BCH Codes

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

October 13, 2015

BCH Codes

- Discovered by Hocquenghem in 1959 and independently by Bose and Chaudhari in 1960
- Cyclic structure proved by Peterson in 1960
- Decoding algorithms proposed/refined by Peterson, Gorenstein and Zierler, Chien, Forney, Berlekamp, Massey…
- We will discuss a subclass of BCH codes — binary primitive BCH codes

Binary Primitive BCH Codes

For positive integers $m \geq 3$ and $t < 2^{m-1}$, there exists an (n, k) BCH code with parameters

- $n = 2^m - 1$
- $n - k \leq mt$
- $d_{min} \geq 2t + 1$

Definition

Let α be a primitive element in F_{2^m}. The generator polynomial $g(x)$ of the t-error-correcting BCH code of length $2^m - 1$ is the least degree polynomial in $\mathbb{F}_2[x]$ that has

$$\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2t}$$

as its roots.

Let $\varphi_i(x)$ be the minimal polynomial of α^i. Then $g(x)$ is the LCM of $\varphi_1(x), \varphi_2(x), \ldots, \varphi_{2t}(x)$.

Binary Primitive BCH Code of Length 7

- $m = 3$ and $t < 2^{3-1} = 4$
- Let α be a primitive element of F_8
- For $t = 1$, $g(x)$ is the least degree polynomial in $\mathbb{F}_2[x]$ that has as its roots α, α^2
  - α is a root of $x^8 + x$

$$x^8 + x = x(x+1)(x^3+x+1)(x^3+x^2+1)$$

  - Let α be a root of $x^3 + x + 1$
  - The other roots of $x^3 + x + 1$ are α^2, α^4
  - For $t = 1$, $g(x) = x^3 + x + 1$
- For $t = 2$, $g(x)$ is the least degree polynomial in $\mathbb{F}_2[x]$ that has as its roots $\alpha, \alpha^2, \alpha^3, \alpha^4$
  - The roots of $x^3 + x^2 + 1$ are $\alpha^3, \alpha^5, \alpha^6$
  - For $t = 2$, $g(x) = (x^3 + x + 1)(x^3 + x^2 + 1)$
- For $t = 3$, $g(x)$ is the least degree polynomial in $\mathbb{F}_2[x]$ that has as its roots $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6 \implies g(x) = (x^3 + x + 1)(x^3 + x^2 + 1)$

Binary Primitive BCH Code of Length 7

For a BCH code with parameters m and t, we have

- $n - k \leq mt$
- $d_{min} \geq 2t + 1$

t	$g(x)$	$n-k$	mt	d_{min}	$2t+1$
1	$x^3 + x + 1$	3	3	3	3
2	$(x^3 + x + 1)(x^3 + x^2 + 1)$	6	6	7	5
3	$(x^3 + x + 1)(x^3 + x^2 + 1)$	6	9	7	7

Definition

A degree m irreducible polynomial in $\mathbb{F}_2[x]$ is said to be primitive if the smallest value of N for which it divides $x^N + 1$ is $2^m - 1$

Lemma

The minimal polynomial of a primitive element is a primitive polynomial.

Single Error Correcting BCH Codes are Hamming Codes

We will prove this for $m = 3$. The proof of the general case is similar.

Proof.

- Consider a BCH code with parameter $m = 3$ and $t = 1$
- Let α be a primitive element of F_8 and a root of $x^3 + x + 1$
- The generator polynomial $g(x) = x^3 + x + 1$
- The code has length 7 and dimension 4
- A polynomial $v(x) = v_0 + v_1 x + v_2 x^2 + \cdots + v_6 x^6$ is a code polynomial $\iff$ $v(x)$ is a multiple of $g(x)$ $\iff$ α is a root of $v(x)$ $\iff$ $v(\alpha) = 0$

$$v(\alpha) = 0 \iff v_0 + v_1\alpha + v_2\alpha^2 + v_3\alpha^3 + \cdots + v_6\alpha^6 = 0$$

Single Error Correcting BCH Codes are Hamming Codes

Proof continued.

