 1)$$

In binary digits, this matrix is

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

Add further rows of elements of $GF(2^4)$ to extend as simple as possible.
Vandermonde Matrices

**Simplest way:** Choose each entry as a function of the original entry at the head of its column.

**Theorem 1.4** $C$ linear code with check matrix $H$,

Minimum distance of $C > d$ iff no set of $d$ columns of $H$ is linearly independent.

**Definition 1.5** An $n \times n$ Vandermonde matrix $V$

$$
V = V(\lambda_1, \lambda_2, \ldots, \lambda_n) = \\
\begin{pmatrix}
\lambda_1 & \lambda_2 & \cdots & \lambda_n \\
\lambda_1^2 & \lambda_2^2 & \cdots & \lambda_n^2 \\
\vdots & \vdots & \ddots & \vdots \\
\lambda_1^n & \lambda_2^n & \cdots & \lambda_n^n
\end{pmatrix}
$$

**Theorem 1.6** If $\lambda_1, \lambda_2, \ldots, \lambda_n$ are distinct nonzero elements of $F$, the columns of $V = V(\lambda_1, \lambda_2, \ldots, \lambda_n)$ are linearly independent over $F$. 
Extending a Hamming Check Matrix

**Definition 1.8** Define the double error correcting BCH code \( \text{BCH}(k,2) \) to have the check matrix \( V_{k,2} \) with columns

\[
\begin{pmatrix}
\alpha^i \\
\alpha^{2i} \\
\alpha^{3i} \\
\alpha^{4i}
\end{pmatrix}
\]

**Example 1.9** \( V_{4,2} \) has the following form.

\[
\begin{pmatrix}
12 & 6 & 3 & 13 & 10 & 5 & 14 & 7 & 15 & 11 & 9 & 8 & 4 & 2 & 1 \\
6 & 13 & 5 & 7 & 11 & 8 & 2 & 12 & 3 & 10 & 14 & 15 & 9 & 4 & 1 \\
3 & 5 & 15 & 8 & 1 & 3 & 5 & 15 & 8 & 1 & 3 & 5 & 15 & 8 & 1 \\
13 & 7 & 8 & 12 & 10 & 15 & 4 & 6 & 5 & 11 & 2 & 3 & 14 & 9 & 1
\end{pmatrix}
\]

**Verification**: Any different four columns \( V_i, V_j, V_k, V_l \) of \( V_{4,2} \) form a Vandermonde matrix, so \( V_i, V_j, V_k, V_l \) are linearly independent. Hence the code has minimum distance 5 and thus can correct 2 errors.
Further Extension

**Definition 1.11** Define $t$ error-correcting BCH code $\text{BCH}(k, t)$ over the field of order $2^k$ based on $\alpha$, to have the $n \times 2t$ check matrix $V_{k,t}$, where $n = 2^k - 1$.

Number the columns $V_i$ of $V_{k,t}$ from 0 to $n - 1$, counting from the right. Then for $i = 0, 1, \ldots, n - 1$, $V_i$ is defined by the formula

\[
\begin{pmatrix}
\alpha^i \\
\alpha^{2i} \\
\alpha^{2ti} \\
\end{pmatrix}
\]

The block length of the code: $n = 2^k - 1$.

For a code to have minimum distance greater than $2t$ we must have $2t < n$.

Hence this definition makes sense for $t < 2^{k-1}$.
Example 1.12 The columns of the check matrix $V_{4,3}$ of BCH(4,3) are of the form

\[
\begin{pmatrix}
2^i \\
2^{2i} \\
2^{6i}
\end{pmatrix}
\]

