# Decoding binary BCH codes

Note Title

$t$-error-correcting binary BCH code of length $n$

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

Zeros of code: $\beta, \beta^2, \ldots, \beta^{2t}$

Generator polynomial:

$$g(x) = LCM\left(M_{\beta}(x), M_{\beta^2}(x), \ldots, M_{\beta^{2t}}(x)\right)$$

$$= LCM\left(M_{\beta}(x), M_{\beta^3}(x), \ldots, M_{\beta^{2t-1}}(x)\right)$$

$$Code = \{ m(x)g(x) : \deg \leq n-1 \}$$

$$\boxed{n-k = \deg(g(x))}$$

$$\deg g(x) \leq mt$$

$$\Downarrow$$

$$k \geq n - mt \quad (\text{tight} : t \text{ small})$$

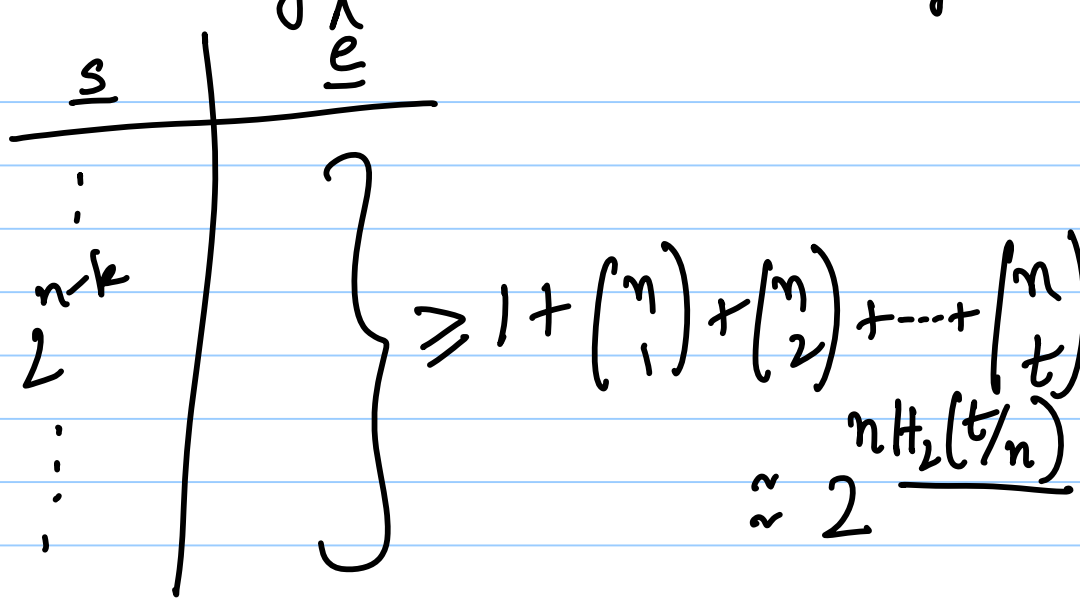
$c(x)$ : codeword iff $c(\beta) = 0$

$c(\beta^2) = 0$

$\vdots$

$c(\beta^{2t}) = 0$

Syndrome decoding: $t$-error-correcting




→ Not practical for moderate $n$ + $t$.

Simplifications:

- decoding in $GF(2^m)$
- bounded-distance decoding

↓

if $wt(\underline{e}) \leq t$, decoding will succeed

Else, no guarantees.

Ex:

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$d = 3 \Rightarrow t = 1$

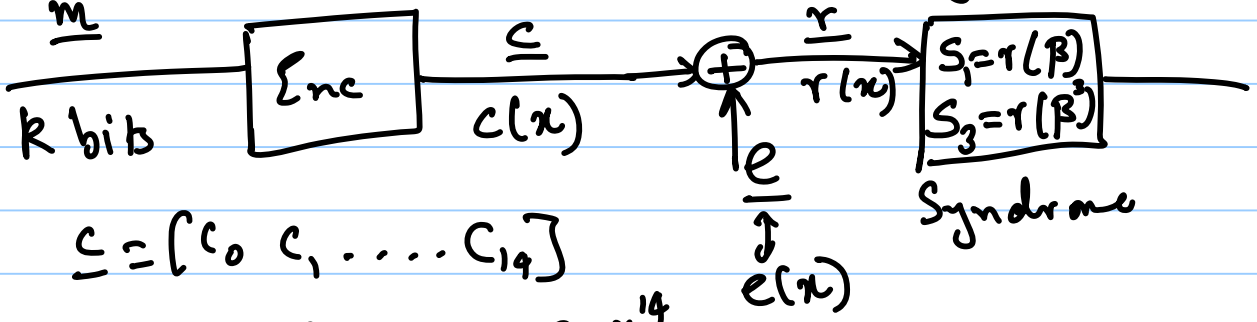
| $\underline{s}$ | $\hat{\underline{e}}$ | |
|---|---|---|
| 000 | 000000 | ← |
| 001 | 001000 | |
| 010 | 010000 | |
| 011 | 000010 | |
| 100 | 100000 | wt-2 error |
| 101 | 000001 | |
| 110 | 000100 | |
| 111 | 100010 | |

