Bounds on the size of codes

Given (n, d) what is the largest k for which there exists an $[n, k, d]$ linear code

$(n, 2^k, d)$ code ?

Singleton bound

For linear codes, every $d-1$ cols of H are linearly independent

$$\#\text{ of rows} = n-k$$

No more than $n-k$ cols can be l.i

$$\Rightarrow \quad d-1 \leq n-k$$

$$d \leq n-k+1$$

Claim: For ANY code, $d \leq n - \lceil \log_q M \rceil + 1$

$$k = \lceil \log_q M \rceil - 1$$

$$q^k \leq M$$

List all possible codewords

Claim : $\exists$ two codewords c_i, c_j st the first l coordinates are the same.

Eg. $l=2$, $q=2$, $M=5$ $n=4$

$\Rightarrow d \leq n-l$

$= n - \lceil \log_q M \rceil + 1$

$= n-k+1$

0	1	1	0
1	0	1	0
0	0	0	1
1	1	1	1
1	0	1	1

Maximum Distance Separable (MDS) codes

A code C_i is MDS if $d = n-k+1$

$= n - \lceil \log_q M \rceil + 1$

$\mathbb{F}_5$

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 2 & 4 \end{bmatrix}$$

$n = 5$

$k = 2$

$n-k+1 = 4$

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 4 & 2 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 3 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{bmatrix}$$

Generalized Reed-Solomon codes

Over $\mathbb{F}_q$, $\alpha_1, \alpha_2, \ldots, \alpha_n$

$$H = \begin{bmatrix} 1 & 1 & & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & & \alpha_n^{n-k-1} \end{bmatrix}$$

$d = n-k+1$

$$\begin{bmatrix} 1 & 1 & & 1 \\ \beta_1 & \beta_2 & \cdots & \beta_{n-k} \\ \beta_1^2 & \beta_2^2 & & \beta_{n-k}^2 \\ \vdots & \vdots & & \vdots \\ \beta_1^{n-k-1} & \beta_2^{n-k-1} & & \beta_{n-k}^{n-k-1} \end{bmatrix}$$

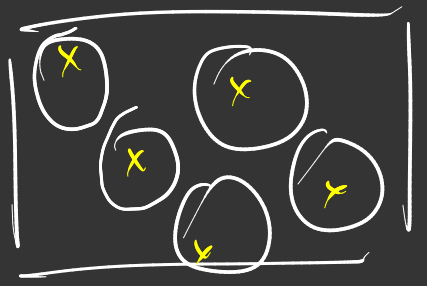
Vandermonde matrix

$$\det = \prod_{i=1}^{n-k} \prod_{j>i+1}^{n-k} (\beta_j - \beta_i)$$

Hamming bound/sphere packing bound

If minimum distance $= d$,

Hamming balls of radius $\frac{d-1}{2}$ centered at codewords cannot intersect



$\mathbb{F}_q^n$

$$M \, V_q(n, r) \leq q^n \qquad r = \frac{d-1}{2}$$

$$M \leq \frac{q^n}{V_q(n, r)}$$

$V_q(n, r)$ = # of pts in $\mathbb{F}_q^n$ which are within Hamming distance r to 0^n

$B_{n,q}(\underline{x}, r)$: Hamming ball of radius r around $\underline{x}$

$$B_{n,q}(\underline{x}, r) = \underline{x} + B_{n,q}(\underline{0}, r)$$

$$V_q(n, r) = \sum_{t=0}^{r} \binom{n}{t} (q-1)^t$$

(0 1 0 1)
(0 1 0 0)
(0 1 1 1)
(0 0 0 1)
(1 1 0 1)

(0 0 0 0)
(0 0 0 1)
(0 0 1 0)
(0 1 0 0)
(1 0 0 0)