where $i = 14, 13, \ldots, 0$ and the complete matrix is

\[
\begin{pmatrix}
12 & 6 & 3 & 13 & 10 & 5 & 14 & 7 & 15 & 11 & 9 & 8 & 4 & 2 & 1 \\
6 & 13 & 5 & 7 & 11 & 8 & 2 & 12 & 3 & 10 & 14 & 15 & 9 & 4 & 1 \\
3 & 5 & 15 & 8 & 1 & 3 & 5 & 15 & 8 & 1 & 3 & 5 & 15 & 8 & 1 \\
13 & 7 & 8 & 12 & 10 & 15 & 4 & 6 & 5 & 11 & 2 & 3 & 14 & 9 & 1 \\
10 & 11 & 1 & 10 & 11 & 1 & 10 & 11 & 1 & 10 & 11 & 1 & 10 & 11 & 1 \\
5 & 8 & 3 & 15 & 1 & 5 & 8 & 3 & 15 & 1 & 5 & 8 & 3 & 15 & 1
\end{pmatrix}
\]

$V_{4,3}$ can also be written in binary form as a $24 \times 15$ matrix, in which each column consists of the binary representations of the elements of $GF(2^4)$ in the matrix above.
The Reduced Check Matrix

The matrix $V_{k,t}$ contains many redundant rows for it to be a practical check.

In fields of characteristic 2, squaring is a linear function and we know that any row of a check matrix that is a linear function of the other rows is redundant.

**Definition 1.13** The matrix $H_{k,t}$ obtained from $V_{k,t}$ by deleting the even-numbered rows is called the reduced check matrix of BCH($k, t$). The rows of $H_{k,t}$ will be numbered with the same indices as in $V_{k,t}$.

**Example 1.14** The reduced check matrix $H_{4,3}$ of BCH(4,3) is

$$
\begin{pmatrix}
12 & 6 & 3 & 13 & 10 & 5 & 14 & 7 & 15 & 11 & 9 & 8 & 4 & 2 & 1 \\
3 & 5 & 15 & 8 & 1 & 3 & 5 & 15 & 8 & 1 & 3 & 5 & 15 & 8 & 1 \\
10 & 11 & 1 & 10 & 11 & 1 & 10 & 11 & 1 & 10 & 11 & 1 & 10 & 11 & 1
\end{pmatrix}
$$
Proposition 1.15 $H_{k,t}$ and $V_{k,t}$ are check matrices of the same code BCH($k$, $t$).

proof. Let $w = (w_{14}, w_{13}, ..., w_0)$ be a code word of $C$ defined by $H_{k,t}$, then $H_{k,t} w^T = 0$. For all odd $k < 2t$ express this product with the equations

$$\sum_{i=0}^{14} w_i \alpha^{ik} = 0$$

For all $i$, $w_i^2 = w_i$, so by squaring this previous equation we find

$$\sum_{i=0}^{14} w_i \alpha^{2ik} = 0$$

for all $k$. But this states that $V_{k,t} w^T = 0$. Hence $w$ is a code word of BCH($k$, $t$). Since the rows of $H_{k,t}$ are a subset of $V_{k,t}$, any code word of BCH($k$, $t$) must be a code word of $C$. Thus two codes are equal.
**Theorem 1.16** BCH($k$, $t$) has a block length $n = 2^k - 1$.

**Theorem 1.17** It has minimum distance at least $2t + 1$, so it can correct all error patterns of weight at most $t$.

*proof.* Assumption: No $2t$ columns of $V_{k,t}$ are linearly independent. Choose $2t$ columns $V_{i(1)}, V_{i(2)}, \ldots, V_{i(2t)}$, and consider the matrix formed by these columns. Denoting the power $\alpha^i(k)$ by $\alpha_k$, we have the following Vandermonde matrix,

$$
\begin{pmatrix}
\alpha_1 & \alpha_2 & \ldots & \alpha_{2t} \\
\alpha_1^2 & \alpha_2^2 & \ldots & \alpha_{2t}^2 \\
\alpha_1^{2t} & \alpha_2^{2t} & \ldots & \alpha_{2t}^{2t}
\end{pmatrix}
$$

so the columns are linearly independent. Hence BCH($k$, $t$) has a minimum distance greater than $2t$. 

