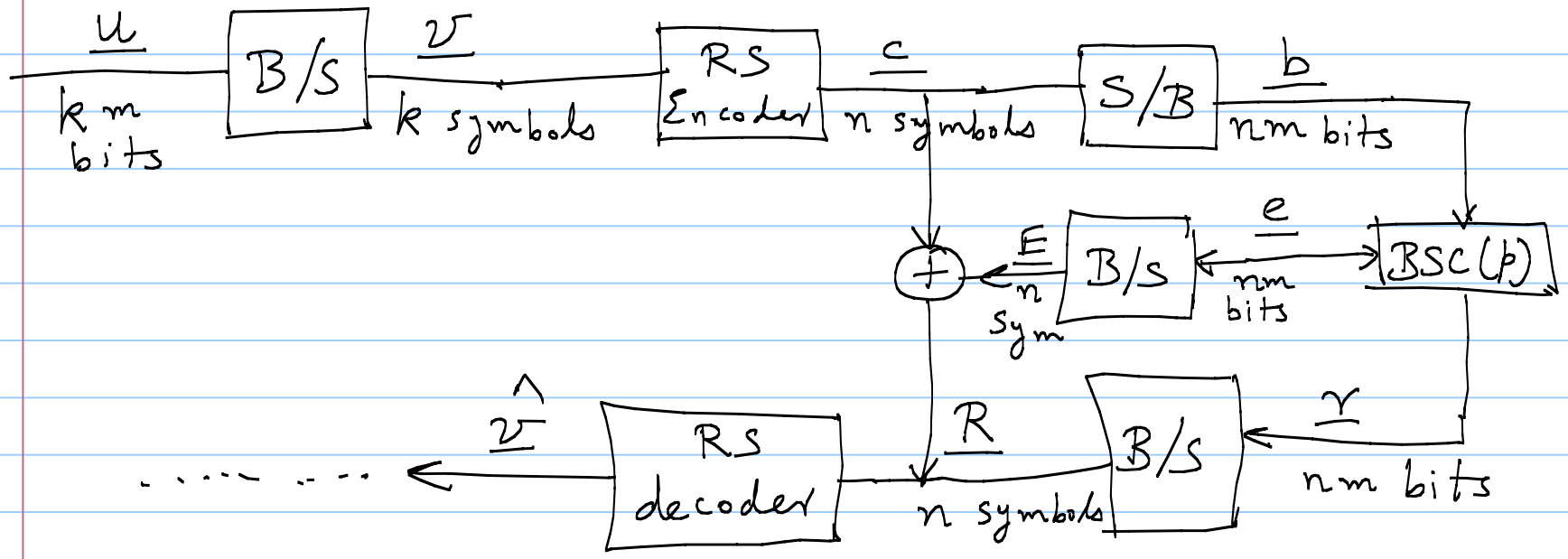
Lecture 16

Note Title 2/8/2008

$n = 2^m - 1 \qquad (n, \underset{k}{n-2t}, 2t+1)$ RS code



$$\underline{e} = [\underbrace{e_{11}\, e_{12} \cdots e_{1m}}_{E_1}\ \underbrace{e_{21}\, e_{22} \cdots e_{2m}}_{E_2} \cdots \underbrace{e_{n1}\, e_{n2} \cdots e_{nm}}_{E_n}]$$

$$\underline{E} = [E_1 \quad E_2 \quad \cdots \quad E_n]$$

Peterson-Gorenstein-Zierler Decoder: (PGZ)

$$c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in$$ t-error-correcting RS code

$$c_i \in F_{2^m}.$$

$$R(x) = R_0 + R_1 x + \cdots + R_{n-1} x^{n-1} \rightarrow \text{received poly.}$$

$$R(x) = c(x) + E(x)$$

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

Syndromes:

$$S_1 = R(\alpha) = E(\alpha)$$
$$S_2 = E(\alpha^2)$$
$$S_3 = E(\alpha^3)$$
$$\vdots \qquad \vdots$$
$$S_{2t} = E(\alpha^{2t})$$

Suppose w symbol errors happened at positions $i_1, i_2, \ldots, i_w$

$$E(x) = Y_1 x^{i_1} + Y_2 x^{i_2} + \cdots + Y_w x^{i_w}$$

$$S_1 = Y_1 X_1 + Y_2 X_2 + \cdots + Y_w X_w$$

$$S_2 = Y_1 X_1^2 + Y_2 X_2^2 + \cdots + Y_w X_w^2$$

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

$$S_{2t} = Y_1 X_1^{2t} + Y_2 X_2^{2t} + \cdots + Y_w X_w^{2t}$$

$X_j = \alpha^{i_j}$ — Error locators

Error locator polynomial

$$\Lambda(x) = (1 + X_1 x)(1 + X_2 x) \cdots (1 + X_w x)$$
$$= 1 + \Lambda_1 x + \Lambda_2 x^2 + \cdots + \Lambda_w x^w$$

