Reed-Solomon codes (vs. BCH codes)

Note Title

t-error-correcting RS code over $GF(2^m)$

length $= n \leq 2^m - 1$ $\quad \beta \in GF(2^m)$, primitive

$$\text{RS code} = \{ c(x) = m(x)\underbrace{(x+\beta)(x+\beta^2)\cdots(x+\beta^{2t})}_{g(x)} : \deg c(x) \leq n-1 \}$$

$k = n - 2t$

$d = 2t+1$

$|\text{RS code}| = (2^m)^k$

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

$$\sigma(x) = (1 + X_1 x)(1 + X_2 x) \cdots (1 + X_w x)$$
$$= 1 + \sigma_1 x + \sigma_2 x^2 + \cdots + \sigma_w x^w$$

→ linear eqns in $\sigma_1, \sigma_2, \ldots, \sigma_w$ + $S_1, S_2, \ldots, S_{2t}$

Key equation ←

$$\sigma(x) S(x) = Z(x) \bmod x^{2t+1}$$

$\sigma(x)$: ?

$Z(x)$: $\deg \le w$ ← minimized in decoder.

Correcting erasures & errors:

w errors and e erasures

$$\underline{r} = [r_0 \; r_1 \; \cdots \; r_{n-1}]$$

$$r_i \in \{GF(2^m), \varepsilon\}$$

ε: erasure

→ Set erased r_i to 0.

X_j: unknown error locations

X'_j: known erasure locations

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

$$\gamma(x) = (1 + X'_1 x)(1 + X'_2 x) \cdots (1 + X'_e x)$$

$\sigma(x)\gamma(x)S(x)$

$\deg = \omega + e$

$X_j = \beta^{i_j}$ → error locators

$X'_{j_m} = \beta^{j_m}$ → erasure locators

$$e(x) = E_1 x^{i_1} + \cdots + E_\omega x^{i_\omega} + E'_1 x^{j_1} + \cdots + E'_e x^{j_e}$$

$$S_l = e(\beta^l) = E_1 X_1^l + \cdots + E_\omega X_\omega^l + E'_1 X'^l_1 + \cdots + E'_e X'^l_e$$

$\sigma(x)\underbrace{\gamma(x)S(x)}_{\text{known}}$: has no terms from $x^{\omega+e+1}$ to x^{2t}

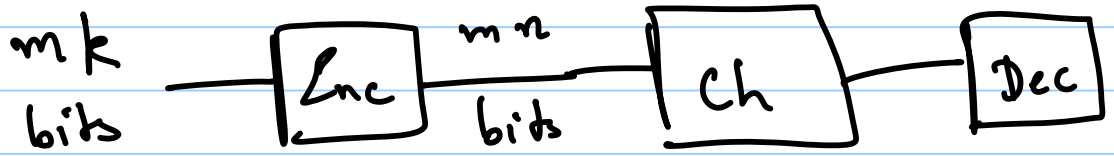
Can solve for w variables $\sigma_1, \sigma_2, \ldots, \sigma_w$

if $2t - w - e \geq w$

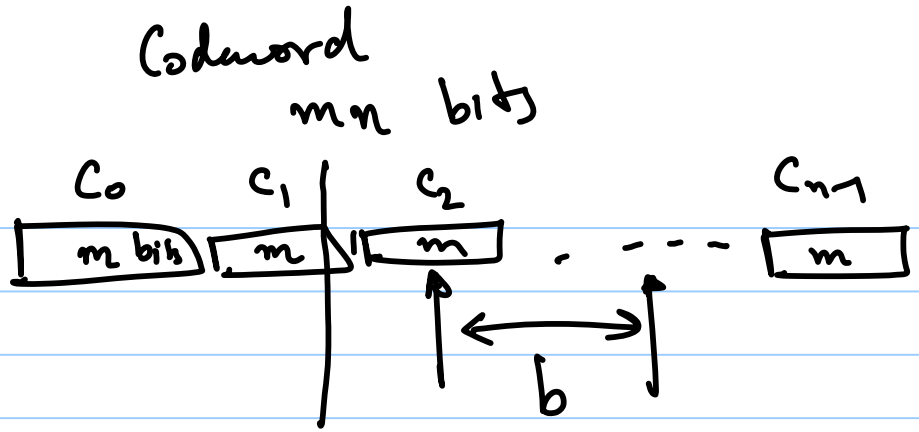
$$w + \frac{e}{2} \leq t$$

Burst-error-correcting capability:

(n, k) t-RS over $GF(2^m)$



errors in bursts of length 'b'.



$$\max b = (t-1)m + 1$$

Interleaving: depth-N

N codewords

$$\begin{bmatrix} c_0^{(1)} & c_1^{(1)} & \cdots & c_{n-1}^{(1)} \\ c_0^{(2)} & c_1^{(2)} & \cdots & c_{n-1}^{(2)} \\ \vdots & & & \\ c_0^{(N)} & c_1^{(N)} & \cdots & c_{n-1}^{(N)} \end{bmatrix}$$

$\max b \approx tNm$

BCH vs. RS codes

block length: fixed as n bits

Error-correcting capability: fixed as t bit errors (random)

BCH code

m: $2^m \geq n$ $(m \approx \log_2 n)$

$\beta \in GF(2^m)$, primitive

$k = n - mt$ (assume)

$n = 2040$

$m = 11$ $M = 8$

RS code

length-N RS code over $GF(2^M)$

$NM \geq n$

$2^M \cdot M \geq n$

$MK = MN - 2tM$

$t = 20 \quad n = 2040$

BCH

$m = 11$

$k = 2040 - 220$

$= 1820$

RS

$m = 8$

$(255, 215)$ over $GF(2^8)$

↓

$(2040, 1720)$ in bits

BCH: $P_r(\underset{(BDD)}{\text{block error}}) = 1 - \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}$

RS: $P_s = 1 - (1-p)^m$, $N = n/m$

$$P_r(\text{block error})_{(BDD)} = 1 - \sum_{i=0}^{t} \binom{N}{i} p_s^i (1-p_s)^{N-i}$$

→ BCH better than RS for fixed n & t (performance)

RS : lesser complexity, burst error models