$\underline{0}\ \underline{0}\ 0\ \underline{0}$
0 0 0 1

$$V_q(n, r) = \sum_{t=0}^{r} \binom{n}{t} (q-1)^t$$

$$M \leq \frac{q^n}{V_q\left(n, \frac{d-1}{2}\right)}$$

$q = 2$

$n = 7, \quad d = 3 \qquad (n, 2^k, 3)$

$$V_q\left(n, \frac{d-1}{2}\right) = \sum_{t=0}^{1} \binom{7}{t} (2-1)^t = 1 + 7 = 8 = 2^3$$

$$M \leq \frac{2^7}{2^3} = 2^4$$

Perfect codes

An $[n, M, d]$ code is perfect if it meets the Hamming bound

$[7, 4, 3]$ Hamming code $\quad n-k+1 = 7-4+1 = 4$

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \qquad [6, 3, 3]$$

$$\frac{q^n}{V_q(n, \frac{d-1}{2})} = \frac{2^6}{V_2(6, 1)} = \frac{2^6}{8}$$

$$= 2^3$$

$n=6$, $d=4$, $k=2$ $\quad \mathbb{F}_2$

$$V_q(n, \frac{d}{2}-1) = \sum_{t=0}^{1} \binom{6}{t} 6^t$$

$$= 31$$

$$49 < \frac{7^6}{31} = 642.116$$

Gilbert-Varshamov bound

- Start with arbitrary $x_1 \in \mathbb{F}_q^n$
- R_1, C_1 : $C_0 = \{y\}$, $R_0 = \mathbb{F}_q^n$
- Do this until $R_i = \emptyset$
  - $C_i = C_{i-1} \cup \{x_i\}$
  - $R_i = R_{i-1} \setminus B_{n,q}(x_i, d-1)$
  - Pick $x_{i+1} \in R_i$
  - $i \leftarrow i+1$

$V_q(n, d-1)$

$$\frac{q^n}{V_q(n, \frac{d-1}{2})} \geq M \geq \frac{q^n}{V_q(n, d-1)}$$

GV bound

s.t.

