April 11

REMINDERS

① HW 5 due 11:59pm Wed (see post on piazza)

② HW 6 (last HW! yay!) out by 11:59pm Wed

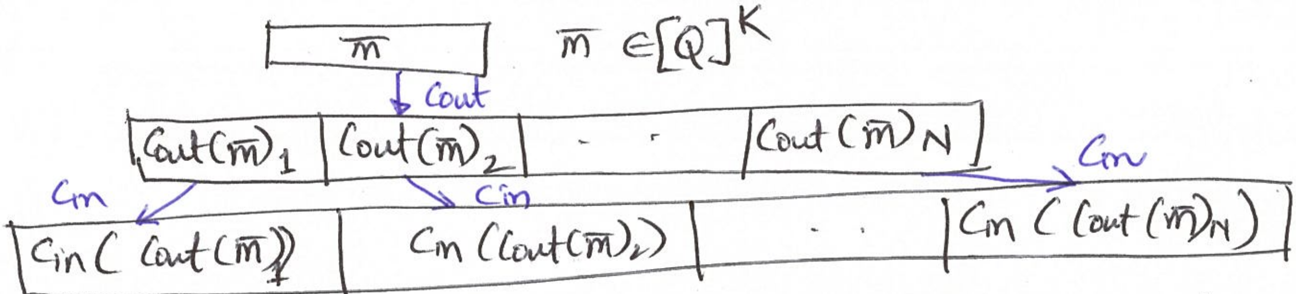
③ Video due ~ 4.5 weeks by 11:59pm Wed, May 11

RECAP:

Q: Explicit asymptotic good codes $\boxed{\text{(that we can efficiently correct from } \rho>0 \text{ frac. of errors)}}$?

(•) Code Concatenation $\quad C_{out} : [Q]^K \to [Q]^N \quad (Q = q^k)$

$\quad C_{in} : [q]^k \to [q]^n$



$C_{out} \circ C_{in}(\bar{m}) = \left(C_{in}(C_{out}(\bar{m})_1), C_{in}(C_{out}(\bar{m})_2), \ldots, C_{in}(C_{out}(\bar{m})_N) \right)$

(•) ~~Justesen codes~~

Wozencraft ensemble: $N = q^k - 1$. Let $\varepsilon > 0$ be small enough.

$\exists$ strongly explicit ensemble $C_{in}^1, \ldots, C_{in}^N$ s.t. $R(C_{in}^j) = \frac{1}{2}$

$\geq (1-\varepsilon)N$ values of $j \in [N]$

$\delta(C_{in}^j) \geq H_q^{-1}(\frac{1}{2} - \varepsilon)$

(•) Justesen codes: $\underset{\text{RS (rate } R)}{C_{out}} \circ (\underbrace{C_{in}^1, \ldots, C_{in}^N}_{\text{Wozencraft ensemble}}) \Rightarrow$ strongly explicit

code of rate $\frac{R}{2}$ & $\delta = (1 - R - \varepsilon) H_q^{-1}(\frac{1}{2} - \varepsilon)$

TODAY

(•) Proof readers: Qi, Juliana

(•) Wozencraft ensemble

(•) Decoding concat code ($\Rightarrow$ answer Q above in affirmative!)

Wozencraft ensemble $N = q^k - 1$

$C_{in}^1, \ldots, C_{in}^N$ $\quad R(C_{in}^i) = \frac{1}{2} \; \forall i$

$\geq (1-\varepsilon)N$ values $j \in [N]$

$\delta(C_{in}^j) \geq H_q^{-1}(\frac{1}{2} - \varepsilon)$

Re-index codes by $\alpha \in \mathbb{F}_{q^k}^*$ $\left[\mathbb{F}^* \overset{\text{def}}{=} \mathbb{F}^* \setminus \{0\} \right]$

$$C_{in}^\alpha : \mathbb{F}_q^k \to \mathbb{F}_q^{2k} \Rightarrow R(C_{in}^\alpha) = \frac{1}{2} \quad \forall \alpha \in \mathbb{F}_{q^k}^*$$

(assuming dist ≥ 1) C_{in}^α is linear

$$\underset{\in \mathbb{F}_q^k}{C_{in}^\alpha(x)} \to (x, \underbrace{\alpha \cdot x}_{\text{mult over } \mathbb{F}_{q^k}})$$

$\alpha, x \in \mathbb{F}_{q^k}$; interpret the result in $\mathbb{F}_q^k$

Fact: $\exists$ a (linear) bijection $\mathbb{F}_{q^k} \to \mathbb{F}_q^k$

Pf: ($\geq (1-\varepsilon) N$ values of $\alpha \in \mathbb{F}_{q^k}^*$)

$$\delta(C_{in}^\alpha) \geq H_q^{-1}(\tfrac{1}{2} - \varepsilon)$$

$Q = q^k$

$C_{out}: (\mathbb{F}_{q^k})^K \to (\mathbb{F}_{q^k})^n$

Goal: For most α, C_{in}^α doesn't have any non-zero codeword of Ham wt $< H_q^{-1}(\frac{1}{2} - \varepsilon) \cdot \underset{=2k}{n_{in}}$