Power	Polynomial	Tuple
0	0	$\begin{pmatrix}0 & 0 & 0\end{pmatrix}$
1	1	$\begin{pmatrix}1 & 0 & 0\end{pmatrix}$
α	α	$\begin{pmatrix}0 & 1 & 0\end{pmatrix}$
α^2	α^2	$\begin{pmatrix}0 & 0 & 1\end{pmatrix}$
α^3	$1+\alpha$	$\begin{pmatrix}1 & 1 & 0\end{pmatrix}$
α^4	$\alpha+\alpha^2$	$\begin{pmatrix}0 & 1 & 1\end{pmatrix}$
α^5	$1+\alpha+\alpha^2$	$\begin{pmatrix}1 & 1 & 1\end{pmatrix}$
α^6	$1+\alpha^2$	$\begin{pmatrix}1 & 0 & 1\end{pmatrix}$

$$v(\alpha) = 0 \iff v_0 + v_1\alpha + v_2\alpha^2 + v_3\alpha^3 + \cdots + v_6\alpha^6 = 0$$

$$\iff \begin{bmatrix}1 & \alpha & \cdots & \alpha^6\end{bmatrix}\begin{bmatrix}v_0\\ v_1\\ \vdots\\ v_6\end{bmatrix} = 0 \iff \begin{bmatrix}1 & 0 & 0 & 1 & 0 & 1 & 1\\ 0 & 1 & 0 & 1 & 1 & 1 & 0\\ 0 & 0 & 1 & 0 & 1 & 1 & 1\end{bmatrix}\begin{bmatrix}v_0\\ v_1\\ \vdots\\ v_6\end{bmatrix} = \mathbf{0}$$

□

Degree of Generator Polynomial

Theorem

For a binary primitive BCH code with parameters m, t and generator polynomial $g(x)$, $\deg[g(x)] \leq mt$*.*

Proof.

- $g(x) = \text{LCM}\{\varphi_1(x), \varphi_2(x), \varphi_3(x), \ldots, \varphi_{2t}(x)\}$
- If i is an even integer, then $i = i'2^a$ where i' is odd
- $\alpha^i = \left(\alpha^{i'}\right)^{2^a} \implies \alpha^i$ and $\alpha^{i'}$ have the same minimal polynomial
- Every even power of α has the same minimal polynomial as some previous odd power of α

$$g(x) = \text{LCM}\{\varphi_1(x), \varphi_3(x), \varphi_5(x), \ldots, \varphi_{2t-1}(x)\}$$

- Since $\deg(\varphi_i)$ divides m, we have $n - k \leq mt$

□

Lower Bound on Minimum Distance

- We want to show that if the generator polynomial has roots $\alpha, \alpha^2, \cdots, \alpha^{2t}$ then $d_{min} \geq 2t + 1$
- Suppose there exists a nonzero codeword $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ of weight $\delta \leq 2t$
- The corresponding code polynomial satisfies $\mathbf{v}(\alpha^i) = 0$ for $i = 1, 2, 3, \ldots, 2t$

$$\begin{aligned} v_0 + v_1\alpha + v_2\alpha^2 + \cdots + v_{n-1}\alpha^{n-1} &= 0 \\ v_0 + v_1\alpha^2 + v_2\alpha^4 + \cdots + v_{n-1}\alpha^{2(n-1)} &= 0 \\ &\vdots \\ v_0 + v_1\alpha^{2t} + v_2\alpha^{4t} + \cdots + v_{n-1}\alpha^{2t(n-1)} &= 0 \end{aligned}$$