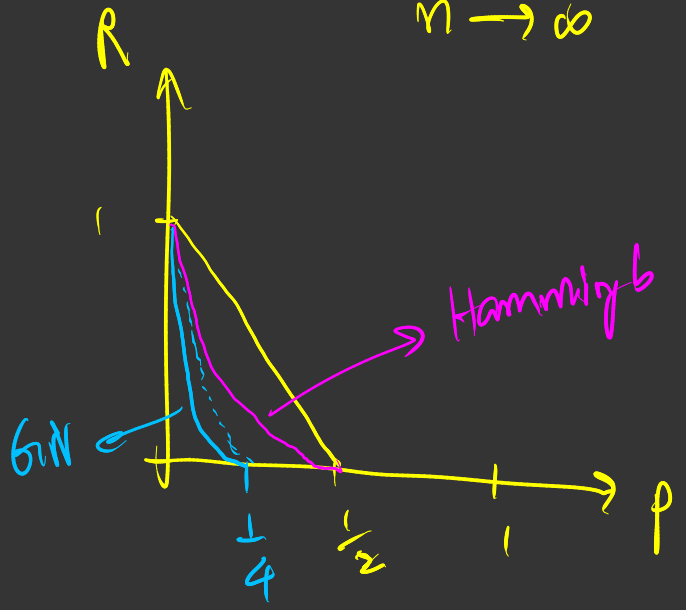
$2^{n(1-h_q(p))}$

$2^{n(1-h_q(2p))}$

$q = 2$

$n \to \infty$

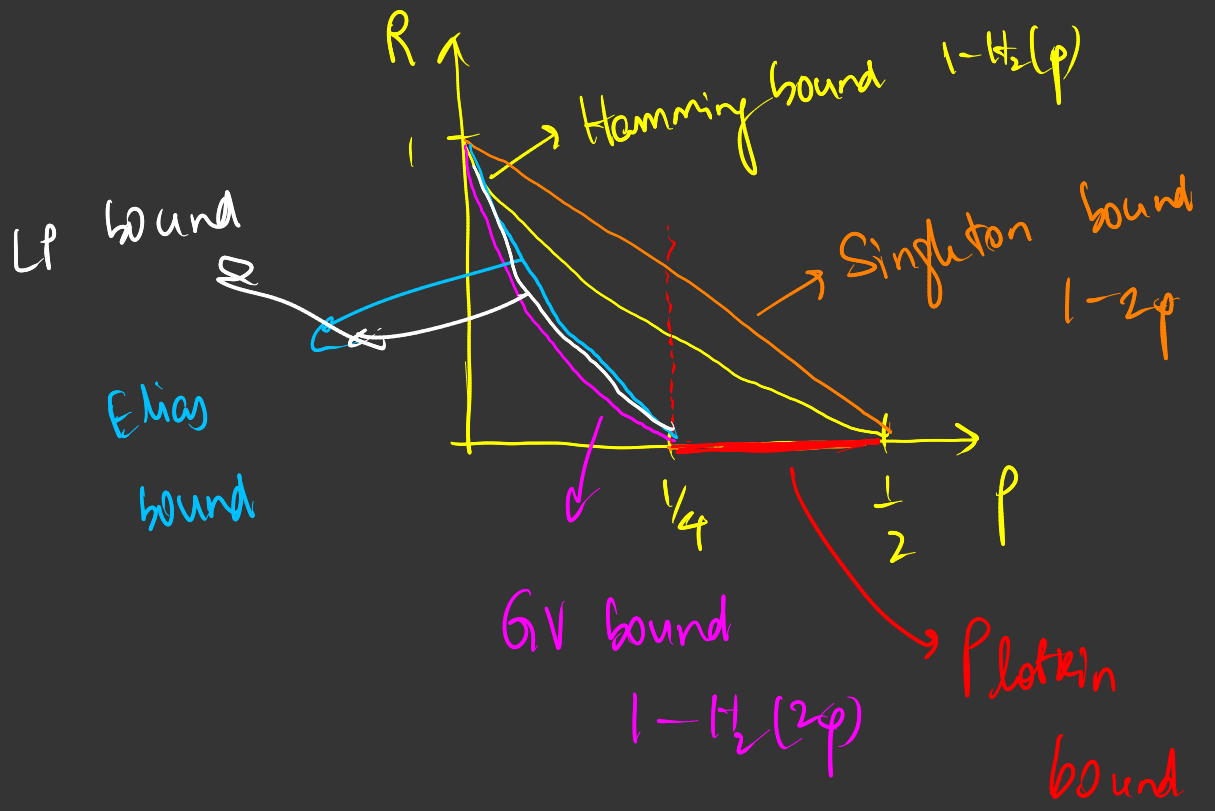
$np \quad V_q(n, 2pn) \approx 2^{nh_q(2p)}$



$k = n - d + 1$

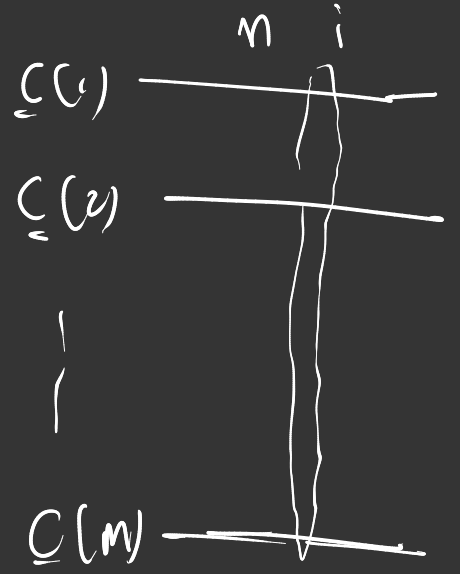
$$\frac{k}{n} = 1 - \frac{d+1}{n} = 1 - \frac{2np+2}{n}$$

$\to 1 - 2p$


R
1
Hamming bound $1-H_2(\rho)$
LP bound
Elias bound
Singleton bound
$1-2\rho$
GV bound
$1-H_2(2\rho)$
Plotkin bound
1/4
1/2
ρ

PLOTKIN BOUND

$$S = \sum_{x \in C} \sum_{y \in C} d_H(x, y)$$



For any (n, M, d) code C,

$$d_H(x, y) \geq d \quad \forall\, x \neq y$$

$$S = \sum_{x \in C} \sum_{y \in C \setminus \{x\}} d_H(x, y) \geq \sum_{x \in C} \sum_{y \in C \setminus \{x\}} d$$

$$= M(M-1)\, d$$

Let us define $n_{i,\alpha}$ = # of times we see α in the i^{th} col of matrix

($\forall 1 \le i \le n, \ \alpha \in \mathbb{F}_q$)

$$= \#\text{ of codewords } \underline{c} \in C \text{ s.t. } c_i = \alpha$$

($\underline{c}(j) \to j^{th}$ codeword)

$$= \sum_{j=1}^{m} 1_{\{c_i(j) = \alpha\}}$$

$$S = \sum_{\underline{x} \in C} \sum_{\underline{y} \in C} d_H(\underline{x}, \underline{y})$$

