February 14, 2019

REMINDERS:

(∘) HW 0 out tonight

↳ <u>OPTIONAL</u> and <u>not</u> graded ← but will provide quick high ~~low~~ level feedback if submitted

(∘) HWs 1-3 out every Th for the next 3 weeks

↳ HW 3 optional for 445 <u>only</u>.

RECAP: Linear code $[n,k,d]_q$

→ Any linear code a $[n,k,d]_q$ C

(1) Can be represented as $C = \{ \bar{x} \cdot G \mid \bar{x} \in \mathbb{F}_q^k \}$

generator matrix $G \in \mathbb{F}_q^{k \times n}$

$$G_{\text{Ham}3} = \begin{pmatrix} 1&0&0&0&0&1&1 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&1&1&1 \end{pmatrix}$$

(2) Also by parity-check matrix $H \in \mathbb{F}_q^{(n-k)\times n}$

$$C = \{ \bar{c} \in \mathbb{F}_q^n \mid H \bar{c}^T = 0 \}$$

$$H_{\text{Ham}3} = \underbrace{\begin{pmatrix} 0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1 \end{pmatrix}}_{\text{binary representation of } 1\text{-}7}$$

(3) C has $O(kn)$ encoding (due to (1))

(4) C has $O((n-k)n)$ error detection (due to (2))

(5) $d(C) = \min\limits_{\substack{\bar{c} \neq 0 \\ \in C}} wt(\bar{c})$

$$MLD_C(y) = \arg\min_{\bar{c} \in C} \Delta(\bar{y}, \bar{c})$$

Volunteer for proof reading?

<u>Another property of linear codes</u>

<u>Lemma 1:</u> Let C be an $[n,k,d]_q$ code with parity-check matrix H. Then d is the <u>minimum</u> number of <u>dependent</u> columns of H. (⇒ any $d-1$ columns are linearly independent)

Note: Max # linearly independent columns can be >> ~~min # of~~ smallest t s.t. any t columns are lin independent.)

Pf: $d \geq$ min # lin dependent columns of H

Let $\bar{c} \in C$ s.t. $wt(\bar{c}) = d$ $\quad \bar{c} = (c_1, \ldots, c_n)$ $\quad S = \{ i \mid c_i \neq 0 \}$

↳ $H\bar{c}^T = 0$

$$\begin{pmatrix} \uparrow & \uparrow & & \uparrow \\ \bar{H}_1 & \bar{H}_2 & \cdots & \bar{H}_n \\ \downarrow & \downarrow & & \downarrow \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0$$

$$\sum_{i=1}^{n} c_i \bar{H}_i = 0 \iff \sum_{i \in S} c_i \bar{H}_i = 0 \Rightarrow \{ \bar{H}_i \mid i \in S \} \text{ is lin dependent}$$

$\Rightarrow d = |S| \geq$ min # lin dependent columns.

→ Other direction in the book.

(General) Hamming Code

$[2^r-1,\ 2^r-r-1,\ 3]_2$ code

$r \geq 2$

So far $r=3$

$$\overset{\longleftarrow\ 2^r-1\ \longrightarrow}{H_r = \left(\quad \boxed{i} \quad \right)} \quad \text{binary representation of } 1 \leq i \leq 2^r-1$$

(H_r has r rows; column i.)

<u>Def</u>: The $[2^r-1,\ 2^r-r-1]_2$ Hamming code $C_{H,r}$ has H_r as its parity check-matrix.

$$C_{H,r} = \{ \bar{c} \in \mathbb{F}_2^{2^r-1} \mid H_r \cdot \bar{c}^T = \bar{0} \}$$

Pf: Argue min # linearly dependent colums $(=t)$ is $=3$

→ $(t \geq 3)$ Any 2 colummns in H_r are linearly independent (they disagree in at least one row)

$\Rightarrow t \geq 3$

→ $(t \leq 3)$ Consider 1st three colums

$$\underset{1}{\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ 1 \end{pmatrix}} + \underset{2}{\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \end{pmatrix}} = \underset{3}{\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 1 \end{pmatrix}}$$

<u>Recall</u>: Hamming Bound $(n,k,3)_2$ code $\Rightarrow k \leq n - \log_2(n+1)$

<u>Note</u>: $C_{H,r}$ is $[2^r-1,\ 2^r-1-r,\ 3]_2$

$\hookrightarrow k = 2^r-1-r = n - \log_2(n+1)$

<u>Def</u>: <u>Perfect</u> code is a code that matches the generalized Hamming bound.

