Example ① $F = GF(2)$, $m=4$, $n=5$.

Codeword length = 5 bits

② $F = GF(2)$, $m=8$, $n=51$.

Codeword length = 51 bits.

③ $F = GF(2)$, $m=8$. $n=255$

Codeword length = 255 bits

④ $F = GF(2^8)$, $m=1$, $n=255$

codeword length = 255 bytes.

If $F = GF(2)$ it is a binary BCH code. Example ①, ②, ③

If $n = ord(F)^m - 1$ then it is a primitive BCH code. Example: ③, ④

* Because the smaller the m, the less complex the computation, we want the smallest m

Secondary:

Theorem: Set $m = ord(F) \bmod n$ will give us the smallest m satisfying $n \mid (order(F))^m - 1$

Primary

Step 3.2. Fix the m value and the

$\boxed{m}$

Step 3,2 : Fix the n value and the

$\beta \in \mathbb{F}_{\boxed{m}}$ value in Step 3,1

Choose any $\boxed{b \geq 0}$ and $2 \leq \delta \leq n$ value.

We choose a subset of $f_0(x) \ldots f_i(x)$ such that the product

$$g(x) = \prod_{l \in \text{subset}} f_l(x)$$

satisfies $g(\beta^a) = 0$ in $\boxed{\mathbb{F}_{\boxed{m}}}$

for all $a \in [b, b+\delta-2]$

$\boxed{\text{The construction is complete!}}$

$\boxed{\text{Intuition: } g(x) \text{ has } (\delta-1) \text{ consecutive roots in } \mathbb{F}_{\boxed{m}}}$

If $\delta = n+1$, then we have n consecutive β^a. Recall that $1, \beta, \beta^2, \ldots, \beta^{n-1}, \beta^n$

$\Rightarrow$ $g(x)$ contains all n roots

$\Rightarrow$ $g(x) = x^n - 1$, a trivial code

That's why we impose $2 \le \delta \le n$.

$*$ If $\boxed{b=1}$, then we say the BCH code is of narrow-sense.

Not $b=0$. even though $b=0$ is a legitimate choice.

Remark on 3.2. since $\deg(g(x)) = n-k$, and since we like to maximize k, we usually choose the $g(x)$ that satisfies ___ ① with the smallest degree.

$\Rightarrow$ An alternative way to describe Step 3.2 is.

let $\Phi_a(x) \in \mathbb{F}[x]$ denote the minimal polynomial of element $\beta^a \in \mathbb{F}^{\boxed{m}}$ Also recall the

conjugacy class $\beta, \beta^p, \beta^{p^2}$

conjugacy class $\beta, \beta^{p}, \beta^{p^2}, \ldots$

then we choose

$$g(x) = L.C.M\left(\phi_a(x) : a \in [b, b+\delta-2]\right)$$

Some properties of BCH code.

① Each coordinate is in $GF(p^i)$ for some i.
$\parallel$ $\mathbb{F}$

② Codeword length n must satisfy

$$n \mid \text{order}(F)^m - 1 \quad \text{for some } m$$

③ $g(x)$ has $\underline{(\delta-1) \text{ consecutive roots}}$
$\in \mathbb{F}[x]$
in $F^{\boxed{m}}$

④ $\deg(g(x)) = n-k$
satisfies $(\delta-1) \le n-k \le m \cdot (\delta-1)$

proof: $g(x)$ has $(\delta-1)$ consecutive nonzero roots $\Rightarrow \deg(g(x)) \geq \delta - 1$.

$g(x) = \text{L.C.M}(\phi_a(x) : a \in [b, b+\delta-2])$

since $\deg(\phi_a(x)) \leq m$ by the property of minimal polynomial in L11_1.pdf

$\Rightarrow \deg(g(x)) \leq m \cdot (\delta - 1)$.

This bound ~~is~~ can be loose, for example if $\mathbb{F} = GF(2)$ and $m \geq 2$, then we have

$$(\delta-1) \leq n-k \leq m \cdot \left\lfloor \frac{\delta-1}{2} \right\rfloor$$

$\Rightarrow n - m(\delta-1) \leq k \leq n - (\delta-1)$

⑤ $d_{min} \geq \delta$.

