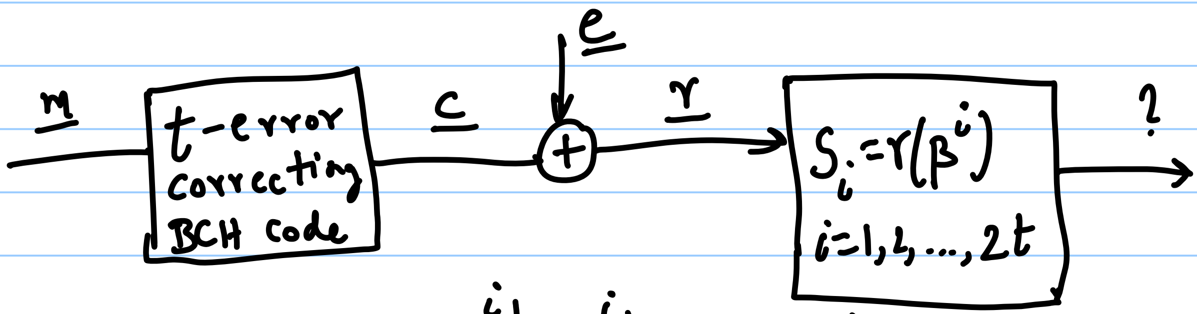
Decoding binary BCH codes

Note Title



$$e(x) = x^{i_1} + x^{i_2} + \cdots + x^{i_w}, \quad w \leq t$$

$$S_1 = X_1 + X_2 + \cdots + X_w$$

$$S_2 = X_1^2 + X_2^2 + \cdots + X_w^2$$

$$\vdots$$

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

error locators

error location

$$X_j = \beta^{i_j}$$

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

Error locator polynomial : Roots are $X_1^{-1}, X_2^{-1}, \dots, X_w^{-1}$

$$\deg \stackrel{!}{=} w \leftarrow \sigma(x) = (1+X_1 x)(1+X_2 x)\cdots\cdots(1+X_w x)$$

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

$$(\sigma_1, \sigma_2, \dots, \sigma_w) \leftarrow (X_1, X_2, \dots, X_w)$$

Coeffs of error locator poly

error locators

$$\sigma_w = X_1 X_2 \cdots X_w$$

$$\sigma_1 = X_1 + X_2 + \cdots + X_w$$

$$\sigma_2 = X_1 X_2 + X_1 X_3 + \cdots + X_{w-1} X_w$$

$$\vdots$$

Syndrome polynomial:

$$
\begin{aligned}
S(x) &= S_1 x + S_2 x^2 + S_3 x^3 + \cdots + S_{2t} x^{2t} \\
&= X_1 x + X_1^2 x^2 + X_1^3 x^3 + \cdots + X_1^{2t} x^{2t} \\
&\quad + X_2 x + X_2^2 x^2 + X_2^3 x^3 + \cdots + X_2^{2t} x^{2t} \\
&\quad + X_3 x + X_3^2 x^2 + X_3^3 x^3 + \cdots + X_3^{2t} x^{2t} \\
&\quad + \vdots \qquad + \ddots \qquad + \ddots \qquad \ddots \qquad + \ddots \\
&\quad + X_\omega x + X_\omega^2 x^2 + X_\omega^3 x^3 + \cdots + X_\omega^{2t} x^{2t}
\end{aligned}
$$

$$
S(x)\,\sigma(x) = S(x)(1 + X_1 x)(1 + X_2 x) \cdots\cdots (1 + X_\omega x)
$$

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

$$\left(S_1 x + S_2 x^2 + S_3 x^3 + \dots + S_{2t-1} x^{2t-1} + S_{2t} x^{2t}\right)$$

$$\left(1 + \sigma_1 x + \sigma_2 x^2 + \sigma_3 x^3 + \dots + \sigma_{\omega-1} x^{\omega-1} + \sigma_\omega x^\omega\right):$$

Coeff of $x^{\omega+1}$: $S_1 \sigma_\omega + S_2 \sigma_{\omega-1} + S_3 \sigma_{\omega-2} + \dots + S_\omega \sigma_1 + S_{\omega+1} = 0$

$x^{\omega+2}$: $S_2 \sigma_\omega + S_3 \sigma_{\omega-1} + S_4 \sigma_{\omega-2} + \dots + S_{\omega+1} \sigma_1 + S_{\omega+2} = 0$