Fix $\bar{y} = (\bar{y}_1, \bar{y}_2) \in (\mathbb{F}_q^k)^2 \setminus \{(\bar{0}, \bar{0})\} \Rightarrow (\bar{y}_1 = \bar{y}_2 = \bar{0} \text{ X})$

Claim: Every $(\bar{y}_1, \bar{y}_2)$ is in at most one C_{in}^α

$(\bar{y}_1, \bar{y}_2) \in C_{in}^\alpha \Rightarrow \bar{y}_2 = \alpha \cdot \bar{y}_1$

Pf: By case analysis

Case 1: $\bar{y}_1 \neq \bar{0}, \bar{y}_2 \neq \bar{0} \Rightarrow \alpha = \dfrac{\bar{y}_2}{\bar{y}_1}$ Note since all ops over $\mathbb{F}_{q^k}$, α is unique.

Case 2: $\bar{y}_1 \neq \bar{0}, \bar{y}_2 = 0 \Rightarrow \alpha = \dfrac{\bar{y}_2}{\bar{y}_1} = 0$ (not possible as $\alpha \neq 0$)

Case 3: $\bar{y}_1 = 0, \bar{y}_2 \neq 0 \Rightarrow \bar{y}_2 = \alpha \cdot \bar{y}_1 = \alpha \cdot 0 = 0$ (not possible as $\bar{y}_2 \neq \bar{0}$)

$$\left| \{\alpha \mid \delta(C_{in}^\alpha) < H_q^{-1}(\tfrac{1}{2} - \varepsilon)\} \right| \quad (\text{want} \leq \varepsilon N)$$

$$\underset{\text{uses claim}}{\leq} \left| \{ \bar{y} \in \mathbb{F}_q^{2k} \setminus \{\bar{0}\} \mid wt(\bar{y}) < H_q^{-1}(\tfrac{1}{2} - \varepsilon) \cdot 2k \} \right|$$

$$\leq Vol_q(H_q^{-1}(\tfrac{1}{2} - \varepsilon) \cdot 2k, 2k)$$

$$\le q^{H_q(H_q^{-1}(\frac{1}{2}-\varepsilon))\cdot 2k} = q^{(\frac{1}{2}-\varepsilon)2k} = \frac{q^k}{q^{2\varepsilon k}} < \varepsilon(q^k-1) = \varepsilon \cdot N$$ ∎

Decoding concatenated codes

$N = Q = q^k$

Assume: (i) C_{out} is RS code $[N,K,D]_Q$ code

(ii) $\exists$ a unique decoder for RS codes in $O(N^3)$ operations over $\mathbb{F}_Q$

Prove this in a later lecture

$\frac{1-R}{2}$ frac of errors

$\Downarrow$

D_{out} for C_{out} decodes $\frac{D}{2}$ errors

$\rightarrow D_{in}$ (unique decoder for C_{in}) $\rightarrow MLD_{C_{in}} \rightarrow q^{O(k)}$ time $=$ poly(N) time $=$ poly(N_n) time ($N = N_n$)

$(\mathbb{F}_q^n)^N \ni \bar{y}$: $\quad | y_1 | y_2 | \cdots | y_N |$

$\downarrow D_{in} \quad \downarrow D_{in} \quad \downarrow D_{in}$

$(\mathbb{F}_q^k)^N \ni \bar{y}'$: $\quad | y_1' | y_2' | \cdots | y_N' |$

$\downarrow D_{out}$

$| \bar{m}' |$ $\quad \bar{m}' \in (\mathbb{F}_{q^k})^K$

Hope: $\bar{m}' = \bar{m}$ (transmitted message)

Algo 1: input $\bar{y} = (y_1, \ldots, y_N) \in (\mathbb{F}_q^n)^N$

1. $\bar{y}' \leftarrow (y_1', \ldots, y_N')$ s.t. $\underbrace{C_{in}(y_i') = D_{in}(\bar{y}_i)}_{\text{poly}(N) \text{ for a given } i}$ $\forall\ 1 \le i \le N$
2. $\bar{m}' \leftarrow D_{out}(\bar{y}') \leftarrow O(N^3)$
3. Return $\bar{m}'$

Overall: $O(N^3) + N \cdot \text{poly}(N) \le \text{poly}(N)$

Lemma 1: Algo can correct from $< \frac{Dd}{4}$

Pf: $\bar{m} \in (\mathbb{F}_q^k)^K$ s.t. $\Delta(\bar{y}, C_{out} \circ C_{in}(\bar{m})) < \frac{Dd}{4}$

$\uparrow$ Such an $\bar{m}$ is unique since dist of $C_{out} \circ C_{in} \ge Dd$

Argue: Algo 1 outputs $\bar{m}$.