(RS Codes, RS Codes, 19/2/2021 <u>Lecture 13</u> BCH Godes

Recap $H_{GRS} = \begin{cases} 0_1 & 0_2 \\ 0_1 & 0_1 & 0_2 \\ 0_1 & 0_1 & 0_2 \\ 0_1 & 0_1 & 0_2 \\ 0_1 & 0_1 & 0_2 \\ 0_1 & 0_1 & 0_2 \\ 0_1 & 0_1 & 0_2 \\ 0_1 & 0_1 & 0_2 \\ 0_2 & 0_2 \end{cases}$

di...., In one nonzero district clement in Fq. -> Code locators/ Column locators

elements in Fg -> Column multipliers

Cars 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 Godes.

LRS Codes are MDS Codes. To prove this, we will show that any n-k columns of Maks form a full rank matrix.

Vandermonde Deferminant Formula

$$\frac{\beta_{1}}{\beta_{1}} \beta_{2} \cdots \beta_{r}$$

$$\frac{\beta_{r}}{\beta_{r}} \beta_{2} \cdots \beta_{r}$$

$$\frac{\beta_{r-1}}{\beta_{r}} \beta_{r-1} \cdots \beta_{r}$$

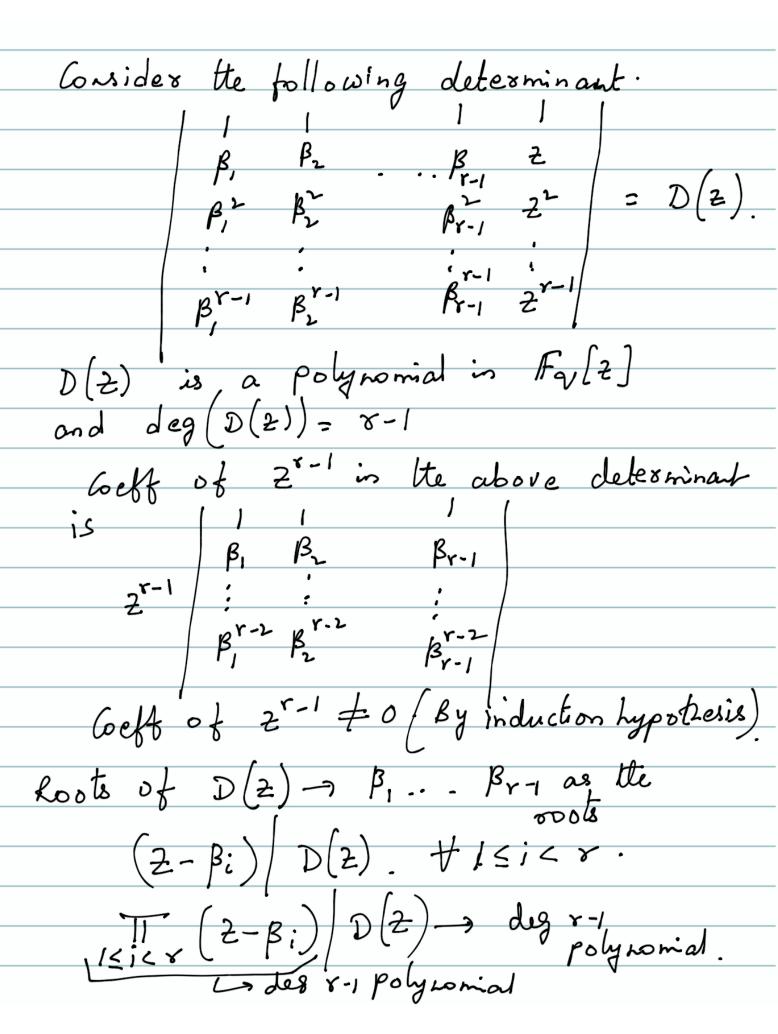
$$\frac{\beta_{r-1}}{\beta_{r}} \beta_{r-1} \cdots \beta_{r}$$

$$\frac{\beta_{r-1}}{\beta_{r}} \beta_{r-1} \cdots \beta_{r}$$

If B, Br..., Br are district elements in the field fly, then determinant is non zero.

Proof is by induction. r= 2 (base case)

Assume induction hypothesis box 8-1



$$D(2) = (Gort) TT(2-13i)$$
.

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

$$\begin{vmatrix}
\beta_1 & \beta_2 & \beta_{r-1} \\
\beta_1^2 & \beta_1^2 & \beta_{r-1}
\end{vmatrix} = \begin{cases}
\beta_1 & \beta_2 & \beta_1 \\
\beta_1^2 & \beta_1^2 & \beta_1^2 & \beta_1 \\
\beta_1^{r-2} & \beta_1^{r-2} & \beta_1^{r-2}
\end{cases}$$
By induction hypothesis.

$$\mathcal{D}\left(2\right):\left(\frac{71}{1\leq i\leq j\leq \gamma-1}\binom{\beta_i-\beta_i}{j-\beta_i}\right)\cdot\left(\frac{71}{1\leq i\leq \gamma}\left(2-\beta_i\right)\right).$$