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

$$= Y_1 X_1 x + Y_2 X_2 x + \cdots + Y_\omega X_\omega x$$
$$+ Y_1 X_1^2 x^2 + Y_2 X_2^2 x^2 + \cdots + Y_\omega X_\omega^2 x^2$$
$$+ \vdots$$
$$+ Y_1 X_1^{2t} x^{2t} + Y_2 X_2^{2t} x^{2t} + \cdots + Y_\omega X_\omega^{2t} x^{2t}$$

$(1 + X_1 x)$
$(1 + X_2 x)$
$\vdots$
$(1 + X_\omega x)$

$S(x) \Lambda(x) =$ poly with coefficients from Y_i, X_i etc.

deg $2t$ deg ω

BUT $x^{\omega+1}$ to x^{2t} will be absent!!

$$Y_1 (X_1 x + X_1^2 x^2 + \cdots + X_1^{2t} x^{2t})(1 + X_1 x) = Y_1 (X_1 x + X_1^{2t+1} x^{2t+1})$$

$$S_1 = Y_1 X_1 + Y_2 X_2 + \cdots + Y_w X_w$$

$$S_2 = Y_1 X_1^2 + Y_2 X_2^2 + \cdots + Y_w X_w^2$$

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

$$S_{2t} = Y_1 X_1^{2t} + Y_2 X_2^{2t} + \cdots + Y_w X_w^{2t}$$

$\Lambda(x) = (1 + X_1 x) \cdots (1 + X_w x)$ ⇓

$S(x)\Lambda(x)$ having zero as coefficients of x^{w+1} to x^{2t} terms.

$$S(x)\Lambda(x) = \left(S_1 x + S_2 x^2 + S_3 x^3 + \cdots + S_{2t} x^{2t}\right)$$
$$\left(1 + \Lambda_1 x + \Lambda_2 x^2 + \cdots + \Lambda_w x^w\right)$$

$$S(x)\Lambda(x) = \left(S_1 x + S_2 x^2 + S_3 x^3 + \cdots + S_{2t} x^{2t}\right)$$
$$\left(1 + \Lambda_1 x + \Lambda_2 x^2 + \cdots + \Lambda_w x^w\right)$$

x^{w+1} : $S_{w+1} + S_w \Lambda_1 + S_{w-1} \Lambda_2 + \cdots + S_1 \Lambda_w = 0$

x^{w+2} : $S_{w+2} + S_{w+1} \Lambda_1 + S_w \Lambda_2 + \cdots + S_2 \Lambda_w = 0$

$\vdots$ $(w \leq t)$

x^{2w} : $S_{2w} + S_{2w-1} \Lambda_1 + S_{2w-2} \Lambda_2 + \cdots + S_w \Lambda_w = 0$

$\vdots$

x^{2t} : - - - -

$$\begin{bmatrix} S_w & S_{w-1} & \cdots & S_1 \\ S_{w+1} & S_w & \cdots & S_2 \\ \vdots & & & \\ S_{2w-1} & S_{2w-2} & \cdots & S_w \end{bmatrix} \begin{bmatrix} \Lambda_1 \\ \Lambda_2 \\ \vdots \\ \Lambda_w \end{bmatrix} = \begin{bmatrix} S_{w+1} \\ S_{w+2} \\ \vdots \\ S_{2w} \end{bmatrix}$$

nonsingular $\Rightarrow$ solvable

what about w?

$\longrightarrow$

$$M_\mu = \begin{bmatrix} S_\mu & S_{\mu-1} & \cdots & S_1 \\ S_{\mu+1} & S_\mu & \cdots & S_2 \\ \vdots & & & \vdots \\ S_{2\mu-1} & S_{2\mu-2} & \cdots & S_\mu \end{bmatrix}$$

$\mu = w, w+1, \ldots, t$

M_μ is nonsingular

M_μ is singular

Λ_i's to X_i's & Y_i's:

$$\Lambda(x) = (1+X_1 x)(1+X_2 x)\cdots(1+X_w x)$$

deg. w

X_i^{-1} : root of $\Lambda(x)$ in F_{2^m}.

Y_i's : given X_i, the original equations become linear in Y_i

($X_j = \alpha^{i_j}$)

$$\hat{E}(x) = \sum_{j=1}^{w} Y_j x^{i_j}, \quad \hat{C}(x) = R(x) + \hat{E}(x)$$