The Check Matrix and Error Patterns

**Definition 1.18** Given linear \((n, m)\)-code \(C\) and check matrix \(H\), the syndrome of a word \(u\) of length \(n\) is \((Hu^T)^T\), so syndrome of a word is a row vector.

**Proposition 1.19** \(u\) code word of \(BCH(k, t)\), \(v\) obtained from \(u\) by adding an error pattern \(e\) of weight at most \(t\), i.e. \(v = u + e\). Then \(e\) is uniquely determined by the syndrome

\[
V_{k,t}v^T
\]

**proof.** Assume that error pattern \(f \neq e\) of weight at most \(t\) produces the same syndrome as \(v\), then

\[
V_{k,t}(v - f)^T = 0
\]

so, \(v - f\) is a code word. The Hamming distance from \(u\) to \(v - f = u + e - f\) is the weight of \(e - f\) which is at most \(2t\) contradicting the fact that the minimum distance of the code is greater than \(2t\).
2 BCH Codes as Polynomial Codes

Checking a binary word \((c_1, c_2, \ldots, c_n)\) is a code word of BCH\((k,t)\) is equivalent to verifying the equations

\[
\sum_{i=0}^{n-1} c_i \alpha^{ik} = 0
\]

for powers \(\alpha^k\) of a primitive element \(\alpha\), \(k = 1, 2, \ldots, 2t\). So, it is natural to identify code words \(c\) with binary polynomials \(c(x)\) of degree less than \(n\). Hence the equations can be rewritten

\[
c(\alpha^k) = 0
\]

**Convention:** Let \(V\) be a vector space \(B^n\) of binary \(n\)-tuples. We write an element \(u \in V\) as \((u_{n-1}, u_{n-2}, \ldots, u_1, u_0)\) and identify it with the polynomial

\[
u(x) = \sum_{i=0}^{n-1} u_i x^i
\]

The polynomial corresponding to a word \(u\) be will be denoted by \(u(x)\). The set of all binary polynomials of degree less than \(n\) will be denoted by \(P_n\).
Example 2.1 The code word $0 0 0 0 1 1 1 0 1 1 0 0 1 0 1$ corresponds to 

$$x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1$$

Proposition 2.2 [Definition of BCH(k,t)] Let $n = 2^k - 1$ and let the columns of the check matrix $V_{k,t}$ be ordered so that $V_{k,t} = (\alpha^{i(n-j)})$. If $c(x) \in P_n$, then $c(x)$ is a code polynomial of BCH($k, t, \alpha$) if and only if 

$$c(\alpha^j) = 0$$

for all powers $j \leq 2t$ of $\alpha$.

Proposition 2.3 $g(x)$ be the product of all the distinct minimal polynomials of $\alpha, \alpha^2, ..., \alpha^{2t}$ over $B$ (each minimal polynomial is taken only once ), then 

"$c(x)$ of degree $< n$ is a code polynomial of BCH($k, t, \alpha$)" iff $g(x) | c(x)$.

Definition 2.4 $g(x)$ is called the generator polynomial of BCH($k, t$).
The generator polynomial of BCH codes

**Corollary 2.5** The generator polynomial of BCH\((k, t)\) is the unique non-zero polynomial of lowest degree in BCH\((k, t)\).

**Example 2.6** [BCH\((4, 3)\)] the generator polynomial is

\[
m_2(x)m_8(x)m_{11}(x) = (x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1
\]

The corresponding code word is

\[
0 0 0 0 1 1 1 0 1 1 0 0 1 0 1
\]

This is the only non-zero code word that starts with four zeros.

