Lecture 12

Note Title 1/31/2008

t-error-correcting BCH codes:

$$n = 2^m - 1 \quad , \quad d = 2t+1$$

$$k \geq n - mt$$

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{n-1} \\ \vdots & & & & \\ 1 & \alpha^{d-1} & (\alpha^{d-1})^2 & \cdots & (\alpha^{d-1})^{n-1} \end{bmatrix}$$

$\alpha \in F_{2^m}$, primitive

Properties: 1) BCH codes are linear

2) BCH codes are cyclic.

if $[v_0 \; v_1 \; \cdots \; v_{n-1}] \in$ BCH code

then $[v_{n-1} \; v_0 \; v_1 \; \cdots \; v_{n-2}] \in$ BCH code

i^{th} row of H:

$$\alpha^i \times \left(v_0 + v_1(\alpha^i) + v_2(\alpha^i)^2 + \cdots + v_{n-1}(\alpha^i)^{n-1} = 0\right)$$

$$v_{n-1} + v_0(\alpha^i) + v_1(\alpha^i)^2 + \cdots + v_{n-2}(\alpha^i)^{n-1} = 0$$

Ex: $t = 1$, $n = 7$ $\quad \alpha \in F_8$, primitive, $\alpha^7 = 1$, $\alpha^3 = 1 + \alpha$

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \end{bmatrix} \rightarrow X$$

$\rightarrow$ Convert to binary

	α^2 α 1
0	0 0 0
1	0 0 1
α	0 1 0
α^2	1 0 0
α^3	0 1 1
α^4	1 1 0
α^5	1 1 1
α^6	1 0 1

$$H_b = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$\downarrow$

$(7, 4, 3)$ Hamming code

$\hookrightarrow$ cyclic code!!

3) Useful to interpret codewords as polynomials

$$\underline{c} = [c_0 \; c_1 \; c_2 \cdots c_{n-1}] \in \text{BCH code}$$

(t – error-correcting)

$\updownarrow$

$$c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$$

row i of H: $c_0 + c_1 (\alpha^i) + c_2 (\alpha^i)^2 + \cdots + c_{n-1} (\alpha^i)^{n-1} = 0$

(or) $c(\alpha^i) = 0$

$\longrightarrow$ $c(x) \in$ BCH code

iff $c(\alpha^i) = 0 \quad i = 1, 2, \ldots, d-1$

{poly. of deg $\leq n-1$
binary coefficients}

$\longrightarrow$ $c(x) \in$ BCH code

iff $(x - \alpha^i) \mid c(x) \quad i = 1, 2, \ldots, d-1$

$\longrightarrow$ $c(x) \in$ BCH code

iff $(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{2t}) \mid c(x)$.

Ex: (7, 4, 3) Hamming code

$t = 1$

$d = 3$

$$H = \begin{bmatrix} p_0 & p_1 & p_2 & & & & \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \longrightarrow p_2 = \underline{m} \cdot [0\ 1\ 1]$$

$\underbrace{\qquad}_{p} \quad \underbrace{\qquad\qquad}_{m}$

$$\underline{c} = [0\ 1\ 0\ 0\ 0\ 1\ 1]$$

$$c(x) = x + x^5 + x^6$$

$$c(\alpha) = \alpha + \alpha^5 + \alpha^6 = 0$$

$$c(\alpha^2) = \alpha^2 + \alpha^3 + \alpha^5 = 0$$

	α^2 α 1
0	0 0 0
1	0 0 1
α	0 1 0
α^2	1 0 0
α^3	0 1 1
α^4	1 1 0
α^5	1 1 1
α^6	1 0 1

$$(x+\alpha)(x+\alpha^2) = x^2 + (\alpha+\alpha^2)x + \alpha^3 = x^2 + \alpha^4 x + \alpha^3$$

$$\begin{array}{r} x^4 \\ x^2 + \alpha^4 x + \alpha^3 \overline{)\ x^6 + x^5 + x} \\ - \\ \hline 0 \end{array}$$

4) $(x+\alpha)(x+\alpha^2)\cdots(x+\alpha^{2t}) \mid c(x)$

$f(x)$

BCH code
(t-error-correcting)

Any $c(x)$ is a multiple of $f(x)$.

requires additional conditions.
why? binary coeffs!!

Minimal polynomial:

$\beta \in F_{2^m}$. Minimal polynomial of β is the least degree binary polynomial with β as a root.

$n = 2^m - 1 \qquad \beta \in F_{2^m}^* \qquad ord(\beta) \mid n$

$\Rightarrow \beta^n = 1$

β is a root of $x^n + 1 \in F_2[x]$