BCH Codes

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

October 14, 2014

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 $\varphi_1(x), \varphi_2(x), \ldots, \varphi_{2t}(x)$

Degree of Generator Polynomial

$$g(x) = \text{LCM}\{\varphi_1(x), \varphi_2(x), \varphi_3(x), \ldots, \varphi_{2t}(x)\}$$

- If i is an even integer, then $i = i'2^a$ where i' is odd
- Since $\alpha^i = \left(\alpha^{i'}\right)^{2^a}$, α^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

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

BCH Codes of Length 15

- Let α be a primitive element of F_{16} and a root of $x^4 + x + 1$

Power	Polynomial	Tuple
0	0	$(0\ 0\ 0\ 0)$
1	1	$(1\ 0\ 0\ 0)$
α	α	$(0\ 1\ 0\ 0)$
α^2	α^2	$(0\ 0\ 1\ 0)$
α^3	α^3	$(0\ 0\ 0\ 1)$
α^4	$1+\alpha$	$(1\ 1\ 0\ 0)$
α^5	$\alpha+\alpha^2$	$(0\ 1\ 1\ 0)$
α^6	$\alpha^2+\alpha^3$	$(0\ 0\ 1\ 1)$
α^7	$1+\alpha+\alpha^3$	$(1\ 1\ 0\ 1)$
α^8	$1+\alpha^2$	$(1\ 0\ 1\ 0)$
α^9	$\alpha+\alpha^3$	$(0\ 1\ 0\ 1)$
α^{10}	$1+\alpha+\alpha^2$	$(1\ 1\ 1\ 0)$
α^{11}	$\alpha+\alpha^2+\alpha^3$	$(0\ 1\ 1\ 1)$
α^{12}	$1+\alpha+\alpha^2+\alpha^3$	$(1\ 1\ 1\ 1)$
α^{13}	$1+\alpha^2+\alpha^3$	$(1\ 0\ 1\ 1)$
α^{14}	$1+\alpha^3$	$(1\ 0\ 0\ 1)$

BCH Codes of Length 15

- Let α be a primitive element of F_{16} and a root of $x^4 + x + 1$
- The minimal polynomials of F_{16} are $\mathbb{F}_2[x]$ factors of $x^{16} + x$

$$x^{16}+x = x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$$

- A single error correcting BCH code of length 15 has generator polynomial $g(x) = \varphi_1(x) = x^4 + x + 1$
- A double error correcting BCH code of length 15 has generator polynomial

$$g(x) = \text{LCM}\{\varphi_1(x), \varphi_3(x)\} = (x^4+x+1)(x^4+x^3+x^2+x+1)$$

- The maximum value of t for a BCH code of length 15 is 7
- What is the generator polynomial for correcting seven errors?

Questions? Takeaways?