**proof.** The degree of a non-zero multiple \(b(x)g(x)\) of \(g(x)\) is equal to at least \(\deg(g(x))\), and the equality holds only if \(b(x)\) is a constant. 1 is the only non-zero constant of \(B\). Hence all non-zero code polynomials have degree at least equal to \(\deg(g(x))\), and the only code polynomial with \(\deg(g(x))\) is \(g(x)\).
Multiplicative encoding

The corollary above gives a simple encoding algorithm for $\text{BHC}(k, t)$. The message space consists of $P_m$. Encode $b(x) \in P_n$ by multiplying it by $g(x)$.

**Example 2.7** [$\text{BCH}(4,3)$] Suppose that we want to encode the message word $b = (1 \ 0 \ 1 \ 1 \ 1)$. The corresponding polynomial is $b(x) = x^4 + x^2 + x + 1$, then the corresponding code word $c(x)$ is obtained by multiplying $b(x)$ with the generator polynomial $g(x) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1$, so

$$c(x) = b(x)g(x) = x^{14} + x^{13} + x^9 + x^6 + x^5 + x^3 + x + 1$$

and the corresponding code word is

$$1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1$$
A Generator Matrix for $\text{BCH}(k, t)$

Represent polynomial multiplication by the generator matrix $g(x)$ by a suitable matrix. The columns of the generator matrix of a code $C$ are the all code words of $C$. We choose as the columns of the code words corresponding to $x^i g(x)$ for $i = m - 1, m - 2, ..., 1, 0$.

**Example 2.8 [BCH(4,3)]** A generator matrix $G$ for BCH(4,3) is

$$
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 \\
1 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1
\end{pmatrix}
$$
For linear codes, we have the following proposition

**Proposition 2.9** Let $C$ be an $(n, m)$ linear code and let $G$ be an $n \times n$ matrix. Then $G$ is a generator matrix for $C$ if and only if it has rank $m$ and its columns are code words.

**Proposition 2.10** Let $g(x)$ be a generator polynomial of BCH($k$, $t$) and let $G$ be the $n \times m$ matrix constructed by taking as its columns the coefficients of $x^i g(x)$ for $i = m - 1, \ldots, 1, 0$. then $G$ is a generator matrix for BCH($k$, $t$)
The Check Polynomial

\[ x^n - 1 = \prod \text{distinct minimal polynomials of non-zero elements of } GF(q). \]

Generator polynomial \( g(x) \) of BCH\((k, t)\) is the product of a certain subset of these minimal polynomials. So we can write \( x^n - 1 = g(x)h(x) \) for some \( h(x) \). Consider the code polynomial \( c(x) = b(x)g(x) \) then,

\[ c(x)h(x) = b(x)g(x)h(x) = b(x)(x^n - 1) \]

**Definition 2.11** The polynomial \( h(x) \) is called the check polynomial of BCH\((k, t)\).

**Proposition 2.12** Let \( c(x) \) be a polynomial of degree less that \( n \). Then \( c(x) \) is a code polynomial of BCH\((k, t)\) if and only if \( x^n - 1 \) divides \( c(x)h(x) \).

*proof.* If \( c(x) \) is a code word, then \( c(x)h(x) \) is a multiple of \( x^n - 1 \).
Multiplicative Decoding for BCH($k, t$)

Check polynomial provides a multiplicative decoder for our code. It incorporates a check for the correctness of the received word, but it does no error processing.

**Observation:** If $\deg(b(x)) < n$, then $b(x)(x^n - 1) = b(x)x^n - b(x)$ so if we multiply a code polynomial $c(x) = b(x)g(x)$ by $h(x)$, the first $m$ coefficients will be the coefficients of $b(x)$.

