|Feb 22| 1 min check-in

REMINDERS

(•) HW 1 due by 11:59pm tonight
  (→) Read piazza posts for some clarifications
(•) Video topic (submit via Google form) by 11:59pm NEXT Wed
  (→) Not submitting this means ZERO ON REST of the project grade
(•) HW 2 out next Wed

RECAP

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

Eg. $C_{Ham} = \{C_{H,r}\}_{r\geq 1}$ $n_r = 2^r-1$, $k_r = 2^r-1-r$, $d_r = 3$

Plan for today (•) (Finish) Family of codes
(•) Decoding Hamming codes
(•) [If there is time] Dual of a linear code

Def: (i) rate $R(C) = \mathrm{Lt}_{i\to\infty} \frac{k_i}{n_i}$ $0 \leq R(C) \leq 1$

(ii) relative distance $\delta(C) = \mathrm{Lt}_{i\to\infty} \frac{d_i}{n_i}$ $0 \leq \delta(C) \leq 1$

} assuming these limits exists

Big Q: What is the optimal tradeoff between $R(C)$ & $\delta(C)$ (over all possible family of codes)?

$$R(C_{H,r}) = \mathrm{Lt}_{r\to\infty} \frac{2^r-1-r}{2^r-1} = \mathrm{Lt}_{r\to\infty} 1 - \overset{\to 0}{\frac{r}{2^r-1}} = 1$$

$$\delta(C_{H,r}) = \mathrm{Lt}_{r\to\infty} \frac{3}{2^r-1} = 0$$

From now on, we'll call a family of codes as (just) code.

$(n,k,d)_q \rightarrow$ "self-contained description"

$\rightarrow$ Algo: Given $i \geq 1$, computes of description of C_i

variables

Eg. If C_i is linear, G_i / H_i

Recall: Set of all linear codes is a family of codes.

$[n,k,d]_q$ linear codes $\rightarrow$ $O(n^2)$ encoding + error detection

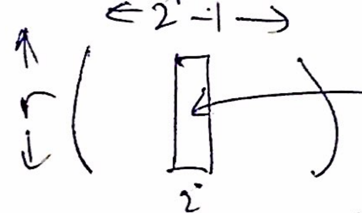
Big Q: $R(C)$ vs. $\delta(C)$ so far: $R(C)=1$, $\delta(C)=0$

(Hamming code, Parity code)

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

Decoding of $C_{H,r}$

$H_r =$



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

bin(i) $\quad d(C_{H,r}) = 3$

$\Rightarrow$ ~~can correct~~ 1-e.c.

MLD to show above $\Rightarrow O(2^k n) \rightarrow 2^{\Omega(n)}$

Q: Efficient decoding of C_{Ham}?

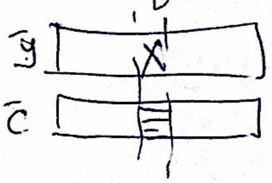
$\hookrightarrow$ Efficient algo $\rightarrow$ run in poly(n) time

$\rightarrow$

Input: $\bar{y} \in \mathbb{F}_2^n$ (Assume $\exists\, \bar{c} \in C_{H,r}$ s.t. $\Delta(\bar{c},\bar{y}) \leq 1$

$O(n^2) \Rightarrow$ output: $\bar{c}$)

```
① If $H_r \bar{y}^T = \bar{0}$ ⇒ return $\bar{y}$   // $\bar{y} \in C_{H,r}$   ∃ i
                                 ↑ O(n)
② else   // $\Delta(\bar{y}, \bar{c}) = 1$
n → for i = 1..n:
        If $H_r(\bar{y}+\bar{e_i})^T = \bar{0}$  }
            return $\bar{y}+\bar{e_i}$           } O(n^2)
③ return ⊥
         ↑ O(1)
```



$\bar{y} = \bar{c} + \bar{e_i}$

$\bar{e_i}$ [0··0|1|0··0]
i

Overall: $O(n^2) + n \cdot O(n^2) + O(1)$

$= O(n^2) + O(n^3) + O(1)$

$= O(n^3)$

Q: Can you do this $O(n^2)$ time ?

Hint: Just need to compute $H_r \bar{y}^T$

$\bar{y} = \bar{c} + \bar{e}_{\textcircled{i}}$ unknown

$$\boxed{H\bar{y}^T} = H(\bar{c} + \bar{e}_i)^T$$
$$= H(\bar{c}^T + \bar{e}_i^T)$$
$$= \underbrace{H\bar{c}^T}_{=\bar{0}} + H\bar{e}_i^T$$
$$= H\bar{e}_i^T$$

$$\underset{H_r}{\begin{pmatrix} \uparrow & & \uparrow & & \uparrow \\ H_1 & \cdots & H_i & - & H_n \\ \downarrow & & \downarrow & & \downarrow \end{pmatrix}} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ \vdots \end{pmatrix} \; i$$

$= H_i \; = \text{bin}(i)$

Algo sketch: (i) $\bar{z} \leftarrow \boxed{H\bar{y}^T}$ $O(n^2)$

(ii) If $\bar{z} = \bar{0}$ $\Rightarrow$ return $\bar{y}$

else

$i' \leftarrow \text{binary}^{-1}(z)$

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

$\Big\}$ $O(n^2)$ algo

General ~~[illegible]~~ algo: $d = 2t+1$ $[n, k, d]_2$ code

↳ t-e.c.

Idea: check all ~~[illegible]~~ error patterns $\bar{e}_{\leq t} \in \mathbb{F}_2^n$ ← $O(n^t)$

$wt(\bar{e}_{\leq t}) \leq t$

If ~~[illegible]~~ $\boxed{H(\bar{y} + \bar{e}_{\leq t})^T = \bar{0}}$ $\Rightarrow$ return $\bar{y} + \bar{e}_{\leq t}$

$O(n^2)$

Overall: $O(n^t) \cdot O(n^2) = O(n^{t+2})$