BCH Codes

G V V Sharma*

Contents

***Abstract*—This manual provides an introduction to BCH codes.**

*The author is with the Department of Electrical Engineering, Indian Institute of Technology, Hyderabad 502285 India e-mail: gadepall@iith.ac.in.

1 Generator Polynomial

1.1 For a BCH code, the minimal polynomials are given by

$$g_1(x) = 1 + x + x^3 + x^5 + x^{14} \tag{1.1}$$
$$g_2(x) = 1 + x^6 + x^8 + x^{11} + x^{14} \tag{1.2}$$
$$g_3(x) = 1 + x + x^2 + x^6 + x^9 + x^{10} + x^{14} \tag{1.3}$$
$$g_4(x) = 1 + x^4 + x^7 + x^8 + x^10 + x^{12} + x^{14} \tag{1.4}$$
$$g_5(x) = 1 + x^2 + x^4 + x^6 + x^8 + x^9 + x^{11} + x^{13} + x^{14} \tag{1.5}$$
$$g_6(x) = 1 + x^3 + x^7 + x^8 + x^9 + x^{13} + x^{14} \tag{1.6}$$
$$g_7(x) = 1 + x^2 + x^5 + x^6 + x^7 + x^{10} + x^{11} + x^{13} + x^{14} \tag{1.7}$$
$$g_8(x) = 1 + x^5 + x^8 + x^9 + x^{10} + x^{11} + x^{14} \tag{1.8}$$
$$g_9(x) = 1 + x + x^2 + x^3 + x^9 + x^{10} + x^{14} \tag{1.9}$$
$$g_{10}(x) = 1 + x^3 + x^6 + x^9 + x^{11} + x^{12} + x^{14} \tag{1.10}$$
$$g_{11}(x) = 1 + x^4 + x^{11} + x^{12} + x^{14} \tag{1.11}$$
$$g_{12}(x) = 1 + x + x^2 + x^3 + x^5 + x^6 + x^7 + x^8 + x^{10} + x^{13} + x^{14} \tag{1.12}$$

Obtain the minimal polynomial matrix.
Solution:

```
https://raw.githubusercontent.com/gadepall/
    EE6317/master/BCH/codes/
    min_poly_mat.py
```

1.2 Obtain the generator polynomial vector.
Solution: The generator polynomial is obtained as

$$g(x) = \prod_{i=1}^{m} g_i(x) \tag{1.13}$$

The following code computes $\mathbf{g}$.

```
https://raw.githubusercontent.com/gadepall/
    EE6317/master/BCH/codes/gen_poly.py
```

2 Encoding

2.1 Let $\mathbf{m}$ be a $k \times 1$ message vector and

$$m(x) = m_{k-1}x^{k-1} + m_{k-2}x^{k-2} + \cdots + m_1 x + m_0 \tag{2.1}$$

be the correspoding Message polynomial.

2.2 Let

$$m(x)x^{n-k} = q(x)g(x) + d(x) \tag{2.2}$$

and

$$c(x) = m(x)x^{n-k} + d(x) \tag{2.3}$$

Write a program to compute the corresponding coefficient vector $\mathbf{c}$. This is the output of the BCH encoder.

3 Decoding

3.1 Let the Received polynomial be $r(x)$ i.e which contains both transmitted codeword polynomial $c(x)$ and the error polynomial $e(x)$

$$e(x) = e_0 + e_1 x^1 + ... + e_{n-1}x^{n-1} \tag{3.1}$$

Where e_i represents the value of the error at the location. For binary BCH codes e_i is either 0 or 1.

$$r(x) = c(x)+e(x) = r_{n-1}x^{n-1}+r_{n-2}x^{n-2}+\cdots+r_1 x+r_0 \tag{3.2}$$

Definie, Syndrome

$$S_i = r(\alpha^i) = c(\alpha^i) + e(\alpha^i) = e(\alpha^i) \tag{3.3}$$

Where α^i is a root of the codeword.
Suppose that v errors occurred, and $0 \le v \le t$.
Let the error occurs at $i_1, i_2, \ldots, i_v$.
The Decoding Process, for a t-error correcting code will follows the basic steps,

3.2 Compute the Syndrome $S = (S_1, S_2, \ldots, S_{2t})$ from the received polynomial $r(x)$

3.3 Determine the error-location polynomial $\sigma(x)$ from the syndrome components $S_1, S_2, \ldots, S_{2t}$ using the Berlekamp's Algorithm.

3.4 Using the Chain searching algorithm, determine the error-locations by finding the roots of $\sigma(x)$, the flip the posisions in $r(x)$. Which is the estimated message vector polynomial $\hat{c}(x)$.

3.5 where $\mathbf{w}$ is $p \times 1$ and $\mathbf{X}$ is $N \times p$. Show that

$$E(\hat{\mathbf{w}}) = \mathbf{w} \tag{3.4}$$

3.6 If the covariance matrix of $\mathbf{y}$ is

$$\mathbf{C_y} = \sigma^2 \mathbf{I} \tag{3.5}$$

show that

$$\mathbf{C_w} = \sigma^2 \left(\mathbf{X}^T \mathbf{X}\right)^{-1} \tag{3.6}$$

3.7 Let

$$\hat{\mathbf{y}} = \mathbf{X}\hat{\mathbf{w}} \tag{3.7}$$

$$\hat{\sigma}^2 = \frac{1}{N-p}\|\mathbf{y} - \hat{\mathbf{y}}\|^2 \tag{3.8}$$

$$\mathbf{y} - \hat{\mathbf{y}} \sim \mathcal{N}\left(\mathbf{0}, \sigma^2 \mathbf{I}\right) \tag{3.9}$$

Show that

$$(N-p)\,\hat{\sigma}^2 \sim \sigma^2 \chi^2_{N-p} \tag{3.10}$$

3.8 Let

$$\hat{z} = \frac{w_j}{\hat{\sigma}\sqrt{v_j}} \tag{3.11}$$

where v_j is the diagonal element of $\left(\mathbf{X}^T \mathbf{X}\right)^{-1}$. If $w_j = 0$, show that z_j has a t_{N-p} distribution.

3.9 Plot $\Pr(|Z| > z)$ for t_{30}, t_{100} and the standard normal distribution.

4 Applications

4.1 Explain how (**??**) can be used to obtain the Nearest Neighbour approximation.

4.2 Repeat the exercise for the least squares method.