**Example 2.14** If the code word $c$ is $1100010011010111$ then

$$c(x)h(x) = 101110000000000010111$$

so, the message word $b$ is

$$10111$$
Determining the error word

Assume that we are using a code BCH\((k, t)\) of block length \(n = 2^k - 1\) which is designed to correct errors at most \(t\). Suppose that a code word \(c\) is sent and the word \(d\) is received. By using the check matrix, if

\[
V_{k, t} b^T \neq 0
\]

we can say that \(d\) is not a code word. We have the following proposition for the linear codes:

**Proposition 3.1** A linear code with a check matrix \(H\). Suppose that a code word \(c\) is transmitted and the word \(d = c + e\) is received, then the syndromes of \(e\) and \(d\) are equal, i.e. \(Hd^T = He^T\)

**Proof.**
\[
Hd^T = Hc^T + He^T = He^T \quad \text{(Since } Hc^T = 0)\]

Let the error word be \(e = d - c\), then we have that

\[
V_{k, t} d^T = V_{k, t} e^T
\]
If \( s \leq t \) errors occurred then from Proposition 1.19 there is exactly one possible error word \( e \) of weight at most \( t \) which satisfies

\[
V_{k,t}d^T = V_{k,t}e^T
\]

The error word \( e \) determines a set of columns of \( V_{k,t} \) whose sum is \( V_{k,t}e^T \). If there is only one error, we have a Hamming code and the search is easy since we just check the \( n \) columns of \( V_{k,t} \) to find which one gives the syndrome \( V_{k,t}d^T \).

However, if \( t > 1 \), we have to consider

\[
\left( \frac{n}{1} \right) + \left( \frac{n}{2} \right) + \ldots + \left( \frac{n}{t} \right)
\]

If \( k = 8 \) and \( t = 3 \), this number is 2763775, so we need to find an efficient procedure.
Let
\[ c = (c_{n-1}, \ldots, c_1, c_0) \] be the code word that is sent,
\[ d = (d_{n-1}, \ldots, d_1, d_0) \] be the received word,
\[ e = (e_{n-1}, \ldots, e_1, e_0) \] be the error where \( e_i - d_i = c_i \).

**Definition 3.2** If the component \( e_i \) of the error word \( e \) is not 0, \( i \) is called error location of \( d \). Let \( M \) be the set of error locations, then \( M \) has \( s \leq t \) elements and \( s \) is the weight of \( e \).

**Example 3.3** Let
\[ c = 1 1 0 1 1 0 0 1 0 1 0 0 0 0 1 \]
\[ d = 1 1 0 0 0 0 0 1 0 1 0 0 0 0 1 \]
\[ e = 0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 \]

then \( s = 2 \) and the error locations are 10 and 11.
The Syndromes of a Received Word

Consider the check matrix $V_{k,t}$, then the full syndrome of $V_{k,t}$ is a word of length $2t$ with the entries

$$S_1, S_2, ..., S_{2t}$$

The corresponding polynomials to the words above are,

$$c(x) = x^{14} + x^{13} + x^{11} + x^{10} + x^7 + x^5 + 1$$
$$d(x) = x^{14} + x^{13} + x^7 + x^5 + 1$$
$$e(x) = x^{11} + x^{10}$$

The rows of $V_{k,t}$ are of the form $(\alpha^{(q-2)j}, ..., \alpha^2j, \alpha^j, \alpha^0)$. Thus $i-th$ entry $S_i$ can be written as

$$S_i = \sum_{j=1}^{n-1} d_j \alpha^{ij} = d(\alpha^i)$$
**Definition 3.4** The values \( S_i = d(\alpha^i), i = 1, 2, \ldots, 2t \) are called the syndromes of \( d(x) \). The word \( V_{k,t}d^T = (S_1, S_2, \ldots, S_{2t}) \) is called the full syndrome or the syndrome vector.

**Proposition 3.5** \( c(x) \) code poly., \( d(x) \) is a polynomial of degree at most \( 2^k - 2 \) and \( e(x) = d(x) - c(x) \),

a. The syndromes \( S_i \) of \( d(x) \) and \( e(x) \) are identical for \( i = 1, 2, \ldots, 2t \)

b. The syndrome \( S_{2i} = S_i^2 \) for \( i = 1, 2, \ldots, t \)

c. \( d(x) \) is a code polynomial of BCH\((k, t)\) iff syndromes \( S_1, S_2, \ldots, S_{2t} \) are all 0.

