# AN EXAMPLE OF THE BCH CODE DECODING ALGORITHM

LECTURE NOTES BY DR. SAMUEL J. LOMONACO

Abstract. We give a simple example of the BCH code decoding algorithm.

Let $GF\left(2^4\right) = GF\left(2\right)\left[x\right]/\left(p(x)\right)$, where $p(x)$ is the primitive polynomial $p(x) = x^4 + x + 1$, and let $\xi$ be the primitive root $\xi = x \bmod p(x)$.

We let $g(x)$ be the monic polynomial of smallest degree having the following zeroes:

$$\xi, \xi^2, \xi^3, \xi^4 \ ,$$

and let $V$ be the length 15 given by the generator polynomial $g(x)$. Hence, since $g(x)$ has four consecutive roots, $V$ is a BCH code with design distance $\delta = 4+1 = 5$. Hence, the minimum distance $d$ of $V$ is bounded below by $\delta$, i.e., $d \geq \delta = 5 = 2 \cdot 2 + 1 = 2t + 1$. This implies that the the BCH code $V$ is capable of correcting at least $t = 2$ errors.

Since $\xi$, $\xi^2$, and$\xi^4$ are all conjugate to each other, and since $\xi$ and $\xi^3$ are not conjugate, $g(x)$ is simply the polynomial of smallest degree having $\xi$ and $\xi^3$ as roots. Thus, the parity matrix is given by

$$H = \begin{pmatrix} \xi^{14} & \xi^{13} & \xi^{12} & \cdots & \xi^{2} & \xi^{1} & 1 \\ \left(\xi^3\right)^{14} & \left(\xi^3\right)^{13} & \left(\xi^3\right)^{12} & \cdots & \left(\xi^3\right)^{2} & \left(\xi^3\right)^{1} & 1 \end{pmatrix}$$

which simplifies to

$$H = \begin{pmatrix} \xi^{14} & \xi^{13} & \xi^{12} & \cdots & \xi^{2} & \xi^{1} & 1 \\ \xi^{12} & \xi^{9} & \xi^{6} & \cdots & \xi^{6} & \xi^{3} & 1 \end{pmatrix} .$$

Let us assume that a code vector $\overrightarrow{c}$ is sent over a BSC, and that the received vector is $\overrightarrow{r} = \overrightarrow{c} + \overrightarrow{\epsilon}$, where $\overrightarrow{\epsilon}$ denotes the error vector. Let us further assume that exactly two errors have occured, i.e.,

$$\overrightarrow{\epsilon} = \overrightarrow{\epsilon_i} + \overrightarrow{\epsilon_j} \ ,$$

where $\overrightarrow{\epsilon_i}$ and $\overrightarrow{\epsilon_j}$ denote length 15 binary with 1 in the $i$-th and the $j$-th posions, respectively, and with all other entries equal to zero. Thus, we have

$$\overrightarrow{c} \longrightarrow \boxed{\text{BSC}} \longrightarrow \overrightarrow{r} = \overrightarrow{c} + \overrightarrow{\epsilon} = \overrightarrow{r} = \overrightarrow{c} + \overrightarrow{\epsilon_i} + \overrightarrow{\epsilon_j} \ .$$

Let us now compute the syndrome of the received vector $\overrightarrow{r}$.

$$Syn\left(\overrightarrow{r}\right) = Syn\left(\overrightarrow{\epsilon}\right)$$

*Date*: December 4, 2007.

If we let $\gamma_j$ denote the $j$-th column of $H$, i.e.,

$$H = \begin{pmatrix} \gamma_{14} & \gamma_{13} & \gamma_{12} & \cdots & \gamma_2 & \gamma_1 & \gamma_0 \end{pmatrix} ,$$

and use the fact that the error vector is of the form

$$\overrightarrow{\epsilon} = \begin{pmatrix} 0 & \cdots & 0 & \underset{\downarrow}{\boxed{\text{loc } i}} \atop 1 & 0 & \cdots & 0 & \underset{\downarrow}{\boxed{\text{loc } j}} \atop 1 & 0 & \cdots & 0 \end{pmatrix}$$

we have

$$Syn\left(\overrightarrow{r}\right) = \overrightarrow{\epsilon} \begin{pmatrix} \gamma_{14}^T \\ \gamma_{13}^T \\ \vdots \\ \gamma_1^T \\ \gamma_0^T \end{pmatrix} = \gamma_i^T + \gamma_j^T = \begin{pmatrix} \xi^i \\ \\ \left(\xi^i\right)^3 \end{pmatrix} + \begin{pmatrix} \xi^j \\ \\ \left(\xi^j\right)^3 \end{pmatrix} = \begin{pmatrix} \xi^i + \xi^j \\ \\ \left(\xi^i\right)^3 + \left(\xi^j\right)^3 \end{pmatrix}$$

We will call the field elements $\xi^i$ and $\xi^j$ **error locators**, since their logs are the locations of the two respective errors. Knowing the error locators is equivalent to knowing the error locations.

