:= Explicit Construction of Codes - IV :=

Distance Bound of BCH (n, δ, q, ℓ).

$$H' = \begin{array}{c|c} & x^0 \quad x^1 \quad x^2 \cdots x^j \cdots x^{n-1} \\ \begin{array}{c} \beta^{\ell} \\ \beta^{\ell+1} \\ \beta^{\ell+2} \\ \vdots \\ \beta^{\ell+i} \\ \vdots \\ \beta^{\ell+\delta-2} \end{array} & \begin{bmatrix} & & \vdots & \\ & & \vdots & \\ & & \vdots & \\ & & \vdots & \\ \cdots & \cdots & \beta^{(\ell+i)j} & \\ & & & \\ & & & \end{bmatrix} \end{array}$$

As we know parity matrix of BCH (n, δ, q, ℓ) is

$H = \Psi(H')$ where $\Psi(H')$ is the matrix we get applying the mapping $\Psi: \mathbb{F}_{q^m} \to \mathbb{F}_q^m$, defined in Eq. 1, on the entries of H'. Also, if a set of columns S in H' are linearly independent, then the set of columns S in H are also linearly independent.

$\Rightarrow$ if any set of $\leq \ell$ columns are linearly independent in H', then any set of $\leq \ell$ columns are linearly independent in H.

$$V = \begin{array}{c c}
 & \begin{array}{cccccccc} x^0 & x^1 & x^2 & x^3 & \cdots & x^j & \cdots & x^{n-1} \end{array} \\
\begin{array}{c} \beta^0 \\ \beta^1 \\ \beta^2 \\ \beta^3 \\ \vdots \\ \beta^i \\ \vdots \\ \beta^{\delta-2} \end{array} &
\begin{bmatrix} & & & & & \vdots & & \\ & & & & & \vdots & & \\ & & & & & \vdots & & \\ & & & & & \vdots & & \\ & & & & & \vdots & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \beta^{ij} & & \\ & & & & & & & \\ & & & & & & & \end{bmatrix}
\end{array}$$

As we know from the study of Reed-Solomon code that any of $\delta-1$ columns of V are linearly independent.

Observe that,

ith column of $H' = \beta^{(i-1)\ell} \cdot$ ith column of V.

Therefore, the linear independence relation of V & H' is same.

$\Rightarrow$ any of $\delta-1$ columns of H' are linearly independent

$\Rightarrow$ any of $\delta-1$ columns of H are linearly independent

$\Rightarrow$ the following claim:

Claim 2: The distance of $BCH(n,\delta,q,\ell)$ is $\geq \delta$.

Q3: Can we say the distance of $BCH = \delta$?

Observe that any set of δ columns of H' are linearly dependent. but they are linearly dependent over the field $\mathbb{F}_{q^m}$, which is an extension of $\mathbb{F}_q$. However, our codewords are over $\mathbb{F}_q$. So, using that linear dependence argument for H' over $\mathbb{F}_{q^m}$, we cannot say that the distance of $BCH(n, \delta, q, l)$ is exactly $= \delta$.

Distance vs. Dimension Tradeoff for BCH codes:

Assume that $l = 0$, $q = 2$ & $n = 2^m - 1$, i.e., $BCH(n, \delta, 2, 0)$ with $n = 2^m - 1$, i.e., primitive BCH codes over binary alphabets & β is a primitive element in $\mathbb{F}_{2^m}$.

The number of rows of H is at most $m \cdot (\delta - 1)$

$$\delta - 1 \leq \text{rank}(H) \leq m \cdot (\delta - 1)$$

$$\Rightarrow \quad n - (\delta - 1)\log_2(n+1) \leq \text{dimension of } BCH(n, \delta, 2, 0) \leq n - \delta + 1.$$

Q4: Can we get better lower bound for dimension of $BCH(n, \delta, 2, 0)$, i.e., better upper bound for rank(H)?

$$\begin{array}{c|c}
 & \begin{matrix} x^0 & x & x^2 & x^3 & \cdots & x^j & \cdots & x^{n-1} \end{matrix} \\
\begin{matrix} 1 = \beta^0 \\ \beta^1 \\ \beta^2 \\ \vdots \\ \beta^i \\ \vdots \\ \beta^{\delta-2} \end{matrix} & \left[\begin{matrix} & & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & \vdots & & \\ - & - & - & - & \cdots & \beta^{ij} \in \mathbb{F}_{2^m} & & \\ & & & & & & & \\ & & & & & & & \end{matrix}\right]_{(\delta-1) \times n} = H'
\end{array}$$

$\Downarrow$ Using natural association b/w $\mathbb{F}_{2^m}$ & $\mathbb{F}_2^m$

$\psi: \mathbb{F}_{2^m} \to \mathbb{F}_2^m$

$$\begin{array}{c} \\ 1 \\ \beta^1 \\ \beta^2 \\ \vdots \\ \beta^i \\ \vdots \\ \beta^{\delta-2} \end{array}
\begin{array}{c} \begin{array}{cccccccc} x^0 & x^1 & x^2 & \cdots & x^j & \cdots & x^{n-1} \end{array} \\
\left[\begin{array}{cccccccc} 1^T & 1^T & 1^T & & 1^T & & 1^T \\ & & & & \vdots & & \\ & & & & \vdots & & \\ & & & & \vdots & & \\ \cdots & & & & \psi(\beta^{ij})^T & & \\ & & & & & & \\ & & & & & & \end{array}\right]_{m(\delta-1)\times n} \end{array} = H$$

Since 1 is represented by $(1, \underbrace{0, 0, 0, \ldots, 0}_{(m-1)\text{ many zeroes}})$

from 2nd row to m^{th} row all are zero.

