Today

BCH Codes.

CS5.318.1
Coding Theory
Lecture 7 (2022-9-19)
Instructor: Prahladh Harsha.

BCH codes: (named after Bose & Raychaudhuri & Hocquenghem)

$q = \mathbb{F}_{2^r} \supseteq \mathbb{F}_2 = \{0,1\}$

$S = \mathbb{F}_{2^r}^*$; $n = q-1 = 2^r-1$

$k = n-2t$

$n = 2^r - 1$
t - parameter

$BCH[n,t] = RS_{\mathbb{F}_{2^r}}[\mathbb{F}_{2^r}^*, 2^r-1-2t] \cap \mathbb{F}_2^{\,n}$ $(n = 2^r-1)$

Thm: $BCH[n,t]$ is a $[2^r-1, \geq 2^r-1-tr, \geq 2t+1]_2$-cyclic code

$|BCH[n,t]| \geq 2^{2^r-1-tr} = \frac{2^n}{2^{tr}} = \frac{2^n}{(n+1)^t}$ $(n = 2^r-1)$

Hamming Bd: (distance $2t+1$) $|C| \leq \frac{2^n}{Vol_2(n,t)} = \frac{2^n}{\Theta(n^t)}$ for small t.

(ie, BCH matches the Hamming Bd upto constants)

Pf: BCH inherits most of its properties from RS

The only thing left to argue is the dim (or rate)

Tools: (1) Trace function

(2) Dual of $RS_{\mathbb{F}}[\mathbb{F}^*, k]$ where $\mathbb{F} = \mathbb{F}_{2^r}$

Trace function $GF(2) \subseteq GF(2^r) = \mathbb{F}$

$$Tr_r : \mathbb{F}_{2^r} \longrightarrow \mathbb{F}$$

$$z \longmapsto z + z^2 + z^4 + \dots + z^{2^{r-2}} + z^{2^{r-1}}$$

Proposition: (1) $Tr(z) \in \mathbb{F}_2$ (ie, $(Tr(z))^2 = Tr(z)$)

(2) $Tr(z)$ is linear (ie $Tr(z_1 + z_2) = Tr(z_1) + Tr(z_2)$)

(3) $Tr(\alpha z)$ is also linear for any $\alpha \in \mathbb{F}_{2^r}$

(4) $Tr(\alpha z) \equiv 0 \iff \alpha = 0$

(5) $\{Tr(\alpha z) / \alpha \in \mathbb{F}_{2^r}\} = Lin(\mathbb{F}_{2^r}, \mathbb{F}_2)$

(6) $\eta_1, \dots \eta_r \in \mathbb{F}_{2^r}$ & $\eta_1 \dots \eta_r$ $\mathbb{F}_2$-linearly independent.

$Tr(\eta_1 z), Tr(\eta_2 z) \dots Tr(\eta_r z)$ is also linearly independent ie Suppose not, $\exists\ \bar{b} \neq 0^n$

$$\sum b_i \, Tr(\eta_i z) \equiv 0$$

$$\Leftrightarrow \; Tr\left(\sum b_i \eta_i \, z\right) \equiv 0$$

$$\Leftrightarrow \; \sum b_i \eta_i = 0$$

$$\mathbb{F}_{2^n} \cong \mathbb{F}_2^n \quad (\text{fix } \eta_1 \ldots \eta_n \text{ - } \mathbb{F}_2\text{-lin independent})$$

$$z \longleftrightarrow (Tr(\eta_1 z), Tr(\eta_2 z), \ldots, Tr(\eta_n z))$$

Dual of $RS_{\mathbb{F}}[\mathbb{F}^*, k]$

Last time: $RS_{\mathbb{F}}[\mathbb{F}, k]^{\perp} = RS_{\mathbb{F}}[\mathbb{F}, q-k]$

using $\displaystyle\sum_{\alpha \in \mathbb{F}^*} \alpha^i = 0 \quad \forall\ 1 \leq i < q-1$

$$\sum_{\alpha \in \mathbb{F}^*} \alpha^i \alpha^j = 0 \qquad \forall \; \begin{array}{l} 0 \leq i < k \\ 1 \leq j \leq q-1-k \\ \quad\; = n-k \quad (n = q-1) \end{array}$$

ie, $\forall\ f \in RS_{\mathbb{F}}[\mathbb{F}^*, k]$

$$\sum_{\alpha \in \mathbb{F}^*} f(\alpha) \alpha^j = 0 \quad \forall\ 1 \leq j \leq n-k.$$

$$RS_{\mathbb{F}}[\mathbb{F}^*, k]^{\perp} = \left\{ \left(\sum_{i=1}^{n-k} g_i x^i \right)_{\alpha \in \mathbb{F}^*} \middle/ g_i \in \mathbb{F} \right\}$$

