Reed-Solomon Codes

Note Title

n: block length, designed error-correcting capability $= t$

$\beta \in GF(2^m)$, $\text{ord}(\beta) \geq n$

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

$\text{rank}(H) = 2t$

$$\text{RS Code} = \left\{ \underline{c} \in \underline{GF(2^m)}^n : H\underline{c}^T = \underline{0} \right\}$$

$H\underline{c}^T = \underline{0}$ $\quad \underline{c} = [c_0\ c_1\ c_2 \cdots c_{n-1}]$

$c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \quad c_i \in GF(2^m)$

first row: $c(\beta) = 0 \Leftrightarrow (x+\beta) \mid c(x)$

2^{nd} row: $c(\beta^2) = 0 \Leftrightarrow (x+\beta^2) \mid c(x)$

$2t$-th row: $c(\beta^{2t}) = 0 \Leftrightarrow (x+\beta^{2t}) \mid c(x)$

$\Leftrightarrow \underbrace{(x+\beta)(x+\beta^2)\cdots(x+\beta^{2t})}_{g(x)} \mid c(x)$

$\deg = 2t$ $\quad g(x)$: generator polynomial

RS code $= \{ c(x) = m(x)g(x) :$

$m(x) = m_0 + m_1 x + \dots + m_{k-1} x^{k-1},$

$k = n - 2t \}$

Dimension $= n - 2t = k$

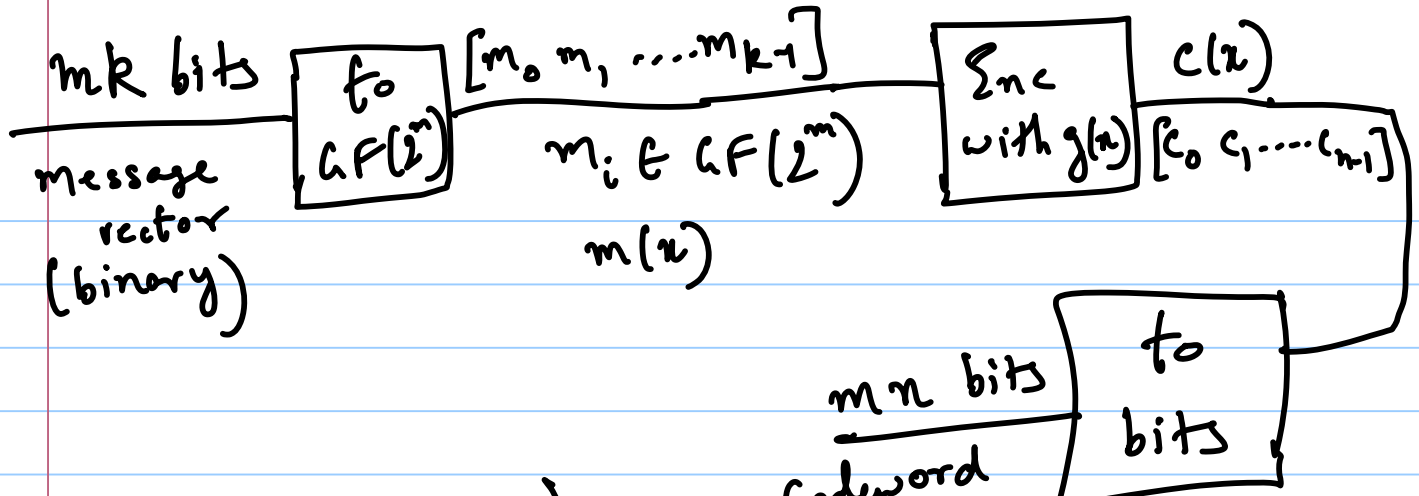
Minimum distance $= 2t + 1 = n - k + 1$

$\Rightarrow$ RS codes have parameters $(n, k, d = n - k + 1)$ ($k \in GF(2^m)$)

