Lecture 15

Note Title 2/7/2008

Reed-Solomon Codes:

$\longrightarrow$ codes over F_{2^m}.

binary codes: subspace of F_2^n

Code over F_{2^m}: subspace of $F_{2^m}^n$
(2^m-ary code)

(n, k, d) code over F_{2^m}: k-dimensional subspace of $F_{2^m}^n$

Codeword $\underline{c} = [c_0\ c_1\ \cdots\ c_{n-1}]$ $\quad c_i \in F_{2^m}$ $\longrightarrow$ called symbols

$\downarrow$

mn-bit representation in practice.

Generator matrix $G = \begin{matrix} k \\ \end{matrix}\overset{n}{\begin{bmatrix} \text{—} & \underline{g}_1 & \text{—} \\ & \vdots & \\ \text{—} & \underline{g}_k & \text{—} \end{bmatrix}}$

$\underline{g}_1, \underline{g}_2, \cdots, \underline{g}_k$: basis for the code

Parity-check matrix, $H = \begin{matrix} n-k \\ \end{matrix}\overset{n}{\begin{bmatrix} \text{—} & \underline{h}_1 & \text{—} \\ & \vdots & \\ \text{—} & \underline{h}_{n-k} & \text{—} \end{bmatrix}}$

$\underline{h}_1, \cdots, \underline{h}_{n-k}$: basis for dual code

$\underline{x}, \underline{y} \in \mathbb{F}_{2^m}^n$ $\quad d_H(\underline{x}, \underline{y}) =$ # of positions in which they differ

$wt_H(\underline{x}) =$ # of non zero positions

$d_H(\underline{x}, \underline{y}) = wt_H(\underline{x} + \underline{y})$

$d =$ min # of places in which two different codewords differ.

$=$ min wt. of a nonzero codeword

$=$ min # of linearly dependent columns of H.

$\#$ of codewords $= (2^m)^k = 2^{mk}$

Singleton bound: $d \leq n - k + 1$.

$t = \left\lfloor \frac{d-1}{2} \right\rfloor$: error-correcting capability

Definition: A t-error-correcting Reed-Solomon code over F_{2^m} with length $n = 2^m - 1$ is defined by the parity-check matrix

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

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

By the same proof as for the BCH case,

$$d \geq 2t+1$$

If $\underline{c} = [c_0 \; c_1 \; \cdots \; c_{n-1}]$ is a codeword,

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

then

$$c(\alpha) = 0 \iff (x+\alpha) \mid c(x)$$
$$c(\alpha^2) = 0 \iff (x+\alpha^2) \mid c(x)$$
$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$
$$c(\alpha^{2t}) = 0 \iff (x+\alpha^{2t}) \mid c(x)$$

$c(x)$ is a codeword iff

$$c(x) = m(x)\underbrace{(x+\alpha)(x+\alpha^2)\cdots(x+\alpha^{2t})}$$

$g(x)$: generator polynomial

$\deg \le n-1$

$\deg \le n-2t-1$

$\Rightarrow k = n-2t$

Using Singleton & BCH bounds, $d = 2t+1$.

t-error-correcting RS code over F_{2^m} : $(2^m-1,\ 2^m-2t-1,\ 2t+1)$

$\downarrow$ MDS codes.

$\downarrow$ n $\quad$ $\downarrow$ $n-2t$ $\quad$ $\downarrow$ d

Ex: 1) F_4 $\quad n = 3$ $\quad \alpha \in F_4,\ \alpha^3 = 1,\ \alpha^2 = 1+\alpha$

$t=1$: $\quad g(x) = (x+\alpha)(x+\alpha^2) = x^2+x+1$

$k = 1$, $d = 3$

	α	1
0	0	0
1	0	1
α	1	0
α^2	1	1

Code $= \{000,\ 111,\ \alpha\alpha\alpha,\ \alpha^2\alpha^2\alpha^2\}$

$\downarrow$ $\quad$ $\downarrow$

Binary Expansion $\{000000,\ 010101,\ 101010,\ 111111\}$

2) F_8, $n=7$, $\alpha \in F_8$, $\alpha^7=1$, $\alpha^3=1+\alpha$

$t=1$: $g(x)=(x+\alpha)(x+\alpha^2)$

$k=7-2=5$

$(7,5,3)$ code

↓ binary expansion

$(21,15,\geq 3)$

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

$(7,3,5)$ code

3) F_{256}, $n=255$ $\alpha \in F_{256}$, primitive

$t=16$: $g(x)=(x+\alpha)\cdots(x+\alpha^{32})$

$(255,223,33)$ code $\longrightarrow (2040,1784,33)$

→ Systematic encoding extends

F_{256} : t errors

RS :→ [m k]

m → message → k bytes

k → $2t$ bytes of parity

$$k = 255 - 2t$$

→ RS codes are cyclic.