If $g(x)$ has k consecutive roots in $\mathbb{F}^{m}$, then $d_{min} \geq k+1$.

Proof: Suppose the codeword is $c(x) \in \mathbb{F}[x]$.

and because $c(x) = m(x) \cdot g(x)$
$\in \mathbb{F}[x]$

$\Rightarrow c(\beta^a) = 0$ in $\mathbb{F}^{\boxed{m}}$ for all
$a \in [b, \cdots, b+\delta-2]$.

$$\Rightarrow \begin{bmatrix} 1 & \beta^b & \beta^{b\cdot 2} & \beta^{b\cdot 3} & \cdots & \beta^{b(n-1)} \\ 1 & \beta^{b+1} & \beta^{(b+1)\cdot 2} & \cdots & & \beta^{(b+1)(n-1)} \\ 1 & & & & & \\ 1 & & & & & \\ 1 & & & & & \\ 1 & \beta^{b+\delta-2} & \beta^{(b+\delta-2)2}, & \cdots & & \beta^{(b+\delta-2)(n-1)} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{n-1} \end{bmatrix}$$

$= 0$ in $\mathbb{F}^{\boxed{m}}$ $\Rightarrow$ Similar role as the parity-check matrix

We now prove that $d_{min} \geq \delta$

Suppose not. $\Rightarrow \exists\ i_1, i_2, \cdots i_{\delta-1}$
$d_{min} \leq \delta - 1$ $\qquad \in [0, \cdots, n-1]$

such that the minimal-weight codeword

such that the minimal-weight codeword satisfies

$$\begin{bmatrix} \beta^{b\cdot i_1} & \beta^{b\cdot i_2} & \cdots & \beta^{b\cdot i_{\delta-1}} \\ \beta^{(b+1)\cdot i_1} & \beta^{(b+1)\cdot i_2} & \cdots & \beta^{(b+1) i_{\delta-1}} \\ \vdots & \vdots & & \\ \beta^{(b+\delta-2) i_1} & \beta^{(b+\delta-2) i_2} & \cdots & \beta^{(b+\delta-2)\cdot i_{\delta-1}} \end{bmatrix} \cdot \begin{bmatrix} C_{i_1} \\ \vdots \\ C_{i_{\delta-1}} \end{bmatrix} = 0 \quad \text{for}$$

$\in \mathbb{F}^{m}$

Some non-zero $\begin{bmatrix} C_{i_1} \\ \vdots \\ C_{i_{\delta-1}} \end{bmatrix}$

$\Rightarrow$ The matrix $\square$ must be non-full rank.

$\Leftrightarrow$ $\det(\square) = 0$

Note that $\det(\square)$

$= \beta^{b(i_1 + i_2 + \cdots i_{\delta-1})}$

$$\cdot \det\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \beta^{1\cdot i_1} & \beta^{1\cdot i_2} & & \beta^{1\cdot i_{\delta-1}} \\ \beta^{2\cdot i_1} & \beta^{2\cdot i_2} & & \beta^{2\cdot i_{\delta-1}} \\ & & & \vdots \\ \beta^{(\delta-2)\cdot i_1} & \beta^{(\delta-2)\cdot i_2} & & \beta^{(\delta-2)\cdot i_{\delta-1}} \end{pmatrix}$$

$$= \underline{\underline{\beta^{b(i_1+i_2+\cdots+i_{\delta-1})}}} \cdot \underline{\underline{\prod_{1\le j_1<j_2\le \delta-1} \left(\beta^{i_{j_2}} - \beta^{i_{j_1}}\right)}}$$

$\hookrightarrow \neq 0 \because \beta \neq 0$

By Vandermonde Matrix property

google $\begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & & & & \\ 1 & & & & \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{bmatrix}$.

(the transposed version is used.)

