Feb 24 | 1 min. check-in

REMINDERS

(1) Video topic due (via Google form) by 11:59pm Wed
- (•) One submission per group please!
- (•) If your group misses this deadline EVERYONE in your group will get 0 on rest of the video points
- (•) If your group member forgets to submit on your group's behalf, YOU'LL pay the penalty as well.
- (•) Reading Assignment; Sec 3.1 + 3.2

RECAP

- (•) Family of codes $\leftarrow$ $[2^r-1, 2^r-1-r, 3]_2$ code
- (•) Can get $R(C)=1$, $\delta(C)=0$ { via $\{C_{H,r}\}_{r\geq 1}$
- (•) Can correct for t errors for any linear code in $O(n^{t+2})$ operations over $\mathbb{F}_q$ (assuming parity check matrix is given)

Plan for today
- (•) Dual of a linear code
- (•) Hadamard code ($\Rightarrow$ $R(C)=0$, $\delta(C)=\frac{1}{2}$ is possible)
- (•) Q: Can we get $R(C)>0$, $\delta(C)>0$

  A: Yes! Via Gilbert-Varshamov (most likely on Wed)
- (•) (Necessary) Digression: q-arty entropy function $\rightarrow$ "Volume" of a Hamming ball

Def (dual of a linear) Let H be a parity check matrix of an $[n,k]_q$ code C. $H \in \mathbb{F}_q^{(n-k)\times n}$

Dual of C ($C^\perp$) is code generated by H. $\underbrace{(\bar{m})}_{n-k} \begin{pmatrix} & H & \end{pmatrix} \updownarrow n-k$, $\leftarrow n \rightarrow$

$C^\perp$ is $[n, n-k]_q$ code $\quad C^\perp = \{\bar{m}\cdot H \mid \bar{m} \in \mathbb{F}_q^{n-k}\}$

rank nullity thm

Ex: $C_{H,r}^\perp \overset{def}{=} C_{Sim,r} \leftarrow H_r$

Simplex code

Hadamard code

$C_{Had,r} \xleftarrow[\text{matrix}]{\text{generator}} H'_r = \begin{array}{c|c} & 1 \quad \cdots \quad 2^r-1 \\ \end{array}$ $r\updownarrow \left(\begin{array}{c|c} 0 & \\ \vdots & H_r \\ 0 & \end{array}\right)$ $\leftarrow 2^r \rightarrow$

ALL vectors in $\in \{0,1\}^r$ are present.

$C_{Sim,r} \quad [2^r-1, r, ?\ ]_2$

$S_{Had,r} \quad [2^r, r, ?\ ]_2$

Proposition: $d(C_{Had,r}) = d(C_{Sim,r}) = 2^{r-1} = \frac{2^r}{2}$

$$wt\left(\boxed{0 \mid \quad c \quad}\right) \underset{=}{\leftarrow} wt\left(\boxed{\quad c \quad}\right)$$

Pf: $d(C_{Had,r}) = 2^{r-1}$ $\qquad$ ~~Every~~ $\min\limits_{\bar{c} \neq \bar{0} \in C_{Had,r}} wt(\bar{c}) = 2^{r-1}$

We'll show Every non-zero $\bar{c} \in C_{Had,r}$ $\quad wt(\bar{c}) = 2^{r-1}$

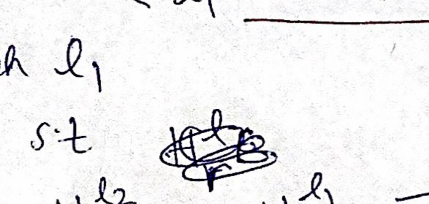
$\equiv \quad \bar{X} \in \mathbb{F}_q^r \setminus \{\bar{0}\} \Rightarrow \exists\, i^* \in [r]$ s.t. $X_{i^*} = 1$ $\qquad H_r^i \doteq bin(i)$