$\Rightarrow$ they contribute nothing to the rank of H

$\Rightarrow$ $\text{rank}(H) \leq m(\delta-1) - (m-1) = m(\delta-2)+1$

$\Rightarrow$ $n - m(\delta-2) - 1 \leq \dim BCH(n, \delta, 2, 0) \leq n - \delta + 1.$

Q5: we further improve the lower bound of $\dim BCH(n, \delta, 2, 0)$ i.e., further improving the upper bound of $\text{rank}(H)$?

Answer: Yes!

Claim 2: Let $f(x)$ be a polynomial in $\mathbb{F}_2[x]$. Let $i \in \{0, 1, 2, \ldots, \delta-2\}$ s.t. $f(\beta^i) = 0$. Then, $f(\beta^{2i}) = 0$.

Proof:

Explanation:

General Scenario: $\mathbb{F}_q \leq \mathbb{F}_{q^m}$, $\alpha \in \mathbb{F}_{q^m}$, $g(x) \in \mathbb{F}_q[x]$ is the minimal polynomial for α i.e., lowest degree irreducible polynomial with α is a root.

$\Rightarrow \alpha, \alpha^q, \alpha^{q^2}, \ldots \alpha^{q^{r-1}}$ are roots of $g(x)$ with $r = \deg(g)$

Also, $\forall\, h(x) \in \mathbb{F}_q[x]$ with $h(\alpha) = 0 \Rightarrow g \mid h$

$\Rightarrow \alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{r-1}}$ are also roots of $h(x)$

Therefore, $f(\beta^i) = 0 \Rightarrow f(\beta^{2i}) = 0$

Detailed Proof: $f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{n-1} x^{n-1}$, $f_i \in \mathbb{F}_2$

$f(\beta^i) = f_0 + f_1 \beta^i + f_2 \beta^{2i} + \cdots + f_{n-1} \beta^{(n-1)i} = 0$

$$f(\beta^{2i}) = f_0 + f_1 \beta^{2i} + f_2 \beta^{4i} + \cdots + f_{n-1} \beta^{(n-1)2i}$$

$$= (f_0 + f_1 \beta^i + f_2 \beta^{2i} + \cdots + f_{n-1} \beta^{(n-1)i})^2$$

$\Rightarrow f(\beta^{2i}) = 0.$

Claim 1 $\Longrightarrow$ if $c \in \mathbb{F}_2^n$ &

$$\begin{array}{c|c}
 & x^0 \quad x^1 \quad x^2 \;\cdots\; x^j \;\cdots\; x^{n-1} \\
\hline
\begin{array}{c} 1 = \beta^0 \\ \beta^1 \\ \beta^3 \\ \beta^5 \\ \vdots \\ \beta^{2i-1} \\ \vdots \\ \vdots \end{array} & \left[\begin{array}{c} \\ \\ \\ \\ \tilde{H} \\ \\ \\ \\ \end{array} \right]
\end{array}
\begin{bmatrix} \\ \\ c \\ \\ \\ \end{bmatrix} = 0$$

$\Downarrow$

$\tilde{H}$ = Submatrix formed by rows of H' corresponding to $\beta^0 = 1$ & odd power of β

$\Rightarrow$ $\quad H' \cdot c = 0$

$\Rightarrow \forall c \in \mathbb{F}_2^n, \quad c \in \ker(\Psi(\tilde{H})) \Longleftrightarrow c \in \mathcal{H} = \Psi(H')$.

$\Rightarrow \quad \text{rank}(H) = \text{rank}(\Psi(\tilde{H})) \leq$ no. of rows of $\Psi(\tilde{H})$

$= mt \quad$ if $\delta = 2t$

$m(t+1) \quad$ if $\delta = 2t+1$

Observe:

$$
\begin{array}{c|ccccccc|}
 & x^0 & x^1 & x^2 & \cdots & x^j & \cdots & x^{n-1} \\
\hline
1 = \beta^0 & \begin{matrix}1\\0\\\vdots\\0\end{matrix} & \begin{matrix}1\\0\\\vdots\\0\end{matrix} & \cdots & \cdots & & & \begin{matrix}1\\0\\\vdots\\0\end{matrix} \\
\beta^1 & & & & & & & \\
\beta^3 & & & & & & & \\
\beta^5 & & & & & & & \\
\vdots & & & & & & & \\
\beta^{2i-1} & & & & & & & \\
\vdots & & & & & & & \\
\beta^{2t-1} & & & & & & &
\end{array}
= \Psi(\tilde{H})
$$

for $\delta = 2t+1$

Again since first m rows representing 1, like the previous case, from 2nd to m^{th} row are zero.