**proof b.**

\[
S_i^2 = \left( \sum_{j=0}^{n-1} d_j \alpha^{ij} \right)^2 = \sum_{j=0}^{n-1} d_j^2 \alpha^{2ij} = \sum_{j=0}^{n-1} d_j \alpha^{2ij} = S_{2i}
\]
Syndromes of $c(x) = x^{14} + x^{13} + x^{11} + x^{10} + x^{7} + x^{5} + 1$

$S_1 = c(2) = 0, \quad S_3 = c(8) = 0, \quad S_5 = c(11) = 0$

Syndromes of $d(x) = x^{14} + x^{13} + x^{7} + x^{5} + 1$

$S_1 = d(2) = 7, \quad S_3 = d(8) = 9, \quad S_5 = d(11) = 1$

Syndromes of $e(x) = x^{11} + x^{10}$

$S_1 = e(2) = 7, \quad S_3 = e(8) = 9, \quad S_5 = e(11) = 1$
Now we consider the case \( s = 2 \), i.e. there are precisely two errors. Test whether the syndromes form a column of the check matrix \( V_{k,t} \). If they do, the column gives the error locations. Let \( M = \{i, j\} \) be the error locations, then we have to solve

\[
\begin{align*}
\alpha^i + \alpha^j &= S_1 \\
\alpha^{2i} + \alpha^{2j} &= S_2 \\
\alpha^{3i} + \alpha^{3j} &= S_3
\end{align*}
\]

**Example 3.7** \( \text{BCH}(4,3) \)

\[
\begin{align*}
\alpha^i + \alpha^j &= 7, & \alpha^{2i} + \alpha^{2j} &= 12, & \alpha^{3i} + \alpha^{3j} &= 9
\end{align*}
\]

then

\[
\alpha^{2i} + 7\alpha^i + 15 = 0
\]

\( \alpha = 10 = 2^{10} \) and \( \alpha = 13 = 2^{11} \)

so 10 and 11 are the error locations, then \( M = \{10, 11\} \).
The Syndrome Polynomial

**Definition 3.8** The syndrome polynomial of the word \( d \) with syndromes \( S_1, S_2, \ldots, S_{2t} \) is the polynomial

\[
s(z) = S_1 + S_2 z + \ldots + S_{2t-1} z^{2t-1} = \sum_{i=0}^{2t-1} S_{i+1} z^i
\]

The syndrome polynomial of \( d(x) \in \text{BCH}(4,3) \) is

\[
s(z) = 14 z^5 + z^4 + 6 z^3 + 9 z^2 + 12 z + 7
\]
Since

\[ S_i = \sum_{j=0}^{n-1} e_j \alpha^{ij} = \sum_{j=0}^{n-1} d_j \alpha^{ij} \]

\( s(z) \) can be rewritten as

\[ s(z) = \sum_{i=0}^{2t-1} S_{i+1} z^i = \sum_{j \in M} e_j \alpha^j \sum_{i=0}^{2t-1} \alpha^{ij} z^i \]

Let \( q = \alpha^j z \), then the inner sum can be written as

\[ \sum_{i=0}^{2t-1} \alpha^{ij} z^i = 1 + q + q^2 + \ldots + q^{2t-1} = \frac{1 - q^{2t}}{1 - q} \]
Formula for Syndrome Polynomial

**Proposition 3.9** The syndrome polynomial \( s(z) \) can be written as

\[
s(z) = \sum_{j \in M} e_j \alpha^j \left( \frac{1-(\alpha^j z)^2}{1-\alpha^j z} \right) = \sum_{j \in M} \frac{e_j \alpha^j}{1-\alpha^j z} - \sum_{j \in M} \frac{e_j \alpha^{(2t+1)j} z^{2t}}{1-\alpha^j z}
\]

where \( M \) is the set of error locations.