$wt(C_{Had,r}(\bar{X})) = 2^{r-1}$

$$C_{Had,r}(\bar{X}) = (X_1 \ldots, X_r) \underbrace{\begin{pmatrix} \uparrow & \uparrow & & \uparrow & & \uparrow \\ H_r^0 & H_r^1 & \cdots & H_r^i & \cdots & H_r^{2^r-1} \\ \downarrow & \downarrow & & \downarrow & & \downarrow \end{pmatrix}}_{H'_r}$$

Claim: Can partition the 2^r columns of H'_r in 2^{r-1} pairs (ℓ_1, ℓ_2) s.t. $\forall$ pairs (ℓ_1, ℓ_2)

$$\left.\begin{array}{l} H_r^{\ell_1}[i^*] \neq H_r^{\ell_2}[i^*] \\ H_r^{\ell_1}[i] = H_r^{\ell_2}[i] \end{array}\right\} (\#)$$



Pf: for every $0 \le \ell_1 \le 2^r - 1$ s.t. $\underline{H_r^{\ell_1}[i^*] = 0}$

~~For~~ each such ℓ_1 $\qquad$ Q: How many such vectors?

ℓ_2 is s.t. $\qquad$ A: 2^{r-1}

$$i^* \begin{bmatrix} ? \\ ? \\ 0 \\ ? \\ ? \end{bmatrix}$$

(ℓ_1, ℓ_2) satisfy $(*)$ by definition $\Leftarrow$ $\quad \underline{H_r^{\ell_2} = H_r^{\ell_1} + \bar{e}_{i^*}}$

There are 2^{r-1} possibilities of ℓ_1 & for each such ℓ_1, exactly one choice of ℓ_2

$\Rightarrow$ # pairs $(\ell_1, \ell_2) = 2^{r-1}$

$\hookrightarrow$ These partition 2^r vectors into 2^{r-1} pairs

Rest of the proof

$$C_{Had,r}(\bar{x}) \begin{cases} \to \text{loc}_n\ l_1 = \langle \bar{x}, H_r^{l_1} \rangle \\ \to \text{loc}_n\ l_2 = \langle \bar{x}, H_r^{l_2} \rangle \end{cases}$$

$$\langle a, b+c \rangle = \langle a, b \rangle + \langle a, c \rangle$$

$$\langle \bar{x}, H_r^{l_1} \rangle + \langle \bar{x}, H_r^{l_2} \rangle = \langle \bar{x}, H_r^{l_1} \rangle + \langle \bar{x}, H_r^{l_1} + \bar{e}_{i^*} \rangle$$

$$= \underbrace{\langle \bar{x}, H_{r}^{l_1} \rangle + \langle \bar{x}, H_r^{l_1} \rangle}_{=0} + \langle \bar{x}, \bar{e}_{i^*} \rangle$$

$$= \langle \bar{x}, \bar{e}_{i^*} \rangle \qquad \langle (x_1 \ldots x_{i^*}, \ldots x_r), (0 \cdots 0\ 1\ 0\ 0) \rangle$$

$$= x_{i^*}$$

$$= 1.$$

$\Rightarrow$ for every non-zero codeword, I can pair the 2^r values in 2^{r-1} pairs s.t. exactly one of the 2 in the pair is 1.

$\Rightarrow wt(C_{Had,r}(\bar{x})) = 2^{r-1}$ ∎

Big Q: optimal tradeoff between R & δ?

$R(C_{Ham}) = 1$, $\delta(C_{Ham}) = 0$

$$R(C_{Had}) = \lim_{r\to\infty} \frac{r}{2^r} = 0$$

$$\delta(C_{Had}) = \lim_{r\to\infty} \frac{2^{r-1}}{2^r} = \lim_{r\to\infty} \frac{2^r}{2 \cdot 2^r} = \frac{1}{2}$$

Q1: Can we get $R > 0, \delta > 0$?

Q2: $R > 0$, $\delta > \frac{1}{2}$

A1: Yes : Gilbert-Varshamov bound (Wed.)

A2: No: $\delta = \frac{1}{2} \Rightarrow R = 0 \to$ Plotkin bound (Fri/Mon)