$(c_1 \dots c_{q-1}) \in RS_{\mathbb{F}}[\mathbb{F}^*, k]$

$\Updownarrow$

$$\underbrace{\begin{bmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{q-1} \\ \alpha_1^2 & \alpha_2^2 & & \alpha_{q-1}^2 \\ \vdots & & & \\ \alpha_1^{n-k} & & & \alpha_{q-1}^{n-k} \end{bmatrix}}_{\alpha \in \mathbb{F}^*,\ \text{rows } i = 1 \dots n-k} \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = 0 \qquad n = q-1$$

In other words $(b_1 \dots b_n) \in BCH[n, t+1]$

$\Updownarrow$

$$\forall\ 1 \leq j \leq 2t, \quad \sum_{i=1}^{n} b_i \alpha_i^j = 0$$

Now, use $z \overset{\varphi}{\longleftrightarrow} \begin{pmatrix} Tr(\eta_1 z) \\ Tr(\eta_2 z) \\ \vdots \\ Tr(\eta_r z) \end{pmatrix}$ where $\eta_1 \dots \eta_n$ - $\mathbb{F}_2$-linearly ind.

$$\underbrace{\sum_{i=1}^{n} b_i \alpha_i^j}_{A} = 0 \iff \begin{pmatrix} Tr(\eta_1 A) \\ Tr(\eta_2 A) \\ \vdots \\ Tr(\eta_r A) \end{pmatrix} = 0^r$$

$$Tr\left(\eta_k \sum_{i=1}^{n} b_i \alpha_i^j\right) = 0 \iff \sum_{k=1}^{n} b_i\, Tr(\eta_k \alpha_i^j) = 0$$

$$\underbrace{\begin{bmatrix} \varphi(\alpha_1) & \varphi(\alpha_2) & \dots & \varphi(\alpha_n) \\ \varphi(\alpha_1^2) & \varphi(\alpha_2^2) & & \varphi(\alpha_n^2) \\ \vdots & & & \\ \varphi(\alpha_1^{2t}) & & & \varphi(\alpha_n^{2t}) \end{bmatrix}}_{\alpha,\ n \text{ columns};\ i,\ 2tr \text{ rows}} \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = 0 \iff (b_1 \dots b_n) \in BCH[n, t]$$

$$\dim(BCH(n,t)) \geq n - 2tr$$

Constraints: $\sum_{i=1}^{n} b_i \alpha_i^{j} = 0 \qquad 1 \leq j \leq 2t$

Consider
$$\sum_{i=1}^{n} b_i \alpha_i^{\ell} = 0$$
$$\sum_{i=1}^{n} b_i \alpha_i^{2\ell} = 0$$

$$\sum b_i \alpha_i^{2\ell} = \left(\sum b_i \alpha_i^{\ell}\right)^2$$
since $b_i \in \{0,1\}$.

ie, Defining constraints for $BCH[n,t]$ are
$$\sum_{i=1}^{n} b_i \alpha_i^{j} \quad ; \; j \in \{1, 3, 5, \dots, 2t-1\}$$

Hence, a parity check matrix for $BCH[n,t]$ is

$$\uparrow r \quad \mathbb{F}_q^{*} \leftarrow r \rightarrow$$

$$tr \updownarrow \begin{matrix} 1 \\ 3 \\ 5 \\ \vdots \\ 2t-1 \end{matrix} \begin{bmatrix} \varphi(\alpha_1) & \cdots & \varphi(\alpha_n) \\ \varphi(\alpha_1^3) & \cdots & \varphi(\alpha_n^3) \\ \vdots & & \vdots \\ \varphi(\alpha_1^{2t-1}) & \cdots & \varphi(\alpha_n^{2t-1}) \end{bmatrix}$$

Hence, $\dim_2 BCH(n,t) \geq n - tr$

∎

Dual-BCH code:

$$\text{dual-}BCH[n,t] = BCH[n,t]^{\perp}$$

By defn, $\text{dual-}BCH[n,t]$ = Span of rows of Parity check matrix of $BCH[n,t]$

How does the span look like?

$$\sum_{k=1}^{r} \sum_{j=1}^{2t} b_{jk} \, Tr(\eta_k \alpha^j) \qquad b_{jk} \in \{0,1\}$$

$$= \sum_{j=1}^{2t} Tr\left(\left(\sum_{k=1}^{r} b_{jk}\eta_k\right)\alpha^j\right)$$

$$= \sum_{j=1}^{2t} Tr(\beta_j \alpha^j) \qquad \beta_j \in \mathbb{F}_{2^r}$$

$$= Tr\left(\sum_{j=1}^{2t} \beta_j \alpha^j\right)$$

Hence dual BCH[n,t] - eval of trace of deg $\le 2t$ (w/o constant term) polynomials.

$$|\text{dual-BCH}[n,t]| \le 2^{rt} \quad \text{(w/ equality for small } t)$$

$$= (n+1)^t \quad \text{(not prove in course)}$$

Thm [Weil Bounds]

$$dist(\text{dual-BCH}[n,t]) \ge \frac{1}{2} - \frac{t}{\sqrt{n}}$$

(beyond the scope of this course)