Let us denote the two components of $Syn\left(\overrightarrow{r}\right)$ by $z_1$ and $z_2$, respectively. Thus,

$$Syn\left(\overrightarrow{r}\right) = \begin{pmatrix} \xi^i + \xi^j \\ \\ \left(\xi^i\right)^3 + \left(\xi^j\right)^3 \end{pmatrix} = \begin{pmatrix} z_1 \\ \\ z_2 \end{pmatrix}$$

We would now like to construct from the components $z_1$ and $z_2$ of the syndrome, the **error location polynomial** $S(x)$. The **error location polynomial** $S(x)$ is the polynomial over $GF\left(2^4\right)$ whose roots are the error locator. In other words,

$$S(x) = \left(x + \xi^i\right)\left(x + \xi^j\right) = x^2 + \left(\xi^i + \xi^j\right)x + \left(\xi^i \cdot \xi^j\right)$$

Since

$$\begin{cases} \xi^i + \xi^j & = & z_1 \\ \\ \left(\xi^i\right)^3 + \left(\xi^j\right)^3 & = & z_2 \end{cases} ,$$

we have

$$z_2 = \left(\xi^i + \xi^j\right)\left(\left(\xi^i\right)^2 + \xi^i\xi^j + \left(\xi^j\right)^2\right) = z_1\left(z_1^2 + \xi^i\xi^j\right) .$$

Hence,

$$\xi^i\xi^j = \frac{z_2}{z_1} + z_1^2 .$$

Thus,

$$S(x) = \left(x + \xi^i\right)\left(x + \xi^j\right) = S(x) = \left(x + \xi^i\right)\left(x + \xi^j\right) = x^2 + z_1 x + \left(\frac{z_2}{z_1} + z_1^2\right)$$

Thus, the error locators can be found simply by finding the roots of the above error locator polnomial (which was computed from the syndrome of the received vector.)

Given the syndrome $Syn\left(\overrightarrow{r}\right) = \begin{pmatrix} z_1, & z_2 \end{pmatrix}^T$ of the received vector $\overrightarrow{r}$, our error correcting scheme is as follows:

**i)** If $z_1 = z_2 = 0$, then we decide that no error has occurred.

**ii)** If $z_1 \neq 0$ and $z_2 = z_1^3$, then we decide that a single error has occurred at the error locator $z_1 = \xi^i$.

**iii)** If $z_1 \neq 0$ and $z_2 \neq z_1^3$, then we decide that two errors have occurred, and we find the two error locators $\xi^i$ and $\xi^j$ by finding the two roots of the error locator polynomial $S(x)$.

**Example 1.** *As an example, let consider the case when two errors have occured at locations* 6 *and* 8. *We will use the attached AntiLog/Log table for our calculations.*

*The syndrome of the recived vector* $\overrightarrow{r}$

$$Syn\left(\overrightarrow{r}\right) = \begin{pmatrix} \xi^6 + \xi^8 \\ \\ \left(\xi^6\right)^3 + \left(\xi^6\right)^3 \end{pmatrix} = \begin{pmatrix} \xi^6 + \xi^8 \\ \\ \xi^3 + \xi^9 \end{pmatrix} = \begin{pmatrix} \xi^{14} \\ \\ \xi \end{pmatrix} = \begin{pmatrix} z_1 \\ \\ z_2 \end{pmatrix}$$

*Since,*

$$\frac{z_2}{z_1} + z_1^2 = \frac{\xi}{\xi^{14}} + \left(\xi^{14}\right)^2 = \xi^2 + \xi^{13} = \xi^{14} \ ,$$

*the error locator polynomial is*

$$S\left(x\right) = x^2 + \xi^{14}x + \xi^{14}$$

*One can easily check that*

$$S\left(x\right) = x^2 + \xi^{14}x + \xi^{14} = \left(x + \xi^6\right)\left(x + \xi^8\right)$$

**Problem 1.** *If the received vector* $\overrightarrow{r}$ *is*

$$\overrightarrow{r} = 10110\ 00101\ 11100\ ,$$

*compute the syndrome* $Syn\left(\overrightarrow{r}\right)$, *and the error locator polynomial* $S(x)$ *Once you have the error locator polynomial* $S(x)$ *use it to find the two error locators* $\xi^i$ *and* $\xi^j$, *and the corrected code vector.*

## References


[1] Berlekamp, Elwyn R., **"Algebraic Coding Theory,"** McGraw-Hill, (1968), Chapter 7.

[2] MacWilliams, F.J., and N.J.A. Sloane, **"The Theory of Error-Correcting Codes,"** North-Halland, (1996), Chapters 3 and 9.

[3] Peterson, W. Wesley, and E.J. Weldon, Jr., **"Error-Correcting Codes,"** MIT Press, (1996), (2nd edition), Chaper 9.

| $GF(2^4)$ | |
|---|---|
| $p(x) = x^4 + x + 1$ | |
| $AntiLog$ $a_0 a_1 a_2\ a_3$ | $Log$ |
| 0000 | $-\infty$ |
| 1000 | 0 |
| 0100 | 1 |
| 0010 | 2 |
| 0001 | 3 |
| 1100 | 4 |
| 0110 | 5 |
| 0011 | 6 |
| 1101 | 7 |
| 1010 | 8 |
| 0101 | 9 |
| 1110 | 10 |
| 0111 | 11 |
| 1111 | 12 |
| 1011 | 13 |
| 1001 | 14 |