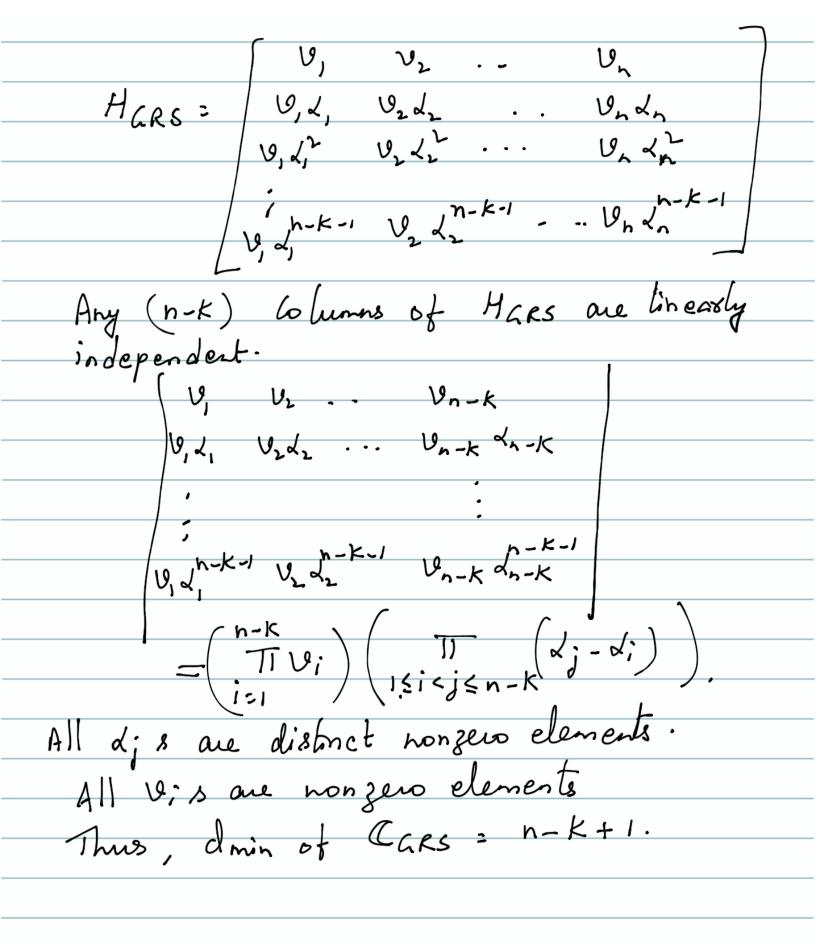
We have defined D(2) by replacing Br with variable 2.

Determinant of Vandermonde matrix of

size 8x8;

D(Br) = (Bj-Bi) (TI (Br-Bi))

[Sicy (Br-Bi)]



Dud of a GRS Gode is also a GRS Gode. Proof - GERS is the parity check matrix for the dual Gode Gars. Hars = 0 Jenevato: matrix & parity check matrix. If there exist 'v', v' ... v' all nonzero elements such that Gars, Hars = 0 we have proved the statement.

We will write (n-1) equations in matrix D Why only n-1, because the equation is only dependent only on the [v',... v'n'] belongs to the Gode.

I Cars with parameters (n,1,n) I a vector which belongs to the Gode is Minimum distance of Cars is his telling you that the vector [vi--.. Vs]
has all nonzero elements.

Interpreting GRS Codewords as polynomial evaluations $\frac{1}{6RS} = \frac{1}{9!} \frac{1}{4!} \frac{1}{4!} \frac{1}{9!} \frac{1}{9$ u = (u0, u,..., uk-1) S= ((1, · --, Cn). $= \frac{u \, G_{RS}}{u_0 \, u_1 \dots u_{k-1}} \int_{1}^{u_1' \, u_2' \, \dots \, u_n'}$ $C_{j} = \sum_{i=0}^{k-1} u_{i} v_{j}(\lambda_{j})^{i} = v_{j}' \left(\sum_{i=0}^{k-1} u_{i} \lambda_{j}^{i}\right)$ Mensage polynomial L k-1 $U(x) = \sum_{i=0}^{\infty} U_i x^i$ $U(x) \longrightarrow \left(V_i u(d_1) V_2 u(d_2) \dots V_n u(d_n)\right)$

Special case of vi=1+j $u(x) \longrightarrow (u(d_1) u(d_2) - \dots u(d_n)).$ Code description of Reed Solomon Code (Case when $0_j'=1+j$) $C_{RS} = \int \left(u(X_1), \dots, u(X_n)\right); u(X_1) \in A_{q_1}[X_1], \dots, u(X_n)$ of $\deg \leq K-1$. Alternate Proof for the MDS property of RS Godes (described in terms of polynomial evaluations). Length of CRS = n. Dinession = K? Look at the menage polynomial u(x) and see Low many free Coeffs are there Up+ u, x+ u2 x2+-- + Uk., xk-1 u; e Haj.

| CRS | is | stu | a | linear | 6 | de | | |
|--------|-------|--------|-----|--------|-----|-------|-------|---|
| Minimu | um (| tistan | æ | of | رنا | neau | Code | |
| = h | ni Wi | n hm | Ha | mmin | g | veigh | t 0 f | a |
| h | on te | no lo | lew | ord. | • | | | |
| f ub | | | | | • | 1 | | |

- =) No. of zero Goordinates in any Lonzero Codeword ≤ K-1
- =) No. of non zero wordinates in any
 hon zero todeword > n-k+1

 dmin > n-k+1

 Singleton
 bound.