19/2/2021

Lecture 13 (GRS Codes, RS Codes, BCH Codes)

Recap

$$H_{GRS} = \begin{bmatrix} v_1 & v_2 & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n \\ v_1\alpha_1^2 & v_2\alpha_2^2 & & v_n\alpha_n^2 \\ \vdots & \vdots & & \vdots \\ v_1\alpha_1^{n-k-1} & v_2\alpha_2^{n-k-1} & & v_n\alpha_n^{n-k-1} \end{bmatrix}_{(n-k)\times n}.$$

$\alpha_1, \ldots, \alpha_n$ are nonzero distinct element in $\mathbb{F}_q$. $\rightarrow$ Code locators/ Column locators

$v_1, \ldots, v_n$ need not be distinct, nonzero elements in $\mathbb{F}_q$ $\rightarrow$ Column multipliers

$\mathcal{C}_{GRS}$ is the code for which the above matrix is a parity check matrix.

$(n, k, n-k+1)$ and Generalized Reed Solomon Codes are MDS Codes.

GRS Codes are MDS Codes.

To prove this, we will show that any $n-k$ columns of H_{GRS} form a full rank matrix.

Vandermonde Determinant Formula

$$\det \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \beta_1 & \beta_2 & \cdots & \beta_r \\ \beta_1^2 & \beta_2^2 & \cdots & \beta_r^2 \\ \vdots & & & \\ \beta_1^{r-1} & \beta_2^{r-1} & \cdots & \beta_r^{r-1} \end{bmatrix}_{r \times r} = \prod_{1 \le i < j \le r} (\beta_j - \beta_i)$$

If $\beta_1, \beta_2, \ldots, \beta_r$ are distinct elements in the field $\mathbb{F}_q$, then determinant is non zero.

Proof is by induction.

$\underline{r=2}$ (base case)

Assume induction hypothesis for $r-1$

Consider the following determinant.

$$\begin{vmatrix} 1 & 1 & & 1 & 1 \\ \beta_1 & \beta_2 & \cdots & \beta_{r-1} & z \\ \beta_1^2 & \beta_2^2 & & \beta_{r-1}^2 & z^2 \\ \vdots & \vdots & & \vdots & \vdots \\ \beta_1^{r-1} & \beta_2^{r-1} & & \beta_{r-1}^{r-1} & z^{r-1} \end{vmatrix} = D(z).$$

$D(z)$ is a polynomial in $\mathbb{F}_q[z]$ and $\deg(D(z)) = r-1$

Coeff of z^{r-1} in the above determinant is

$$z^{r-1} \begin{vmatrix} 1 & 1 & & 1 \\ \beta_1 & \beta_2 & & \beta_{r-1} \\ \vdots & \vdots & & \vdots \\ \beta_1^{r-2} & \beta_2^{r-2} & & \beta_{r-1}^{r-2} \end{vmatrix}$$

Coeff of $z^{r-1} \neq 0$ (By induction hypothesis).

Roots of $D(z) \rightarrow \beta_1 \ldots \beta_{r-1}$ as the roots

$$(z-\beta_i) \mid D(z). \quad \forall\, 1 \leq i < r.$$

$$\underbrace{\prod_{1 \leq i < r} (z-\beta_i)}_{\hookrightarrow \text{ deg } r-1 \text{ polynomial}} \mid D(z) \rightarrow \text{deg } r-1 \text{ polynomial}.$$

$$D(z) = (\text{Const}) \prod_{1 \le i < r} (z - \beta_i).$$

Constant = Coeff of z^{r-1} in $D(z)$.

$$= \begin{vmatrix} 1 & 1 & & 1 \\ \beta_1 & \beta_2 & & \beta_{r-1} \\ \beta_1^2 & \beta_2^2 & \cdots & \beta_{r-1}^2 \\ \vdots & \vdots & & \vdots \\ \beta_1^{r-2} & \beta_2^{r-2} & & \beta_{r-1}^{r-2} \end{vmatrix} = \prod_{1 \le i < j \le r-1} (\beta_j - \beta_i)$$

By induction hypothesis.

$$D(z) = \left(\prod_{1 \le i < j \le r-1} (\beta_j - \beta_i) \right) \left(\prod_{1 \le i < r} (z - \beta_i) \right).$$

We have defined $D(z)$ by replacing β_r with variable z.

Determinant of Vandermonde matrix of size $r \times r$;

$$D(\beta_r) = \left(\prod_{1 \le i < j \le r-1} (\beta_j - \beta_i) \right) \left(\prod_{1 \le i < r} (\beta_r - \beta_i) \right)$$

$$H_{GRS} = \begin{bmatrix} v_1 & v_2 & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n \\ v_1\alpha_1^2 & v_2\alpha_2^2 & \cdots & v_n\alpha_n^2 \\ \vdots & & & \\ v_1\alpha_1^{n-k-1} & v_2\alpha_2^{n-k-1} & \cdots & v_n\alpha_n^{n-k-1} \end{bmatrix}$$

Any $(n-k)$ columns of H_{GRS} are linearly independent.

$$\begin{vmatrix} v_1 & v_2 & \cdots & v_{n-k} \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_{n-k}\alpha_{n-k} \\ \vdots & & & \vdots \\ v_1\alpha_1^{n-k-1} & v_2\alpha_2^{n-k-1} & & v_{n-k}\alpha_{n-k}^{n-k-1} \end{vmatrix} = \left(\prod_{i=1}^{n-k} v_i\right)\left(\prod_{1\le i<j\le n-k}(\alpha_j - \alpha_i)\right).$$

All α_j's are distinct nonzero elements.

All v_i's are nonzero elements

Thus, d_{min} of $\mathbb{C}_{GRS} = n-k+1$.

