April 4, 2019

REMINDERS.

① Reports to be graded by Tue
② HW 3 grading a week after that
③ Video due 3 weeks from this coming Tue

RECAP:

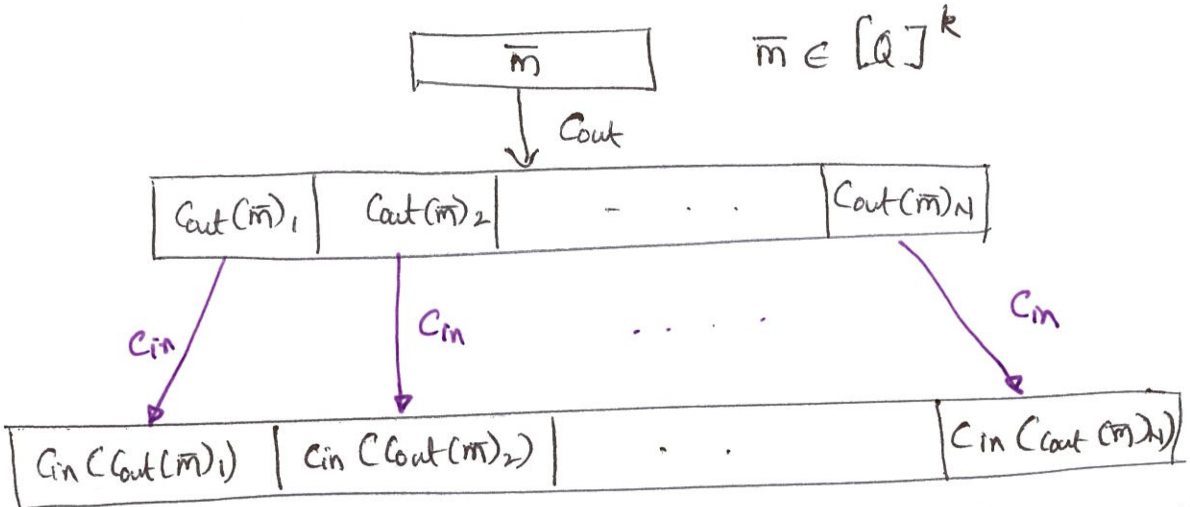
Q: (Strongly) Explicit asymptotically good code (i.e. $R>0, \delta>0$)?

Code Concatenation:

$C_{out} : [Q]^K \rightarrow [Q^N]$ $\quad Q = q^k$

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

$\overline{m} \in [Q]^k$



THM: If C_{out} is an $(N,K,D)_Q$ code $\Rightarrow$ $C_{out} \circ C_{in}$ is an $(Nn, Kk, Dd)_q$ code. $\quad D, d \geq 1$

C_{in} ——— $(n,k,d)_q$ ———

↖ Did not prove this last time.

Ex: Linearity is preserved.

TODAY [Proof reader: Yunus]

(•) Prove THM above
(•) Zyablov bound
- ↳ Explicit code
- ↳ $R>0, \delta>0$

(•) Strongly explicit asymptotically good code.

Pf of THM 1: $C_{out} \circ C_{in}$ $(\mathcal{N}, \mathcal{K}, \mathcal{D})_q$ code.

$\mathcal{N} = Nn$. As we'll argue $\mathcal{D} = Dd$ (≥ 1) $\Rightarrow \mathcal{K} = Kk$.

Let $S = \{ i \in [N] \mid C_{out}(\bar{m}_1)_i \neq C_{out}(\bar{m}_2)_i \}$ fix $\bar{m}_1 \neq \bar{m}_2 \in [q^k]^K$

$\Rightarrow$ If $i \in S$ $\Rightarrow$ $\Delta(C_{in}(C_{out}(\bar{m}_1)_i), C_{in}(C_{out}(\bar{m}_2)_i)) \geq d$

$\Rightarrow$ Overall Dist $\geq |S| \cdot d \geq Dd$

as C_{out} has dist D.