# Example of decoding

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

$t = 2$ Zeros: $\beta, \beta^2, \beta^3, \beta^4$ ; $g(x) = M_\beta(x) M_{\beta^3}(x)$

$k = 7$ $\deg = 8$




$\underline{c} = [c_0\ c_1 \dots c_{14}]$

$c(x) = c_0 + c_1 x + \dots + c_{14} x^{14}$

$S_1 = r(\beta) = e(\beta)$

$S_3 = r(\beta^3) = e(\beta^3)$

$wt(e) \le 2$ (bounded-distance assumption)

$\underline{wt(e)=2}$: $e(x) = x^i + x^j$, $0 \le i < j \le n-1$

$$\left.\begin{aligned} r(\beta) = S_1 &= \beta^i + \beta^j \\ r(\beta^3) = S_3 &= \beta^{3i} + \beta^{3j} \end{aligned}\right\} \text{ find } i \text{ and } j$$

$$S_3 = \underbrace{(\beta^i + \beta^j)}_{S_1}(\beta^{2i} + \beta^i\beta^j + \beta^{2j})$$

$$\beta^i\beta^j = S_3/S_1 + S_1^2$$

Solve: $y^2 + S_1 y + \left(\frac{S_3}{S_1} + S_1^2\right) = 0$ to get roots $y_0$ and $y_1$ in $GF(16)$.

if $y_0 \neq y_1$, then declare $y_0 = \beta^i$ and

$y_1 = \beta^j$.

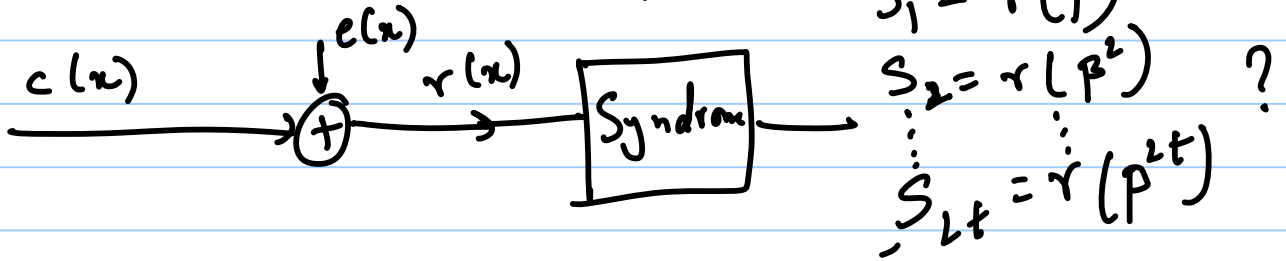
→ Flip the bits at $i$ & $j$.

→ Algebraic decoders

General case: $t$-error-correcting

$n$: $\beta \in GF(2^m)$, $ord \geq n$

Zeros: $\beta, \beta^2, \ldots, \beta^{2t}$



$wt(e) = w \leq t$

$$e(x) = x^{i_1} + x^{i_2} + \cdots + x^{i_w}$$

known:

$$\begin{cases} S_1 = \beta^{i_1} + \beta^{i_2} + \cdots + \beta^{i_w} \\ S_2 = \beta^{2i_1} + \beta^{2i_2} + \cdots + \beta^{2i_w} \\ S_3 = \beta^{3i_1} + \beta^{3i_2} + \cdots + \beta^{3i_w} \\ \vdots \\ S_{2t} = \beta^{2ti_1} + \beta^{2ti_2} + \cdots + \beta^{2ti_w} \end{cases}$$

Unknown: $w$, $i_1, i_2, \ldots, i_w$

$$X_j = \beta^{i_j}, \quad j = 1, 2, \ldots, \omega$$

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

power sums, symmetric polynomials

$$\sum_{i,j,k} X_i X_j X_k$$