Question can we have $\beta^{i_{j_2}} = \beta^{i_{j_1}}$

for two different locations $i_{j_1} \neq i_{j_2}$

Ans: Note that $0 \le i_j \le n-1$

and by Step 3.2.

$$\underbrace{\beta^0 = 1, \beta^1, \beta^2, \cdots, \beta^{n-1}, \beta^n}_{\text{First repeat.}}$$

$\Rightarrow \beta^{i_{j_2}} \neq \beta^{i_{j_1}}$ for all differ locations $0 \leq i_{j_1} < i_{j_2} \leq n-1$ #

That's why in Step 3.1, we choose m and $\beta \in \mathbb{F}^m$ that satisfies.

* Also, in Step 3.2, we choose consecutive roots. This design choice manifests at creating the Vandermonde matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ \beta^{1 \cdot i_1} & \beta^{1 \cdot i_2} & & & \end{bmatrix}$$

$$\begin{bmatrix} \beta^{1\cdot i_1} & \beta^{1\cdot i_2} \\ \beta^{2\cdot i_1} & \beta^{2\cdot i_2} \\ \beta^{(\delta-2)\cdot i_1} & \beta^{(\delta-2)\cdot i_2} \end{bmatrix}$$

Examples:

GF(2), $m=5$. $n=31$. $\Rightarrow$ codeword length $=31$ bits

$\because n = 2^5 - 1$

$\Rightarrow$ It is a primitive BCH.

Suppose $GF(2^m)$ is generated by
$= GF(2^5)$

$x^5 + x^2 + 1$.

We then write down the minimal polynomial

$((\beta)^p)^{p\cdots}$

$\beta = \alpha^l$ where $\alpha = 00010 = 2$ is a primitive elements of $GF(2^5)$ and is also a primitive root of $x^n - 1$

element in $GF(2^5) \setminus \{0\}$.	minima polynomia in $GF(2)[x]$
$\{\alpha^0\}$	$x+1$
$\{\alpha^1, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}\}$	$x^5 + x^2 + 1$

$\{\alpha^1, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}\}$ $\qquad x^5+x^2+1$

$\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{17}\}$ $\qquad x^5+x^4+x^3+x^2+1$

$\{\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^9, \alpha^{18}\}$ $\qquad x^5+x^4+x^2+x+1$

$\{\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{25}, \alpha^{19}\}$ $\qquad x^5+x^3+x^2+x+1$

$\{\alpha^{11}, \alpha^{22}, \alpha^{13}, \alpha^{26}, \alpha^{21}\}$ $\qquad x^5+x^4+x^3+x+1$

$\{\alpha^{15}, \alpha^{30}, \alpha^{29}, \alpha^{27}, \alpha^{23}\}$ $\qquad x^5+x^3+1$

Say we like to correct $t=1$ error

$\Rightarrow \delta = 3 \leq d_{min} \Rightarrow \delta - 1 = 2$ consecutive roots.

Three good choices: Choice #1: $\{\alpha^1, \alpha^2\}$ (Narrow-sense)

$g(x) = x^5 + x^2 + 1$, $\deg(g(x)) = 5$

$\Rightarrow k = 26$. We have an $(31, 26)$ code

(Hamming)

Choice #2: $\{\alpha^{29}, \alpha^{30}\}$ $g(x) = x^5 + x^3 + 1$

$\Rightarrow$ We have an $(31, 26)$ code.

* It is equivalent to choice # 1 since the $g(x)$ is the reciprocol of choice # 1.

Choice # 3 : $\{\alpha^9, \alpha^{10}\}$

$$g(x) = x^5 + x^4 + x^2 + x + 1 \quad \deg(g(x)) = 5$$

We have an $(31, 26)$ code.

Say we like to correct $t=2$ errors.

$d_{min} = 5 = \delta \Rightarrow$ we need 4 consecutive roots.

Choice 1: Narrow-sense $\{\alpha^1, \alpha^2, \alpha^3, \alpha^4\}$.

$$\Rightarrow g(x) = (x^5 + x^2 + 1) \cdot (x^5 + x^4 + x^3 + x^2 + 1)$$

$$= x^{10} + x^9 + x^8 + x^6 + x^5 + x^3 + 1$$

A $(31, 21)$ code with $d_{min} \geq 5$