Zyablov bound:

C_{out}: Singleton bound. RS code of rate R, $\delta_{out} \geq 1-R$

C_{in}: GV bound; rate r, δ_{in} $\quad r \geq 1 - H_q(\delta_{in}) - \varepsilon$

$\equiv \delta_{in} \geq H_q^{-1}(1-r-\varepsilon)$

$C_{out} \circ C_{in}$: $\mathcal{R} = Rr$, rel dist $\delta = \delta_{out} \cdot \delta_{in}$

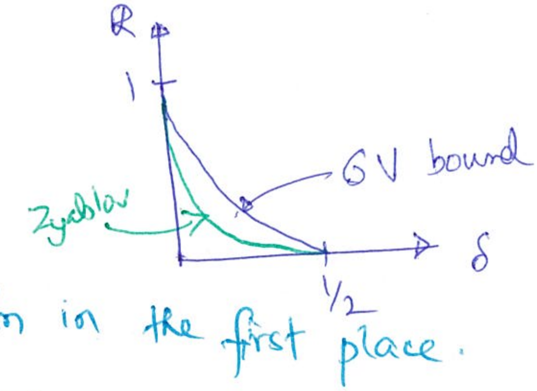
$\geq (1-R)\, H_q^{-1}(1-r-\varepsilon)$

$$R = 1 - \frac{\delta}{H_q^{-1}(1-r-\varepsilon)} \quad \Leftarrow$$

$$\mathcal{R} \geq \max_{0 \leq r < 1 - H_q(\delta) - \varepsilon} r\left(1 - \frac{\delta}{H_q^{-1}(1-r-\varepsilon)}\right).$$

$\Rightarrow$ $\delta = \frac{1}{2} - \varepsilon$, $R_{GV} \geq \Omega(\varepsilon^2)$

$R_Z \geq \Omega(\varepsilon^3)$



Q: How do we get our hands on C_{in} in the first place.

→ get such a code in $q^{O(kn)}$ time

→ ——— $q^{O(n)}$ ——— (Q2 on HW2)

use this!

C_{out}: $RS \Rightarrow N = q^k \Rightarrow k \leq O(\log_q N)$

assume $r > 0 \Rightarrow n = O(k) \Rightarrow n \leq O(\log_q N)$

$\Rightarrow q^{O(n)} = q^{O(\log_q N)} = N^{O(1)} = N^{O(1)}$.

$\Rightarrow$ Construct code of $R > 0$ on Zyblov bound in poly(N) ~~time~~ time

$\Rightarrow$ ~~As~~ Explicit Asymptotically good code.

Q: Strongly Explicit asymptotically good codes?

Justesen codes

Idea: Use different inner codes $\overbrace{C_{in}^{1}, \ldots, C_{in}^{N}}^{\text{ensemble}}$

$$C_{out} \circ C(C_{in}^{1}, \ldots, C_{in}^{N})(\bar{m}) = \left(C_{in}^{1}\left(C_{out}(\bar{m})_1\right), C_{in}^{2}\left(C_{out}(\bar{m})_2\right), \ldots, C_{in}^{N}\left(C_{out}(\bar{m})_N\right)\right)$$

Wozencraft ensemble: Let $\varepsilon > 0$, $\exists$ an strongly explicit ensemble

all linear $\{C_{in}^{1}, \ldots, C_{in}^{N}$ s.t. $R(C_{in}^{j}) = \frac{1}{2}$, $N = q^k - 1$ s.t.

for at least $(1-\varepsilon)N$ values of j $\quad \delta(C_{in}^{j}) \geq H_q^{-1}(\frac{1}{2} - \varepsilon)$

Justesen code: $\quad C_{out}$: rate R $\quad$ RS $\quad N = q^k - 1$ eval pts $= \mathbb{F}_{q^k}^{*}$

$\delta_{out} = 1 - R$

$$C^{*} = C_{out} \circ (\underbrace{C_{in}^{1}, \ldots, C_{in}^{N}}_{\text{Wozencraft ensemble.}}) \qquad R(C^{*}) = \underbrace{R}_{C_{out}} \cdot \underbrace{\frac{1}{2}}_{\text{Wozencraft ensemble}} = \frac{R}{2}$$

PROP: $\delta(C^{*}) \geq (1 - R - \varepsilon) \cdot H_q^{-1}(\frac{1}{2} - \varepsilon)$.

$\Rightarrow$ Strongly explicit code of an rate $0 < R < \frac{1}{2}$, $\delta > 0$.