**Example 3.10** By using this formula, the syndrome polynomial \( s(z) \) of \( d(x) \) is

\[
s(z) = \frac{2^{10}}{1-2^{10}z} + \frac{2^{11}}{1-2^{11}z} - \frac{2^{70}z^6}{1-2^{10}z} - \frac{2^{77}z^6}{1-2^{11}z}
\]

\[
= 14z^5 + z^4 + 6z^3 + 9z^2 + 12z + 7
\]
Introduction to Fundamental Equation

By adding fractions, the syndrome polynomial can be expressed as difference

$$s(z) = \frac{w(z)}{l(z)} - \frac{u(z)z^{2t}}{l(z)}$$

It is clear that

$$l(z) = \prod_{j \in M} (1 - \alpha^j z)$$

The roots of $l(z)$ are the inverses of the powers $\alpha^j$, $j \in M$. So $l(z)$ can used to determine the error locations. $l(z)$ is called the error locator polynomial of $d(x)$. However, finding $l(z)$ is still a problem since we assumed that the error polynomial $e(x)$ is known.

Example 3.11 The error locations of $d(x)$ are 10 and 11 so the error locator is

$$l(z) = (1 - 2^{10} z)(1 - 2^{11} z) = (1 - 10z)(1 + 13z) = 15z^2 + 7z + 1$$
Proposition 3.12 The polynomials $w(z)$ and $u(z)$ satisfy the following formulas

$$w(z) = \sum_{j \in M} e_j \alpha^j \prod_{i \in M, i \neq j} (1 - \alpha^i z)$$

$$u(z) = \sum_{j \in M} e_j \alpha^{(2t+1)j} \prod_{i \in M, i \neq j} (1 - \alpha^i z)$$

**proof.** From the definition

$$w(z) = \sum_{j \in M} e_j \alpha^j \frac{1}{1 - \alpha^j z} \Rightarrow w(z) = \sum_{j \in M} e_j \alpha^j l(z) = \sum_{j \in M} e_j \alpha^j \prod_{i \in M} (1 - \alpha^j z)$$

$$= \sum_{j \in M} e_j \alpha^j \prod_{i \in M, i \neq j} (1 - \alpha^i z)$$

**Example 3.13** With the error locations 10 and 11,

$$w(z) = 2^{10} (1 + 2^{11} z) + 2^{11} (1 + 2^{10} z) = 10(1 + 13z) + 13(1 + 10z) = 7$$

$$u(z) = 2^{70} (1 + 13z) + 2^{77} (1 + 2^{10} z) = 14 + 12z$$
Once we know the error locator \( l(z) \) and hence error locations, \( w(z) \) can be used to calculate the error values. It is called the error evaluator. The polynomial \( u(z) \) can also be used to determine the error values and it is called the error co-evaluator. In practice, \( w(z) \) is used.

**The Fundamental Equation**

The equation

\[
w(z) = l(z)s(z) + u(z)z^{2t}
\]

obtained from

\[
s(z) = \frac{w(z)}{l(z)} - \frac{u(z)z^{2t}}{l(z)}
\]

is called the fundamental equation for BCH codes.

**Example 3.14** By using the calculated polynomials \( l(z) \), \( w(z) \) and \( u(z) \) we see that the fundamental equation is

\[
l(z)s(z) + u(z)z^{2t} = 12z^7 + 14z^6 + 7 + 12z^7 + 14z^6 = w(z)
\]
Now we present an efficient algorithm invented by Sugiyama in 1975. It is based on the Euclid’s algorithm. The knowledge of the error locator enables us to calculate is roots and thus to find the error locations and correct the received word. The key to the solution of this problem is the fundamental equation

\[ w(z) = l(z)s(z) + u(z)z^{2t} \]

**BCH Algorithm with Example BCH(4,3)**

The algorithm that we will use is based on the fact that all the polynomials that we are looking for appear in the table produced when Euclid’s algorithm applied to \( z^{2t} \) and \( s(z) \).
Step 1.

