Note Title

Finite fields: F_{p^m}, p: prime

- unique

$\pi(x)$: irred poly in $Z_p[x]$, deg m

$$F_{p^m} = \{ a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} : a_i \in Z_p \}$$

$x \bmod \pi(x)$

$\exists\, \alpha$: primitive

$$F_{p^m} = \{ 0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^m - 2} \}$$

Factoring $x^n - 1$ over $\mathbb{Z}_p[x]$

Assume $(n, p) = 1$. $\exists\ m$ s.t. $n \mid (p^m - 1)$

(n, p): gcd(n, p)

$\Downarrow$

$\exists\ \beta \in F_{p^m}$ s.t.

$\text{ord}(\beta) = n$

why? $x^n - 1 = (x - \beta)(x - \beta^2) \cdots (x - \beta^{n-1})(x - 1)$

$\downarrow$ over $F_{p^m}[x]$

Cyclotomic cosets: mod n under mult. by p

$$C_0 = \{0\} \longleftrightarrow \{\beta^0\} = \{1\} : x-1$$

$$C_1 = \{1, p, p^2, \dots\} \longleftrightarrow \{\beta, \beta^p, \beta^{p^2}, \dots\} : M_\beta(x)$$

(mod n)

$\vdots$

- Cyclotomic cosets: partition of $\{0, 1, \dots, n-1\}$

Ex: $n = 9$, $p = 2$ $\quad C_0 = \{0\}, C_1 = \{1, 2, 4, 8, 7, 5\}$

$C_3 = \{3, 6\}$

$\beta \in F_{2^m}$ s.t. $\text{ord}(\beta) = 9$

$$x^9+1 = (x+1)(x+\beta^3)(x+\beta^6)(x+\beta)(x+\beta^2)(x+\beta^4)(x+\beta^8)(x+\beta^5)(x+\beta^7)$$

$(x+1)$ → C_0

$(x+\beta^3)(x+\beta^6)$ → C_3, x^2+x+1

$(x+\beta)(x+\beta^2)(x+\beta^4)(x+\beta^8)(x+\beta^5)(x+\beta^7)$ → $M_{\beta}^{(2)}$, C_1

Ex: $n=10$, $p=3$

$C_0=\{0\}$, $C_1=\{1,3,9,7\}$, $C_2=\{2,6,8,4\}$

$C_5=\{5\}$

BCH codes (binary?)

Linear block code with a PC matrix

H

Minimum distance, d = min # of cols of H that are lin dep

n: block length

We need $\beta \in F_{p^m}$ s.t. $\text{ord}(\beta) > n$.

