Lecture 11

Note Title 1/30/2008

GF(2^m) or $F_{2^m} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}\}$ $\alpha^{2^m-1} = 1$

$\alpha^m = a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}$

$\pi(\alpha)$: deg-m primitive

BCH codes

Bose-Chaudiri-Hocque...

d : target minimum distance

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

→ we will construct H to achieve d using elements from F_{2^m}.

H : $r \times n$ matrix with entries from F_{2^m}

$$C = \{ \underline{v} \in F_2^n : H\underline{v}^T = \underline{0} \}$$

$$\begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1n} \\ h_{21} & \cdots & & \\ \vdots & & & \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} h_{11}v_1 + h_{12}v_2 + \cdots + h_{1n}v_n \\ \vdots \end{bmatrix}$$

in F_{2^m}

$v_i \in \{0, 1\}$

$\in C$

should be $\underline{0}$

→ dimension is a problem.

Ex: 1) $F_4 = \{0, 1, \alpha, \alpha^2\}$ $\alpha^3 = 1$, $\alpha^2 = \alpha + 1$

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ \alpha & 1 & 0 \end{bmatrix} \qquad C = \{\underline{v} \in F_2^3 : H\underline{v}^T = \underline{0}\}$$

$[0\ 0\ 0] \in C$

$C = [000\}$

2) $$H = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ \alpha & \alpha^2 & 1 \end{bmatrix} \qquad C = [000, 111\}$$

$$H = \begin{matrix} r \\ \end{matrix} \overset{n}{\begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1n} \\ h_{21} & h_{22} & \cdots & h_{2n} \\ \vdots & \vdots & & \vdots \\ h_{r1} & h_{r2} & \cdots & h_{rn} \end{bmatrix}} \qquad h_{ij} \in F_{2^m}$$

first row: one equation in F_{2^m} ← $h_{11} v_1 + h_{12} v_2 + \cdots + h_{1n} v_n = 0$

- replace h_{ij} by its vector notation to get m equations over F_2 $(m \times 1)$

Ex: 1)

	α	1
0	0	0
1	0	1
α	1	0
α^2	1	1

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ \alpha & 1 & 0 \end{bmatrix} \overset{\text{to binary}}{\Longrightarrow} \begin{matrix} \\ 4 \end{matrix} \overset{3}{\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}}$$

2) $H = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ \alpha & \alpha^2 & 1 \end{bmatrix}$ $\xrightarrow{\text{to binary}}$ $\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$ → X, → X

lin. dep. on 1st two rows

3) $H = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha \end{bmatrix} \Rightarrow \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$ → X, → X

$C = \{000, 111\}$

RREF (H) in F_4 $= \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$

why?

$$(x+y)^2 = x^2 + y^2 + 2xy$$

char. $= 2 \Rightarrow$ $x^2 + y^2 = (x+y)^2$

char. $= p \Rightarrow$ $x^p + y^p = (x+y)^p$

Eqn. from 1st row $\longrightarrow v_1 \cdot 1 + v_2 \cdot \alpha + v_3 \alpha^2 = 0$

Squaring, $(v_1 \cdot 1 + v_2 \cdot \alpha + v_3 \cdot \alpha^2)^2 = 0$

$$v_1^2 \cdot 1 + v_2^2 \cdot \alpha^2 + v_3^2 \cdot \alpha = 0$$

$v_i \in \{0, 1\} \Rightarrow v_i^2 = v_i$

$$v_1 \cdot 1 + v_2 \cdot \alpha^2 + v_3 \cdot \alpha = 0$$

BCH codes (definition): $n = 2^m - 1$, d: minimum distance

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

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & (\alpha^2)^3 & \cdots & (\alpha^2)^{n-1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{d-1} & (\alpha^{d-1})^2 & (\alpha^{d-1})^3 & \cdots & (\alpha^{d-1})^{n-1} \end{bmatrix}$$

min. distance $\geq d$?