$$= \sum_{i=1}^{n} \sum_{j_1=1}^{m} \sum_{j_2=1}^{m} 1_{\{c_i(j_1) \neq c_i(j_2)\}}$$

$$= \sum_{i=1}^{n} \sum_{j_1=1}^{m} \sum_{j_2=1}^{m} \sum_{\alpha \in \mathbb{F}_q} 1_{\{c_i(j_1)=\alpha\}} 1_{\{c_i(j_2)\neq\alpha\}}$$

$$= \sum_{i=1}^{n} \sum_{\alpha \in \mathbb{F}_q} \sum_{j_2=1}^{m} \underbrace{\sum_{j_1=1}^{m} 1_{\{c_i(j_1)=\alpha\}}}_{n_{i,\alpha}} 1_{\{c_i(j_2)\neq\alpha\}}$$

$$= \sum_{i=1}^{n} \sum_{\alpha \in \mathbb{F}_q} \underbrace{\sum_{j_2=1}^{m} 1_{\{c_i(j_2)\neq\alpha\}}}_{m-n_{i,\alpha}} (n_{i,\alpha})$$

$$= \sum_{i=1}^{n} \sum_{\alpha \in \mathbb{F}_q} (m-n_{i,\alpha})\, n_{i,\alpha}$$

$$= n \sum_{i=1}^{n} \sum_{\alpha \in \mathbb{F}_q} n_{i,\alpha} - \sum_{i=1}^{n} \sum_{\alpha \in \mathbb{F}_q} n_{i,\alpha}^2$$

$$= n M^2 - \sum_{i=1}^{n} \left(\sum_{\alpha \in \mathbb{F}_q} n_{i,\alpha}^2 \right)$$

$$M^2 = \left(\sum_{\alpha \in \mathbb{F}_q} n_{i,\alpha} \right)^2 \leq \|\underline{n}_i\|_2^2 \, \|\underline{1}\|^2$$

$$= \left(\sum_{\alpha \in \mathbb{F}_q} n_{i,\alpha}^2 \right) (q)$$

$$\langle \underline{n}_i, \underline{1} \rangle$$

$$\underline{n}_i = (n_{i,0}, n_{i,1}, \ldots)$$

$$q$$

$$\Rightarrow \quad \sum_{a \in \mathbb{F}_q} n_{i,a}^2 \geq \frac{M^2}{q}$$

$$M(M-1)d \leq S \leq nM^2 - \sum_{i=1}^{n} \frac{M^2}{q}$$

$$= nM^2 - \frac{nM^2}{q}$$

$$M(M-1)d \leq nM^2\left(1-\frac{1}{q}\right)$$

$$(M-1)d \leq nM\left(1-q^{-1}\right)$$

$$M\left(d - n(1-q^{-1})\right) \leq d$$

$$M \leq \frac{d}{d - n(1-q^{-1})}$$

Plotkin bound $M \leq \left\lfloor \frac{d}{d - n(1-q^{-1})} \right\rfloor$ for $d > n(1-q^{-1})$

$\Rightarrow$ if $d > n(1-q^{-1})$, $R \to 0$ as $n \to \infty$

For $\mathbb{F}_2$,

$d > n/2$, $R \to 0$

$p > 1/4$, $R \to 0$ as $n \to \infty$

Elias bound

Theorem: Let $\alpha = 1 - \frac{1}{q}$. & take $w \le \alpha n$

& $w^2 - 2\alpha n w + n\alpha d \ge 0$

Then,

$$M \le \frac{n\alpha d}{w^2 - 2\alpha n w + n\alpha d} \cdot \frac{q^n}{V_q(n, w)}$$

$\downarrow$

$$M \le \min_{w:\ \text{constr}} \left(\quad \right)$$

constr

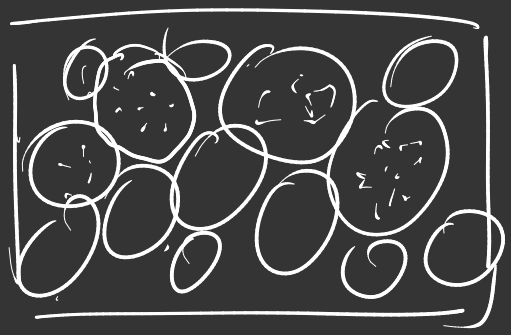
As $n \to \infty$, $M \le \dfrac{n\alpha d}{w^2 - 2\alpha n w + n\alpha d} \, 2^{n(1 - H_2(w) + o(1))}$