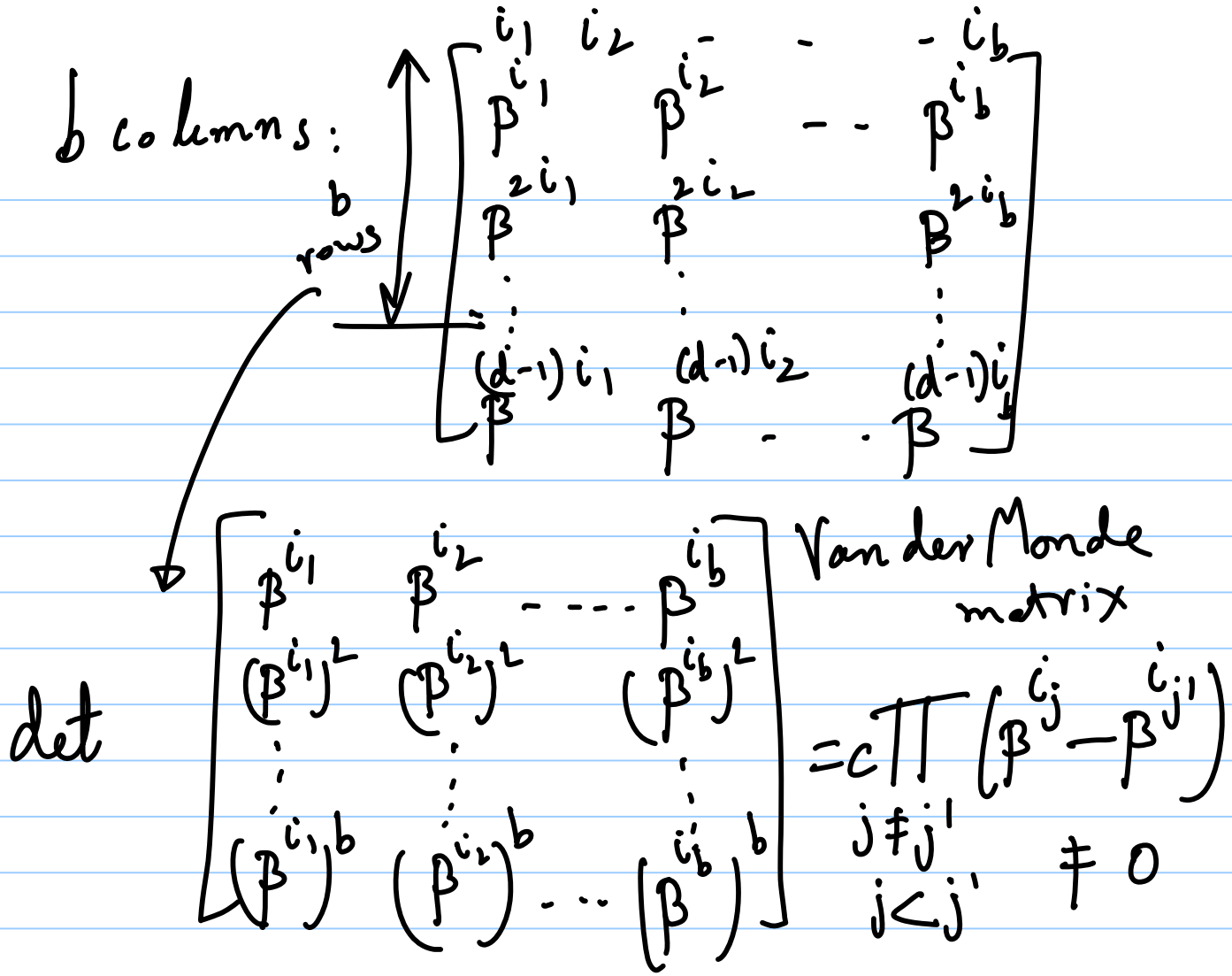
$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & \beta^2 & (\beta^2)^2 & \cdots & (\beta^2)^{n-1} \\ \vdots & & & & \\ 1 & \beta^{d-1} & (\beta^{d-1})^2 & \cdots & (\beta^{d-1})^{n-1} \end{bmatrix}$$

$\text{ord}(\beta) \geq n$

Cols: 0 1 2 ... $n-1$

Claim: $d-1$ or fewer columns are linearly independent

Pf: $b \leq d-1$; b columns: $i_1, i_2, \ldots, i_b$


b columns:
b rows
i_1 i_2 - - - i_b
β^{i_1} β^{i_2} - - β^{i_b}
β^{2i_1} β^{2i_2} β^{2i_b}
$\beta^{(d-1)i_1}$ $\beta^{(d-1)i_2}$ $\beta^{(d-1)i_b}$
β β - - β
det
β^{i_1} β^{i_2} - - - β^{i_b}
$(\beta^{i_1})^2$ $(\beta^{i_2})^2$ $(\beta^{i_b})^2$
$(\beta^{i_1})^b$ $(\beta^{i_2})^b$ - - $(\beta^{i_b})^b$
Vandermonde matrix
$= c \prod_{\substack{j \neq j' \\ j < j'}} (\beta^{i_j} - \beta^{i_{j'}}) \neq 0$

Examples: $n = 15$ $\beta \in GF(16)$, primitive

$d = 3$

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{14} \\ 1 & \beta^2 & \beta^4 & \cdots & \beta^{28} \end{bmatrix}$$

$d = 5$

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{14} \\ 1 & \beta^2 & \beta^4 & \cdots & \beta^{28} \\ 1 & \beta^3 & \beta^6 & \cdots & \beta^{42} \\ 1 & \beta^4 & \beta^8 & \cdots & \beta^{56} \end{bmatrix}$$

.

.

Binary codes from non-binary PC matrices

a) H: $n-k \times n$ matrix over $GF(2^m)$

(n, k, d) Code over $GF(2^m)$: $\{\underline{c} \in \underbrace{GF(2^m)^n}_{} : H\underline{c}^T = \underline{0}\}$

Code over $GF(2)$: $\{\underline{c} \in \underline{GF(2)^n} : H\underline{c}^T = \underline{0}\}$

(sub-field, sub-code) $(n, ?)$ $\quad d_{min} \geq d$