Feb 18 REMINDERS

(•) Project groups assigned (•) Video topic due ~ 2 weeks

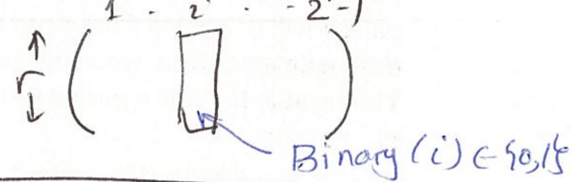
(•) HW 1 is out ; Due by 11:59pm Wed next week (Mar 2)

RECAP:

→ $[n,k,d]_q$ code

→ $r \geq 2$: $[2^r-1, 2^r-1-r, 3]_2$ Hamming code $C_{H,r} = \{ \bar{c} \in \mathbb{F}_2^{2^r-1} \mid H_r \cdot \bar{c}^T = 0 \}$

↳ Parity check matrix H_r =



Proof readers: Shaik , Vinu

Plan for today (1) family of codes (2) Decoding Hamming codes [If there is time left] (3) Dual of a linear code

---

Family of codes (Book: Sec 1.8)

So far: codes with specific n & k e.g. $C_\oplus$ $[5,4,2]_2$ code

from now on: family of codes

$(n,k)_q \rightarrow$ multiple codes

variable

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

E.g. $C_{Ham} = \{C_{H,r}\}_{r \geq 1}$ is ~~an~~ a family of codes $(n_r = 2^r-1, k_r = 2^r-1-r, d_r = 3)$

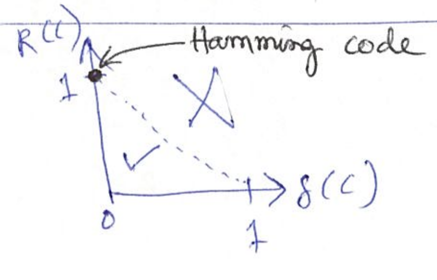
Define:

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

(2) the (relative) distance $\delta(C) = \mathrm{Lt}_{i \to \infty} \frac{d_i}{n_i}$

if the limit ∃

Big Q: What is the optimal tradeoff b/w $R(C)$ & $\delta(C)$ ~~for~~ over all families of codes C?



$$R(C_{Ham}) = \underset{r\to\infty}{Lt} \frac{k_r}{n_r} = \underset{r\to\infty}{Lt} \frac{2^r-1-r}{2^r-1} = \underset{r\to\infty}{Lt}\, 1 - \frac{r}{2^r-1}$$

$$= 1.$$

$$\delta(C_{Ham}) = \underset{r\to\infty}{Lt} \frac{d_r}{n_r} = \underset{r\to\infty}{Lt} \frac{3}{2^r-1} = 0$$

From now on, we'll call a family of code to be (just) code

$(n,k,d)_q$ code $\to$ (intuitive)

variables

$\to$ Algo : given $i \geq 1$, computes a description of C_i

Recall: linear codes as a family of code

$[n,k,d]_q$ code $O(n^2)$ encoding

$O(n^2)$ error detection

Big Q: $R(C)$ vs $\delta(C)$

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

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

Decoding of $C_{H,r}$ $d(C_{H,r}) = 3 \Rightarrow$ correct 1-error.

MLD! In general $2^{O(n)}$

Q: Efficient decoding of ~~$C_{H,r}$~~ C_{Ham}?

$\uparrow$ Efficient algo $\to$ runs in poly(n) time.

Input: $y \in \mathbb{F}_2^n$ $n = 2^r - 1$

$O(n^2)$

[~~Output~~ Assume $\exists\, \overline{c} \in C_{H,r}$ s.t $\Delta(\overline{y}, \overline{c}) \leq 1$]

$\Rightarrow$ output $\overline{c}$

```
① If $\boxed{H_r \cdot \overline{y}^T} = \overline{0}$ ⇒ return $\overline{y}$  // $\overline{y} \in C_{H,r}$
② else // $\Delta(\overline{y}, \overline{c}) = 1$ or $\overline{y} = \overline{c} + \overline{e_i}$
   $O(n^3)$ {  for $i = 1..n$
                  if $H_r \cdot (\overline{y} + \overline{e_i})^T = \overline{0}$   } $O(n^2)$
                     return $\overline{y} + \overline{e_i}$
③ return $\perp$ ← $O(1)$
```

$\overline{e_i}$ $\nearrow$ $[0 \text{—} 0 \,|\, \overset{i}{1} \,|\, 0 \text{—} 0]$ i^{th} standard basis vector

$\equiv$ ~~$\overline{y} \oplus \overline{e_i} \equiv$~~ $\overline{c} = \overline{y} - \overline{e_i}$

holds over $\mathbb{F}_2$ since ~~we are working over $\mathbb{F}_2$~~ $= \overline{y} + \overline{e_i}$

Overall : $O(n^2) + O(n^3) + O(1) = O(n^3)$.

Q: Can you do decoding in $O(n^2)$? for $C_{H,r}$

$\bar{y} = \bar{c} + \bar{e}_i$ $\qquad H\bar{y}^T = H(\bar{c} + \bar{e}_i)^T$

$$= H(\bar{c}^T + \bar{e}_i^T)$$

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

$$\begin{pmatrix} \uparrow & & \uparrow \\ H_1 & \cdots & H_n \\ \downarrow & & \downarrow \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} i = \begin{pmatrix} H_i \end{pmatrix} = \text{binary}(i) \text{ for } C_{H,r}$$

Algo sketch: (i) ~~compute~~ $\bar{z} = H\bar{y}^T$ $\}$ $O(n^2)$

(ii) $i \leftarrow \text{binary}(\bar{z})$

(iii) return $\bar{y} + \bar{e}_i$ $\}$ $O(n)$ $\Rightarrow$ overall $O(n^2)$

General algo: $d = 2t+1$ $\qquad [n,k,d]_2$ code $\qquad O(n^t)$

check all possible error patterns $\bar{e}_{\leq t}$ s.t. $wt(\bar{e}_{\leq t}) \leq t$

If $H \cdot (\bar{y} + \bar{e}_{\leq t})^T = \bar{0} \Rightarrow$ output $\bar{y} + \bar{e}_{\leq t}$

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