Lemma 1 Let C be an (n, M_1, d) code where all codewords have Hamming wt $\leq w \leq qn$

Then, $$d \leq \frac{M_1 w}{M_1 - 1}\left(2 - \frac{w}{qn}\right)$$

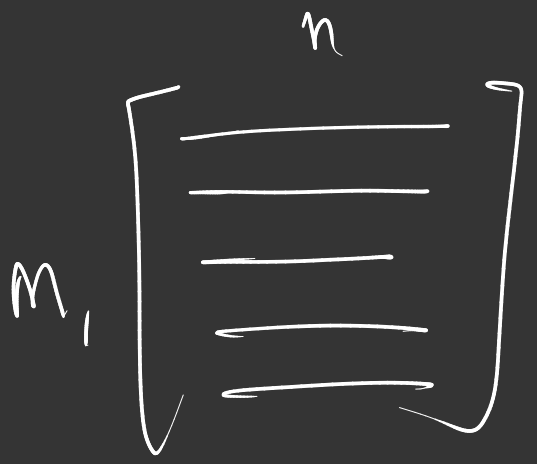
or $$M_1 \leq \frac{nqd}{w^2 - 2nqw + nqd}$$

$n_{i,\alpha}$ = # of codewords c st $c_i = \alpha$.



$$\sum_{\alpha \in \mathbb{F}_q} n_{i,\alpha} = M_1$$

$$T = \sum_{i=1}^{n} n_{i,0} = \#\text{ of } 0\text{'s in codeword matrix}$$



In each codeword, # of 0's $> n - w$

$$T \geq M_1 (n-w)$$

Cauchy Schwartz: $\left(\sum_{\alpha \in \mathbb{F}_q^*} n_{i,\alpha}^2\right) \langle \underline{1}, \underline{1} \rangle \geq \left(\sum_{\alpha \in \mathbb{F}_q^*} n_{i,\alpha}\right)^2$ where $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$

$\underline{\tilde{n}}_i$ = vector of $(n_{i,\alpha} : \alpha \neq 0)$

$$\sum_{\alpha \in \mathbb{F}_q^*} n_{i,\alpha}^2 \geq \frac{1}{q-1} (M_1 - n_{i,0})^2$$

Cauchy Schwartz $\left(\sum_{i=1}^{n} n_{i,0}^2\right) \langle \underline{1}, \underline{1} \rangle \geq \left(\sum_{i=1}^{n} n_{i,0}\right)^2$ | $\underline{N} = (n_{1,0}, n_{2,0} \dots n_{n,0})$

↓ length n

$$\sum_{i=1}^{n} n_{i,0}^2 \geq \frac{1}{n} T^2 \geq \frac{1}{n} M_1^2 (n-w)^2$$

$$\sum_{\alpha \in \mathbb{F}_q^*} n_{i,\alpha}^2 \geq \frac{1}{q-1} (M_1 - n_{i,0})^2$$

$$T \geq M_1(n-w)$$

$$M_1(M_1-1)d \leq S = \sum_{x,y \in C} d(x,y) \leq nM_1^2 - \sum_{i=1}^{n} \sum_{\alpha \in \mathbb{F}_q} n_{i,\alpha}^2$$

$$M_1(M_1-d) \le nM_1^2 - \sum_{i=1}^{n} n_{i,0}^2 - \sum_{i=1}^{n} \sum_{\alpha \in \mathbb{F}_q^\times} n_{i,\alpha}^2$$

$$\le nM_1^2 - \frac{M_1^2(n-w)^2}{n} - \sum_{i=1}^{n} \frac{1}{q-1}(M_1 - n_{i,0})^2$$

$$= nM_1^2 - \frac{M_1^2(n-w)^2}{n} - \frac{1}{q-1}\sum_{i=1}^{n}\left(M_1^2 + n_{i,0}^2 - 2n_{i,0}M_1\right)$$

$$= nM_1^2 - \frac{M_1^2(n-w)^2}{n} - \frac{1}{q-1}\left[nM_1^2 + \frac{1}{n}M_1^2(n-w)^2 - 2M_1^2(n-w)\right]$$