$\Downarrow$

MDS codes

n : elements of $GF(2^m)$



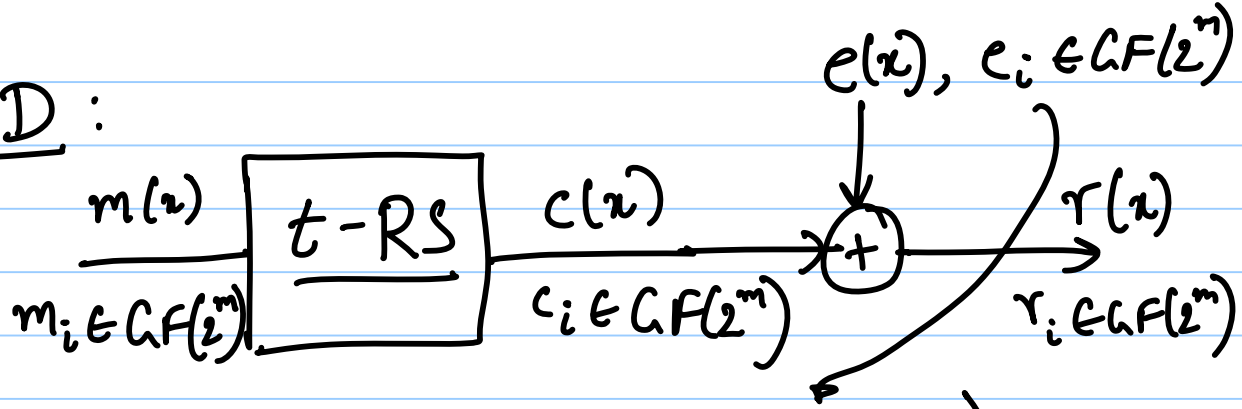
$m = 8$, $GF(256)$

Ex: $k = 239$, $n = 255$

$mk = 1912$ bits, $nm = 2040$ bits

$n = ord(\beta) \Rightarrow$ RS codes will be cyclic.

BDD:



w errors $\Rightarrow wt([e_0\ e_1 \cdots e_{n-1}]) = w$

$w \le t$ $\qquad P_r = \binom{n}{w} p_s^{\,w} (1-p_s)^{n-w}$

$P_r(e_0 \neq 0) = 1 - (1-p)^m = p_s$ "prob of symbol error"

Form of $e(x)$ with ω errors: $e(x) = E_1 x^{i_1} + E_2 x^{i_2} + \cdots + E_\omega x^{i_\omega}$

$E_i \in GF(2^m)$

Decoding task: Find $i_1, i_2, \ldots, i_\omega$ and $E_1, E_2, \ldots, E_\omega$.

Syndrome:

$$S_1 = r(\beta) = E_1 \beta^{i_1} + E_2 \beta^{i_2} + \cdots + E_\omega \beta^{i_\omega}$$

$$S_2 = r(\beta^2) = E_1 \beta^{2i_1} + E_2 \beta^{2i_2} + \cdots + E_\omega \beta^{2i_\omega}$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$S_{2t} = r(\beta^{2t}) = E_1 \beta^{2t i_1} + \cdots + E_\omega \beta^{2t i_\omega}$$

Error locator: $X_j = \beta^{i_j}$

$j = 1, 2, \ldots, \omega$

Error values: E_j

Known:

$$S_1 = E_1 X_1 + E_2 X_2 + \cdots + E_\omega X_\omega$$
$$S_2 = E_1 X_1^2 + E_2 X_2^2 + \cdots + E_\omega X_\omega^2$$
$$\vdots$$
$$S_{2t} = E_1 X_1^{2t} + E_2 X_2^{2t} + \cdots + E_\omega X_\omega^{2t}$$

Error locator poly, $\sigma(x) = (1 + X_1 x)(1 + X_2 x) \cdots (1 + X_\omega x)$

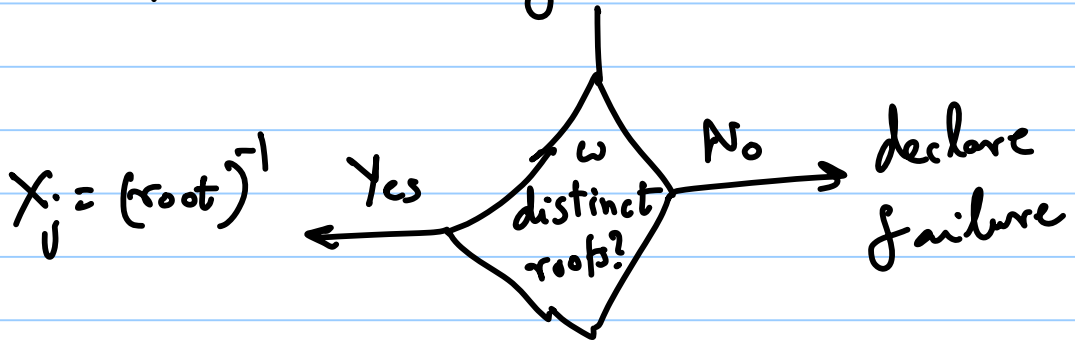
$$= 1 + \sigma_1 x + \cdots + \sigma_\omega x^\omega$$

$$S(x) = S_1 x + S_2 x^2 + \cdots + S_{2t} x^{2t}$$

$S(x)\sigma(x)$: coeffs of $x^{\omega+1}, \ldots, x^{2t}$ are zero

Find $\sigma_1, \sigma_2, \ldots, \sigma_\omega$.

Find roots of $\sigma(x)$ in $GF(2^m)$.



→ Use w syndrome equations (now linear in E_j)

to find $E_1, E_2, \ldots, E_w$.