Calculate $S_i = d(\alpha^i)$ for $i = 1, 3, \ldots, 2t - 1$ and find $S_{2i} = S_i^2$ for $i = 1, 2, \ldots, t$. Then calculate the syndrome polynomial

$$s(z) = \sum_{i=1}^{2t} S_{i+1}z^i$$

If $s(z) = 0$, then STOP. The received word has no errors.

We found that syndrome polynomial of $d(x)$ is

$$s(z) = 14z^5 + z^4 + 6z^3 + 9z^2 + 12z + 7$$
Step 2.

Apply Euclid's algorithm to $a(z) = z^{2t}$ and $b(z) = s(z)$. Finish at the stage where the remainder $r_j(z)$ has degree less that $t$. We can use the notation $r_j(z) = w'(z)$, $u_j(z) = u'(z)$, $v_j(z) = l'(z)$.

Applying Euclid's algorithm to $z^{2t}$ and $s(z) = 14z^5 + z^4 + 6z^3 + 9z^2 + 12z + 7$, we find that

$$r_2(z) = 5 = w'(z)$$

$$u_2(z) = 2z + 10 = u'(z)$$

$$v_2(z) = 14z^2 + 5z + 4 = l'(z)$$
Step 3.

If \( r_j(z) = 0 \), there are more than \( t \) errors so STOP. Otherwise, put \( l'(z) = v_j(z) \). This differs from \( l(z) \) only by a nonzero constant factor, find the roots \( \beta_1, \beta_2, \ldots, \beta_s \).

Theorem 3.16 Denote the polynomials calculated by the BCH algorithm by \( l'(z), u'(z), w'(z) \) and true error locator, evaluator polynomials \( l(z), w(z), u(z) \). If \( s \leq t \) errors occurred, then there exists a non-zero constant \( K \) such that

\[
l'(z) = K \cdot l(z)
\]

\[
w'(z) = K \cdot w(z)
\]

\[
u'(z) = K \cdot u(z)
\]
Since \( l'(z) \) differs from \( l(z) \) by a constant factor, they have same roots.

For our example,

\[
l'(z) = 14z^2 + 5z + 4 = 4(15z^2 + 7z + 1)
\]

\[
w'(z) = 5 = 4 \cdot 7
\]

\[
u'(z) = 2z + 10 = 4(12z + 14)
\]

Now consider \( l'(z) = 14z^2 + 5z + 4 \). Since \( 4 \cdot 9^2 + 5 \cdot 9 + 4 = 0 \) \( 9 \) is a root of \( l'(z) \), and since \((z - 9)(14z - 6) = l'(z)\) the roots of \( l'(z) \) are 9 and \( 6/14 = 11 \).
Step 4.

If the roots of $l'(z)$ are $\beta_i = \alpha^{p(i)}$, then the errors occurred at the place $2^k - p(i) - 1$ counting from the right, starting from 0.

$9 = 2^4$ and $11 = 2^5$ so that the error locations are 16-4-1=11 and 16-5-1=10.
**Termination of the Algorithm**

**Proposition 3.17** Assume that $1 < s \leq t$ errors occurred, then the step 2 of the algorithm will end with a non-zero $r_j(z)$ such that $\deg(r_j(z)) < t$ and $\deg(r_{j-1}(z)) \geq t$.

**proof.** From the fundamental equation $w(z) = l(z)s(z) + u(z)z^{2t}$, the greatest common divisor $(s(z), z^{2t})$ of $s(z)$ and $z^{2t}$ divides $w(z)$ so that

$$\deg(s(z), z^{2t}) \leq \deg(w(z)) < s \leq t$$

Also $\deg(z^{2t}) = 2t > t$ Since the Euclid's algorithm terminates with $(s(z), z^{2t}) = r_j(z)$, there exists a $j$ such that $\deg(r_j(z)) < t$ and $\deg(r_{j-1}(z)) \geq t$. 