$$M_1(M_1-1)d \le M_1^2 w\left(2 - \frac{w}{nn}\right)$$

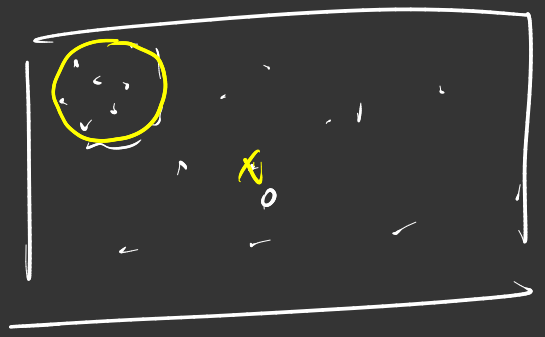
$$d \leq \frac{M_1}{M_1 - 1} w \left(2 - \frac{w}{nn}\right)$$

$$M_1 \leq \frac{nnd}{w^2 - 2nnw + nnd}$$

Lemma: Let C be an (n, M, d) code.
Then there exists an (n, M_1, d) with max wt w
& $M_1 \geq M \frac{V_q(n, w)}{q^n}$

$$M_1 = \max_{x} |B(0,w) \cap (C + x)|$$

Hamming ball of radius w



$$\geq \frac{1}{q^n} \sum_{x \in \mathbb{F}_q^n} |B(0,w) \cap (C + x)|$$

$$= \frac{1}{q^n} \sum_{x \in \mathbb{F}_q^n} \sum_{b \in B(0,w)} \sum_{c \in C} |\{b\} \cap \{c + x\}|$$

$$= \frac{1}{q^n} \sum_{b \in B(0,w)} \sum_{c \in C} \underbrace{\sum_{x \in \mathbb{F}_q^n} 1_{\{b = c + x\}}}_{=1}$$

$$M_1 \geq \frac{1}{q^n} V_q(n, w) \quad M$$

From Lemma 1,

$$\frac{nMd}{w^2 - 2nrw + nrd} \geq M_1 \geq \frac{V_q(n,w)}{q^n} M$$

Linear Programming bounds

For $0 \le w \le n$

$$B_w = \frac{1}{|C|} \sum_{x \in C} |\{ y \in C : d(y, x) = w \}|$$

$|\{ y \in C : d(y, x) = w \}|$: # of c_w at distance w to x

$B_w = 0$ for $1 \le w \le d-1$

$B_0 = 1$

$$\sum_{w=0}^{n} B_w = \frac{1}{|C|} \sum_{x \in C} \left(\sum_{w=0}^{n} \#\text{ of } c_w \text{ at dist } w \text{ to } x \right)$$

$\sum_{w=0}^{n} \#\text{ of } c_w \text{ at dist } w \text{ to } x = |C|$

$= |C|$

$$K_k^{n,q}(x) = \sum_{j=0}^{k} (-1)^j (q-1)^{k-j} \binom{x}{j} \binom{n-x}{k-j}$$