- Let $j_1, j_2, \ldots, j_\delta$ be the nonzero locations in the codeword

$$v_{j_1}(\alpha^i)^{j_1} + v_{j_2}(\alpha^i)^{j_2} + \cdots + v_{j_\delta}(\alpha^i)^{j_\delta} = 0$$

for $i = 1, 2, \ldots, 2t$

Lower Bound on Minimum Distance

$$\begin{bmatrix} v_{j_1} & v_{j_2} & \cdots & v_{j_\delta} \end{bmatrix} \begin{bmatrix} \alpha^{j_1} & (\alpha^2)^{j_1} & \cdots & (\alpha^{2t})^{j_1} \\ \alpha^{j_2} & (\alpha^2)^{j_2} & \cdots & (\alpha^{2t})^{j_2} \\ \alpha^{j_3} & (\alpha^2)^{j_3} & \cdots & (\alpha^{2t})^{j_3} \\ \vdots & \vdots & & \vdots \\ \alpha^{j_\delta} & (\alpha^2)^{j_\delta} & \cdots & (\alpha^{2t})^{j_\delta} \end{bmatrix} = \mathbf{0}$$

$$\Longrightarrow \begin{bmatrix} 1 & 1 & \cdots & 1 \end{bmatrix} \begin{bmatrix} \alpha^{j_1} & (\alpha^{j_1})^2 & \cdots & (\alpha^{j_1})^{2t} \\ \alpha^{j_2} & (\alpha^{j_2})^2 & \cdots & (\alpha^{j_2})^{2t} \\ \alpha^{j_3} & (\alpha^{j_3})^2 & \cdots & (\alpha^{j_3})^{2t} \\ \vdots & \vdots & & \vdots \\ \alpha^{j_\delta} & (\alpha^{j_\delta})^2 & \cdots & (\alpha^{j_\delta})^{2t} \end{bmatrix} = \mathbf{0}$$

Lower Bound on Minimum Distance

$$\implies \begin{bmatrix} 1 & 1 & \cdots & 1 \end{bmatrix} \begin{bmatrix} \alpha^{j_1} & \left(\alpha^{j_1}\right)^2 & \cdots & \left(\alpha^{j_1}\right)^\delta \\ \alpha^{j_2} & \left(\alpha^{j_2}\right)^2 & \cdots & \left(\alpha^{j_2}\right)^\delta \\ \alpha^{j_3} & \left(\alpha^{j_3}\right)^2 & \cdots & \left(\alpha^{j_3}\right)^\delta \\ \vdots & \vdots & & \vdots \\ \alpha^{j_\delta} & \left(\alpha^{j_\delta}\right)^2 & \cdots & \left(\alpha^{j_\delta}\right)^\delta \end{bmatrix} = \mathbf{0}$$

$$\implies \begin{vmatrix} \alpha^{j_1} & \left(\alpha^{j_1}\right)^2 & \cdots & \left(\alpha^{j_1}\right)^\delta \\ \alpha^{j_2} & \left(\alpha^{j_2}\right)^2 & \cdots & \left(\alpha^{j_2}\right)^\delta \\ \alpha^{j_3} & \left(\alpha^{j_3}\right)^2 & \cdots & \left(\alpha^{j_3}\right)^\delta \\ \vdots & \vdots & & \vdots \\ \alpha^{j_\delta} & \left(\alpha^{j_\delta}\right)^2 & \cdots & \left(\alpha^{j_\delta}\right)^\delta \end{vmatrix} = 0$$

Lower Bound on Minimum Distance

$$\Longrightarrow \alpha^{(j_1+\cdots+j_\delta)} \begin{vmatrix} 1 & \alpha^{j_1} & \cdots & \alpha^{(\delta-1)j_1} \\ 1 & \alpha^{j_2} & \cdots & \alpha^{(\delta-1)j_2} \\ 1 & \alpha^{j_3} & \cdots & \alpha^{(\delta-1)j_3} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{j_\delta} & \cdots & \alpha^{(\delta-1)j_\delta} \end{vmatrix} = 0$$

- $\alpha^{j_1+\cdots+j_\delta} \neq 0$ since α is a nonzero field element
- The determinant is a Vandermonde determinant which is not zero
- This contradicts our assumption that a nonzero codeword of weight $\delta \leq 2t$ exists

Questions? Takeaways?