=: Explicit Constructions of Codes - III :=

:: BCH codes :=

Raj Chandra ISI affiliate.

BCH Codes: discovered by R. C. Bose & D. K. Ray-Chaudhuri (1960) & indepently by A. Hocquenghem (1959).

Dijen Kumar

- $BCH(n, \delta, q, \ell)$: alphabet $\Sigma = \mathbb{F}_q$

  Block-length: n . ; $\gcd(n, q) = 1$.

Codes are defined as follows:

Consider the polynomial $x^n - 1$

Let β be an n^{th} primitive root of unity, i.e.,

$1 = \beta^0, \beta, \beta^2, \ldots, \beta^{n-1}$ are roots of $x^n - 1$.

$\ell \in \mathbb{Z}_{\geq 0}$ & $\delta \in \mathbb{Z}_{\geq 2}$ & consider $\beta^\ell, \beta^{\ell+1}, \beta^{\ell+2}, \ldots, \beta^{\ell+\delta-2}$.

Then, codewords in $BCH(n, \delta, q, \ell)$ are a set of polynomials over $\mathbb{F}_q$ of degree less than n s.t.

$$f(x) \in BCH(n, \delta, q, \ell) \text{ iff } f(\beta^\ell) = f(\beta^{\ell+1}) = \ldots = f(\beta^{\ell+\delta-2}) = 0$$

- δ – is called the designed distance of BCH codes.

Q1: Does β exists? Yes! Since every univariate polynomial has a splitting field.

Q2: what is the splitting field? An extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ is the splitting field of $x^n - 1$ iff $\mathbb{F}_{q^m}$ contains n^{th}-primitive roots of unity. $\Leftrightarrow$ $n \mid q^m - 1$ $\Leftrightarrow$ $m = Or_n(q)$, i.e., m is the smallest positive integer s.t. $q^m - 1 \equiv 0 \pmod{n}$.

$\Rightarrow \beta \in \mathbb{F}_{q^m}$; so, β may not be in the field $\mathbb{F}_q$.

- for $n = q^m - 1$, $BCH(q^m-1, \delta, q, \ell)$ is called primitive BCH code.

Parity matrix:

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

$H' \in \mathbb{F}_{q^m}^{(\delta-1)\times n}$ &

$$BCH(n, \delta, q, \ell) = \{ c \in \mathbb{F}_q^n \mid H \cdot c = 0 \}.$$

Representation of H' over $\mathbb{F}_q$:

Since $\mathbb{F}_{q^m}$ is an m-dimensional vector space over $\mathbb{F}_q$, there exists a natural association b/w elements of $\mathbb{F}_{q^m}$ & $\mathbb{F}_q^m$; let $\psi : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q^m$ be that natural association. Then,

$$
H = \begin{array}{c} \\ \beta^{\ell} \\ \beta^{\ell+1} \\ \beta^{\ell+2} \\ \vdots \\ \beta^{\ell+i} \\ \vdots \\ \beta^{\ell+\delta-2} \end{array}
\begin{array}{c} \begin{array}{cccccccc} x^0 & x^1 & x^2 & x^3 & \cdots & x^j & \cdots & x^{n-1} \end{array} \\
\left[\begin{array}{ccccc} & & & \vdots & \\ & & & \vdots & \\ & & & \vdots & \\ & & & \vdots & \\ \cdots & \cdots & \cdots & \psi\left(\beta^{j(\ell+i)}\right)^T & \\ & & & & \\ & & & & \end{array} \right] \end{array} \quad \cdots \text{(Eq. 1)}
$$

Then, $H \in \mathbb{F}_q^{m.(\delta-1)\times n}$ & H is the parity matrix of $BCH(n, \delta, q, \ell)$ whose entries are in $\mathbb{F}_q$.

Generator matrix for $BCH(n, \delta, q, \ell)$:

$\forall\, i \in \{0, 1, 2, \ldots, \delta-2\}$, f_i is the minimal polynomial over $\mathbb{F}_q$ for $\beta^{\ell+i}$, i.e., $\beta^{\ell+i}$ is the root of f_i. f_i is a monic polynomial, i.e., coefficient of the highest degree monomial is 1, & $f_i(x)$ is such a polynomial of lowest degree.

$\Rightarrow$ f_i an irreducible polynomial & any polynomial $p(x)$ for which $\beta^{\ell+i}$ is a root, $f_i(x) \mid p(x)$.

Let $g(x) = \mathrm{lcm}(f_0, f_1, \ldots, f_{d-2})$.

Then, $c(x) \in BCH(n, \delta, q, \ell)$ iff $g(x) \mid c(x)$.

$\Rightarrow \; BCH(n,\delta,q,l) = \operatorname{Span}_{\mathbb{F}_q}\{g(x), x\,g(x), \ldots, x^{k-1}g(x)\}$

where $\deg(g) = n-k$.

Let $g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_{n-k}x^{n-k}$.

then generator matrix G for $BCH(n,\delta,q,l)$ is the following:

$$\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & 0 & \cdots \\ 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots \\ 0 & 0 & g_0 & \cdots & g_{n-k-2} & g_{n-k-1} & g_{n-k} & \cdots \\ \vdots & \vdots & \vdots & & & & & \end{bmatrix}_{k\times n}$$

Claim 1: The dimension of $BCH(n,\delta,q,l)$ is

$$n-\deg(g)$$

However, this bound is not numerically useful. We see some good lower bound on the dimension of $BCH(n,\delta,q,l)$ which will lead to Hamming ball packing bound.