Krawtchouck

$$\sum_{w=0}^{n} B_w K_k^{n,q}(w) \geq 0 \qquad \text{for } 0 \leq k \leq n$$

ASSIGNMENT

C $[n, k, d]$ linear code

$d-1$

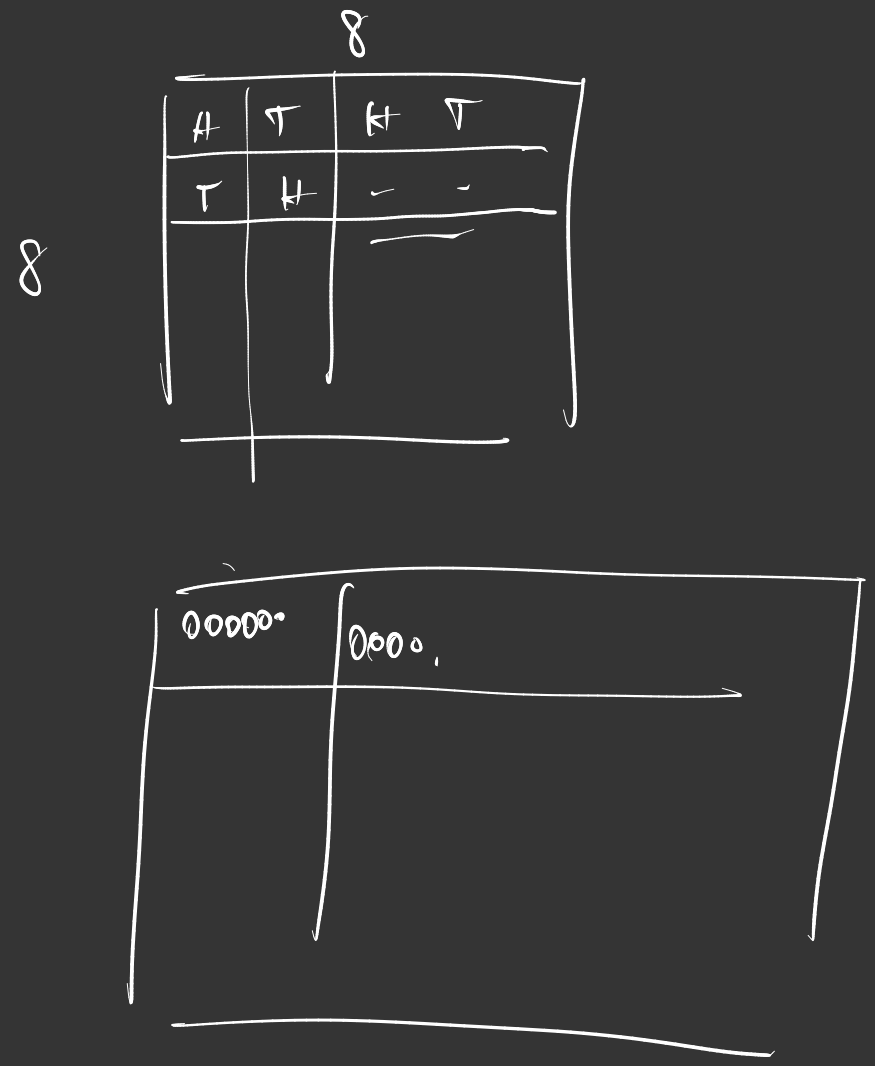
$\underline{x}$ $\qquad$ $\underline{y} = [\underbrace{e\ e\ e \cdots e}_{\underline{x}_E}, \underbrace{x_d, x_{d+1} \cdots x_n}_{\underline{x}_{E^c}}]$

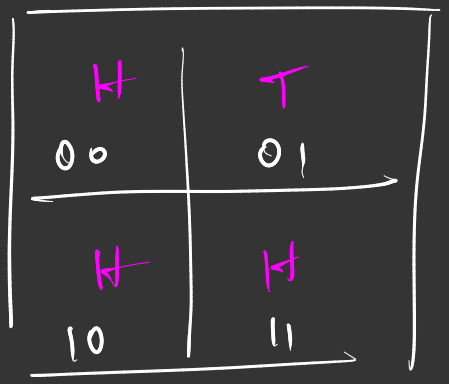
$$H \underline{x}^T = \underline{0}$$

$$\underset{n-k}{\begin{bmatrix} \overset{n}{\overbrace{H_E}^{\leftarrow d-1 \rightarrow}} & H_{E^c} \end{bmatrix}} \begin{bmatrix} \underline{x}_E^T \\ \underline{x}_{E^c}^T \end{bmatrix} = \underline{0}$$

$\underline{b}$

$$H_E \underline{x}_E^T \oplus H_{E^c} \underline{x}_{E^c}^T = \underline{0} \Rightarrow H_E \underline{x}_E^T = -\underline{b}$$

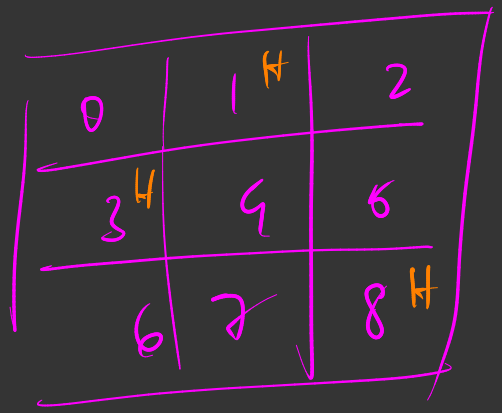

8
8
H
T
H
T
T
H



$00 \oplus 10 = 10$ State

B says 01

$10 \oplus 01 = 11$



$\mathbb{Z}_9$

$S_I \in \mathbb{Z}_9$

$l \in \mathbb{Z}_9$

$S_N = l$

$S_I = r_1 \oplus r_2 \oplus \cdots \oplus r_m$

S_N