$\Rightarrow$ $\operatorname{rank} H = \operatorname{rank}(\tilde{H}) \leq m(t+1) - (m-1) = mt+1$ if $\delta = 2t+1$

$mt - m + 1 = m(t-1) + 1$ if $\delta = 2t$.

This implies that

Claim 3: The dimension of $BCH(n, \delta, 2, 0)$ with $n = 2^m - 1$ is at least $n - \lfloor \frac{\delta - 1}{2} \rfloor \cdot \log(n+1) - 1$

Q6: Is the asymptotic bound on dimension is optimal?
Using Hamming ball packing arguement, we show that for $\delta = n^{o(1)}$, for example, $\delta = \text{poly}(\log n)$, bound in claim 3 is optimal. i.e., we cannot improve the lower bound to $n - \lfloor \frac{\delta - 1}{2-\varepsilon} \rfloor \log(n+1)$ for some $\varepsilon > 0$.

Let $d = \text{dis } BCH(n, \delta, 2, 0)$. Then, $d \geq \delta$.

From Hamming ball packing $Vol_2(\lfloor \frac{d-1}{2} \rfloor, n)$

$$= \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} {}^nC_i \quad \cdots\cdots \quad (3')$$

$$\geq {}^nC_{\lfloor \frac{d-1}{2} \rfloor} \geq \left(\frac{n}{\frac{d-1}{2}} \right)^{\frac{d-1}{2}}$$

From Hamming Ball Bound,

$$\dim BCH(n, \delta, 2, 0) \leq n - \log_2 \left(Vol_2(\lfloor \tfrac{d-1}{2} \rfloor, n) \right)$$

$$\leq n - \log_2 \left[\frac{2n}{(d-1)} \right]^{\lfloor \frac{d-1}{2} \rfloor}$$

$$= n - \lfloor \tfrac{d-1}{2} \rfloor . \log n + \lfloor \tfrac{d-1}{2} \rfloor \log \frac{d-1}{2} \quad \cdots\cdots \quad (1)$$

On the other hand, $d \geq \delta$ so,

$$\dim BCH(n, \delta, 2, 0) \geq n - \lfloor \tfrac{d-1}{2} \rfloor \log(n+1) - 1$$

Also, we know, $d \le m\delta$ [Exercise: $d \le 2\delta$. $BCH(2^m-1, \delta, 2, 1)$]

From (1),

$$\dim BCH(n, \delta, 2, 0) \le n - \lfloor \tfrac{d-1}{2} \rfloor \log n + \lfloor \tfrac{d-1}{2} \rfloor \log\left(\tfrac{m\delta}{4}\right) \quad \cdots \quad (2)$$

$$= n - \lfloor \tfrac{d-1}{2} \rfloor \left(\log n - \log\log(n+1) - o(\log(n))\right)$$

for $\delta = n^{o(1)}$

$$= n - \lfloor \tfrac{d-1}{2} \rfloor \cdot \left[\log n - o(\log n)\right]$$

$\Rightarrow$ for $\delta = n^{o(1)}$, Bound in Claim 3 is optimal.

Therefore, unlike Hamming Code, BCH code gives a family of optimal codes with unbounded distance.

Distance vs. Distance tradeoff:

1. An interesting regime is $\delta = \frac{n}{\omega(\log n)}$, e.g., $\delta = \frac{n}{\log^2 n}$,
   then dimension $\ge (1 - o(1))\, n$
   i.e. distance $\to 0$
   But, dimension $\to 1$.
2. But, $\delta = \frac{n}{o(\log n)}$, e.g., $\delta = \frac{n}{\sqrt{\log n}}$
   then Claim 3 is not giving anything interesting.

However, in general, primitive BCH codes are asymptotically bad, i.e., if C_v is a $[n_v, k_v, d_v]$ primitive BCH code for $v = 1, 2, 3, \ldots$ & $n_v \to \infty$.

then either $\frac{k_\nu}{n_\nu} \to 0$ or $\frac{d_\nu}{n_\nu} \to 0$

["Long BCH codes are Bad" by
SHU LIN & E. J. WELDON JR.]

Exercise: Let $\beta \in \mathbb{F}_{q^m}$ be an n^{th}-primitive roots of unity.
& $E = \{1, \beta, \beta^2, \ldots, \beta^{n-1}\}$. Then

1. $BCH(n, \delta, q, 0) = RS(E, \delta - 1, q^m)^{\perp} \cap \mathbb{F}_q^n$
2. $BCH(n, \delta, q, 1) = RS(E, n-\delta+1, q^m) \cap \mathbb{F}_q^n$
3. $BCH(n, \delta, q, \ell) = \{ (p(1), p(\beta), p(\beta^2), \ldots, p(\beta^{n-1})) \mid p(x) \in \mathbb{F}_{q^m}[x]$ s.t. $p(x) = x^{n-\ell+1} \cdot c(x)$ with $\deg(c(x)) < n-\delta \} \cap \mathbb{F}_q^n$.