$\vdots$

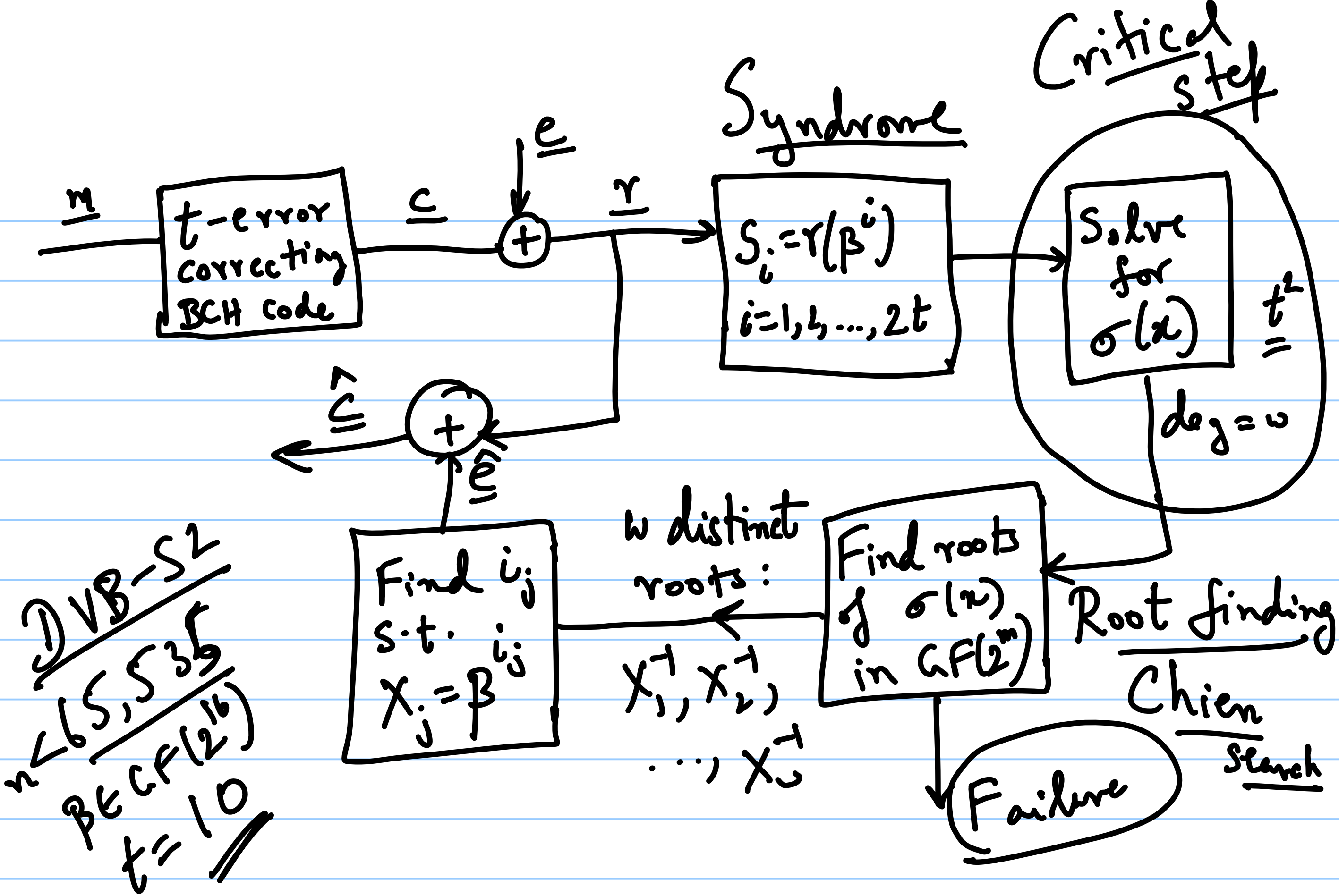
$x^{2\omega}$: $S_\omega \sigma_\omega + S_{\omega+1} \sigma_{\omega-1} + \dots + S_{2\omega-1} \sigma_1 + S_{2\omega} = 0$

$$\underbrace{\begin{bmatrix} S_1 & S_2 & \cdots & S_w \\ S_2 & S_3 & \cdots & S_{w+1} \\ S_3 & S_4 & \cdots & S_{w+2} \\ \vdots & & & \\ S_w & S_{w+1} & \cdots & S_{2w-1} \end{bmatrix}}_{\text{full rank}} \begin{bmatrix} \sigma_w \\ \sigma_{w-1} \\ \vdots \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} S_{w+1} \\ S_{w+2} \\ \vdots \\ S_{2w} \end{bmatrix}$$

w': actual # of errors

$w \le w'$: rank is full

$w > w'$: $\det = 0$



$\underline{m}$
t-error correcting BCH code
$\underline{c}$
$\underline{e}$
$\underline{r}$
Syndrome
$S_i = r(\beta^i)$
$i = 1, 2, \ldots, 2t$
Critical step
Solve for $\sigma(x)$
$\underline{\underline{t^2}}$
$\deg = \omega$
Find roots of $\sigma(x)$ in $GF(2^m)$
Root finding
Chien search
Failure
ω distinct roots:
$X_1^{-1}, X_2^{-1}, \ldots, X_\omega^{-1}$
Find i_j s.t. $X_j = \beta^{i_j}$
$\underline{\hat{e}}$
$\underline{\hat{c}}$
DVB-S2
$n < 65,535$
$\beta \in GF(2^{16})$
$t = 10$

Example: $n=15$, $\beta \in GF(16)$, primitive

$t=3$ zeros: $\beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6$

$$S(x)\,\sigma(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_\omega x^{\omega} + x^{2t+1} + \text{higher}$$

$\sigma(x) \to \deg \omega$

Find least degree $\sigma(x)$ that satisfies above equation.

$\sigma^{(1)}(x)$: deg 1

$\downarrow$

$\sigma^{(2)}(x) \ldots\ldots \sigma^{(\omega)}(x)$

$$S(x) = S_1 x + S_2 x^2 + \cdots$$

$$\sigma(x) = 1 + \sigma_1 x + \sigma_2 x^2 + \cdots$$

$$S_1 + \sigma_1 = 0$$

$$S(x)\underline{\underline{\sigma(x)}} = S_1 x + \underbrace{S_1\sigma_1 x^2 + S_2 x^2}_{} + \cdots$$

Set $\sigma_1 = S_2/S_1$

$$\sigma^{(1)}(x) = 1 + S_1 x$$

deg 3 term in $S(x)\sigma^{(1)}(x)$

$w=3$ errors:

$$\underbrace{\begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix}}_{\text{if det} \neq 0\text{, done}} \begin{bmatrix} \sigma_3 \\ \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} S_4 \\ S_5 \\ S_6 \end{bmatrix}$$

if det $=0$, $w=2$:

$$\begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} S_3 \\ S_4 \end{bmatrix}$$