Ex: $F_{16} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\}$, $\alpha^{15} = 1$, $\alpha^4 = \alpha + 1$

$n = 15$

$d = 3$

BCH: $$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \cdots & \alpha^{14} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \cdots & \alpha^{28} \end{bmatrix}$$

$\Downarrow$ to binary

only first row provides independent eqns.

why? (second row) = (first row)^2

$\longrightarrow$ $n = 15$, binary Hamming code.

$\longrightarrow$ $(15, 11, 3)$ code.

$d = 5$

BCH:

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{14} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \cdots & \alpha^{28} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \cdots & \alpha^{42} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \cdots & \alpha^{56} \end{bmatrix}$$

$\alpha^{28} \rightarrow X$ lin. dep.

$\alpha^{56} \rightarrow X$ in binary version.

$n = 15, \quad d \geq 5, \quad k = ?$

Char $= 2 \Rightarrow$

$$(x+y)^{2^s} = x^{2^s} + y^{2^s}$$

In binary, row 1 & 3 provide 8 lin. ind. checks

$$k = 15 - 8 = 7$$

$\longrightarrow$ $(15, 7, 5)$ code

Proof for min. distance: (BCH bound)

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{i} & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2i} & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 1 & \alpha^{d-1} & (\alpha^{d-1})^2 & \cdots & \alpha^{(d-1)i} & \cdots & (\alpha^{d-1})^{n-1} \end{bmatrix}$$

(α^i: i^{th} col)

Suppose $w \leq d-1$ and $\underline{v} = [v_0 \; \cdots \; v_{n-1}]$ with $wt(\underline{v}) = w$ s.t.

$$H \underline{v}^T = \underline{0}$$

Let 1s in $\underline{v}$ be at positions $i_1, i_2, \ldots, i_w$

$$\begin{bmatrix} \alpha^{i_1} & \alpha^{i_2} & \cdots & \alpha^{i_w} \\ \alpha^{2i_1} & \alpha^{2i_2} & \cdots & \alpha^{2i_w} \\ \vdots & \vdots & & \vdots \\ \alpha^{(d-1)i_1} & \alpha^{(d-1)i_2} & \cdots & \alpha^{(d-1)i_w} \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} = \underline{0}$$

$$\begin{bmatrix} \alpha^{i_1} & \alpha^{i_2} & \cdots & \alpha^{i_w} \\ \alpha^{2i_1} & \alpha^{2i_2} & \cdots & \alpha^{2i_w} \\ \vdots & \vdots & & \vdots \\ \alpha^{wi_1} & \alpha^{wi_2} & \cdots & \alpha^{wi_w} \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} = \underline{0}$$

$\det \neq 0$

$w \times w$

Vandermonde matrix

$$\begin{bmatrix} a_1 & a_2 & \cdots & a_s \\ a_1^2 & a_2^2 & \cdots & a_s^2 \\ \vdots & \vdots & & \vdots \\ a_1^s & a_2^s & \cdots & a_s^s \end{bmatrix} = \prod_{i<j} (a_i - a_j)$$

$n = 2^m - 1$, d: min-distance

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

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^i & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2i} & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 1 & \alpha^{d-1} & (\alpha^{d-1})^2 & \cdots & \alpha^{(d-1)i} & \cdots & (\alpha^{d-1})^{n-1} \end{bmatrix}$$

$m = 10$

$n = 1023$, $d \geq 17$

$\alpha \in F_{1024}$, primitive

→ implementation can be a problem

→ Finding k is also a problem.

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

H: $2t \times n$ matrix

↓

even-numbered rows are lin. dep.

H: in binary will have $\leq mt$ lin. indep. rows

$k \geq n - mt \rightarrow$ tight for small t

$m = 8$, BCH code parameters

$t = 1$	$(255, 247, 3)$	$\rightarrow$ binary Hamming code
$t = 2$	$(255, 239, 5)$	⋮
$t = 3$	$(255, 231, 7)$	$t = 16$
$t = 4$	$(255, 223, 9)$	$(255, 127, 33)$