Q: What are the perfect binary codes?

A: (1) Hamming code

(2) Trivial code: All 0s & all 1s vector as codeword

(3) 2 specific codes due to Golay

<u>and that's it (provably)</u>

Family of codes

So far: codes with specific n & k (except $C_{H,r}$; $C_{rep,r}$)

→ from now on: families of codes

$(n, k)_q$ → multiple codes

variable

Def (family of codes) $C = \{C_i\}_{i \geq 1}$ where C_i is an (n_i, k_i, d_i) code ($n_{i+1} > n_i$) is a family of codes. Define

(1) the rate $R(C) = \lim_{i \to \infty} \frac{k_i}{n_i}$

(2) relative distance $\delta(C) = \lim_{i \to \infty} \frac{d_i}{n_i}$

Ex: $C_i = [2^i - 1, 2^i - i - 1, 3]_2$ Hamming code C_H

$$R(C_H) = \lim_{i \to \infty} \frac{2^i - i - 1}{2^i - 1} = 1 - \lim_{i \to \infty} \frac{i}{2^i - 1} = 1$$

$$\delta(C_H) = \lim_{i \to \infty} \frac{3}{2^i - 1} = 0$$

---

from now on, family of codes → Algo: given $i \geq 1$, computes a description of C_i

(intuitive)

↳ $(n, k, d)_q$ code

→ (Def) An algo for an $(n, k, d)_q$ code is one that runs in time poly(n).

Recall: linear codes as a family of codes $[n, k, d]_q$ $O(n^2)$ encoding / error detection algo are efficient.

Big Q: What is the optimal tradeoff between $R(C)$ & $\delta(C)$ for some code family C?

So far: $R(C) = 1$, $\delta(C) = 0$

Next (week): $R(C) = 0$, $\delta(C) = \frac{1}{2}$

Decoding of ~~Hadamard~~ Hamming codes ($C_{H,r}$)

$d(C_{H,r}) = 3 \Rightarrow$ can correct up to 1 error.

MLD runs in time $2^{\Theta(n)}$ $\quad \boxed{n = 2^r - 1}$

$\underline{Q}$: Efficient decoding algo for $C_{H,r}$

$\bar{y} \in \mathbb{F}_2^n$

$$\bar{e}_i = \begin{array}{c} 1 \;\cdots\; n \\ \boxed{0 \text{---} 0 \,|\, 1 \,|\, 0 \text{---} 0} \end{array}$$

$\bar{e}_i$: ith standard basis vector

$O(n^2)$ ① If $\bar{y} \in C_{H,r} \Rightarrow$ return $\bar{y}$

error detection $\Rightarrow O(n^2)$

$O(n^3)$ ② else // exactly one ~~err~~ error $\Rightarrow \bar{y} = \bar{c} + \bar{e}_i$

n times $\rightarrow$ for $i = 1 .. n$

$\bar{y}_i = \bar{y} + \bar{e}_i$

If $\bar{y}_i \in C_{H,r} \Rightarrow$ return $\bar{y}$ $\quad O(n^2)$

③ return NULL. $\quad$ **OVERALL: $O(n^3)$**

$O(1)$

Q: Do the above in $O(n^2)$ $\rightarrow$ Do one mult with H.

$\bar{y} = \bar{c} + \bar{e}_i$ $\quad$ (i unknown)

$$H\bar{y}^T = H(\bar{c}^T + e_i^T) = Hc^T + He_i^T = 0 + He_i^T$$

$$\begin{pmatrix} \uparrow & & \uparrow & & \uparrow \\ H_1 & \cdots & H_i & \cdots & H_n \\ \downarrow & & \downarrow & & \downarrow \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i$$

$= \bar{H}_i \Rightarrow$ can compute e_i from it

$\Rightarrow$ return $\bar{y} + \bar{e}_i$.

If $d = 2t+1$ & binary linear code. Algo to correct $\leq t$ errors?

$O(n^{t+2})$ algo?

Check all $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}$ possible error locations

$\Rightarrow \bar{e}_{\leq t}$ check if $\bar{y} + \bar{e}_{\leq t} \in \mathcal{C} \Rightarrow O\left(n^2 \sum_{i=0}^{t} \binom{n}{i}\right)$

$= O(n^{t+2})$