Dual of a GRS Code is also a GRS Code.

Proof :- G_{GRS} is the parity check matrix for the dual code

$$G_{GRS} = \begin{bmatrix} v_1' & v_2' & \cdots & v_n' \\ v_1'\alpha_1 & v_2'\alpha_2 & \cdots & v_n'\alpha_n \\ \vdots & & & \\ v_1'\alpha_1^{k-1} & v_2'\alpha_2^{k-1} & \cdots & v_n'\alpha_n^{k-1} \end{bmatrix}$$

$$\boxed{G_{GRS} \cdot H_{GRS}^T = 0}$$ ← True for any generator matrix & parity check matrix.

↓

If there exist $v_1', v_2' \ldots v_n'$ all nonzero elements such that

$$G_{GRS} \cdot H_{GRS}^T = 0$$

then we have proved the statement.

$$\begin{bmatrix} v_1'\alpha_1^i & v_2'\alpha_2^i & \cdots & v_n'\alpha_n^i \end{bmatrix} \cdot \begin{bmatrix} v_1\alpha_1^l \\ v_2\alpha_2^l \\ \vdots \\ v_n\alpha_n^l \end{bmatrix} = 0. \quad \forall i, l.$$

$0 \le i \le k-1$

$0 \le l \le n-k-1.$

$\underline{0 \le i + l \le n-2}$

We will write $(n-1)$ equations in matrix form

(Why only $n-1$, because the equation is only dependent only on the value of $i+l$)

$$\begin{bmatrix} v_1 & v_2 & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n \\ v_1\alpha_1^2 & v_2\alpha_2^2 & \cdots & v_n\alpha_n^2 \\ \vdots & & & \\ v_1\alpha_1^{n-2} & v_2\alpha_2^{n-2} & \cdots & v_n\alpha_n^{n-2} \end{bmatrix} \begin{bmatrix} v_1' \\ v_2' \\ \vdots \\ v_n' \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

$n-k-1 = n-2$

$H'_{GRS}(n, 1, n)$ $\boxed{H'_{GRS}\,\underline{v}' = \underline{0}}$

$[v_1' \ldots v_n']$ belongs to the code.

C'_{GRS} with parameters $(n, 1, n)$

$\exists$ a vector which belongs to the code is clear

Minimum distance of C'_{GRS} is n is telling you that the vector $[v_1' \ldots v_n']$ has all nonzero elements.

Interpreting GRS Codewords as polynomial evaluations

$$G_{GRS} = \begin{bmatrix} v_1' & v_2' & \cdots & v_n' \\ v_1'\alpha_1 & v_2'\alpha_2 & \cdots & v_n'\alpha_n \\ \vdots & & & \\ v_1'\alpha_1^{k-1} & v_2'\alpha_2^{k-1} & \cdots & v_n'\alpha_n^{k-1} \end{bmatrix}$$

$\underline{u} = (u_0, u_1, \ldots, u_{k-1})$

$\underline{c} = (c_1, \ldots, c_n)$.

$$\underline{c} = \underline{u}\, G_{GRS}.$$

$$= \begin{pmatrix} u_0 & u_1 & \cdots & u_{k-1} \end{pmatrix} \begin{bmatrix} v_1' & v_2' & \cdots & v_n' \\ , & & & \\ \vdots & & & \\ v_1'\alpha_1^{k-1} & v_2'\alpha_2^{k-1} & \cdots & v_n'\alpha_n^{k-1} \end{bmatrix}$$

$$c_j = \sum_{i=0}^{k-1} u_i v_j' (\alpha_j)^i = v_j' \left(\sum_{i=0}^{k-1} u_i \alpha_j^i \right)$$

Message polynomial $\leftarrow$

$$u(x) = \sum_{i=0}^{k-1} u_i x^i$$

$$u(x) \longrightarrow \left(v_1' u(\alpha_1) \;\; v_2' u(\alpha_2) \;\cdots\; v_n' u(\alpha_n) \right).$$

Special case of $v_j' = 1 \ \forall j$

$$u(x) \longrightarrow \left(u(\alpha_1) \ u(\alpha_2) \ \ldots \ u(\alpha_n) \right).$$

Code description of Reed Solomon Code

(Case when $v_j' = 1 \ \forall j$)

$$\mathcal{C}_{RS} = \left\{ \left(u(\alpha_1), \ldots, u(\alpha_n) \right) : \begin{array}{l} u(x) \in \mathbb{F}_q[x] \\ \text{of deg} \leq k-1 \end{array} \right\}.$$

Alternate Proof for the MDS property of RS Codes (described in terms of polynomial evaluations).

Length of $C_{RS} = n$.

Dimension $= k$ (?). Look at the message polynomial $u(x)$ and see how many free coeffs are there

$$u_0 + u_1 x + u_2 x^2 + \cdots + u_{k-1} x^{k-1}$$

$u_i \in \mathbb{F}_q$.

$\mathbb{C}_{RS}$ is still a linear code

Minimum distance of a linear code

= minimum Hamming weight of a nonzero codeword.

$\left(u(\alpha_1)\ u(\alpha_2)\ \ldots\ \ u(\alpha_n)\right)$

and see how many zeros are there for some nonzero polynomial $u(x)$.

No. of zeros of atmost deg $k-1$ polynomial $\leq (k-1)$

$\Rightarrow$ No. of zero coordinates in any nonzero codeword $\leq k-1$

$\Rightarrow$ No. of nonzero coordinates in any nonzero codeword $\geq n-k+1$

$d_{min} \geq n-k+1$

$\Rightarrow$ $d_{min}(\mathbb{C}_{RS}) = n-k+1$ (Singleton bound).