Pf of PROP: $\quad \bar{m}_1 \neq \bar{m}_2 \in (\mathbb{F}_{q^k})^K$

$$S = \{ \underset{\in [N]}{j} \mid C_{out}(\bar{m}_1)_j \neq C_{out}(\bar{m}_2)_j \}$$

$|S| \geq (1-R) N \quad$ (as C_{out} has $\delta_{out} \geq 1-R$)

$S_g = \{ j \in S \mid \delta(C_{in}^{j}) \geq H_q^{-1}(\frac{1}{2} - \varepsilon) \}$; $S_b = S \setminus S_g$

Claim: ~~$\Delta(C^{*}(\bar{m}_1), C^{*}(\bar{m}_2)) \geq$~~ $|S_g| \geq (1 - R - \varepsilon) N$

$\Rightarrow \Delta(C^{*}(\bar{m}_1), C^{*}(\bar{m}_2)) \geq (1 - R - \varepsilon) N \cdot H_q^{-1}(\frac{1}{2} - \varepsilon) n$

$\Rightarrow \delta \geq (1 - R - \varepsilon) H_q^{-1}(\frac{1}{2} - \varepsilon)$.

$$|S_g| = |S| - |S_b| \geq |S| - \varepsilon N \geq (1-R-\varepsilon)N$$

$|S_b| \leq \varepsilon N$

$S_b \subseteq \underbrace{\{ j \in [N] \mid \delta(C_{in}^j) < H_q^{-1}(\tfrac{1}{2}-\varepsilon) \}}_{\text{this set has size } \leq \varepsilon N \text{ (by Wozencraft ensemble)}}$

Wozencraft ensemble: $N = q^k - 1$ $\quad R(C_{in}^j) = \frac{1}{2}$ $\quad \geq (1-\varepsilon)N$ values of j $\quad \delta(C_{in}^j) \geq H_q^{-1}(\tfrac{1}{2}-\varepsilon)$

Re-index the codes by $\alpha \in \mathbb{F}_{q^k}^*$

$$C_{in}^{\alpha} : \mathbb{F}_q^k \to \mathbb{F}_q^{2k} \quad (\Rightarrow R(C_{in}^j) = \tfrac{1}{2})$$

$$\underset{\uparrow\, \mathbb{F}_q^k}{C_{in}^{\alpha}(X)} = (X, \underbrace{\alpha \cdot X}_{\mathbb{F}_q^k})$$

over $\mathbb{F}_{q^k}$; $\mathbb{F}_{q^k}$

} linear code (strongly) explicit

Pf (for $\geq (1-\varepsilon)N$ frac of αs $\quad \delta(C_{in}^{\alpha}) \geq H_q^{-1}(\tfrac{1}{2}-\varepsilon)$)

Goal: Most αs C_{in}^{α} doesn't have any non-zero codewords of wt $< H_q^{-1}(\tfrac{1}{2}-\varepsilon) \cdot \underbrace{n}_{2k}$

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

Claim: $(\bar{y}_1, \bar{y}_2) \in \mathbb{F}_{q^k}^{2k} \setminus \{\bar{0}\}$ is in atmost one C_{in}^{α}.

Pf: $(\bar{y}_1, \bar{y}_2) \in C_{in}^{\alpha} \xrightarrow[\text{by defn}]{} \bar{y}_2 = \alpha \cdot \bar{y}_1$

Case 1: $\bar{y}_1 \neq 0, \bar{y}_2 \neq 0 \Rightarrow \alpha = \frac{\bar{y}_2}{\bar{y}_1} \neq 0$

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

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!)

$$\left|\{\alpha \mid \delta(G_{in}^{\alpha}) < H_q^{-1}(\tfrac{1}{2}-\varepsilon)\}\right|$$

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

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

$$\leq q^{H_q(H_q^{-1}(1/2-\varepsilon))\cdot 2k}$$

$$= q^{(\frac{1}{2}-\varepsilon)2k}$$

$$= q^{k-2\varepsilon k} = \frac{q^k}{q^{2\varepsilon k}} < \varepsilon(q^k-1)$$

$$= \varepsilon N \quad \blacksquare$$