| Apr 17 | 1 min checkin

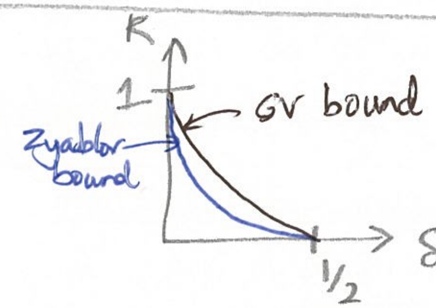
REMINDERS

(•) HW 6 due by 11:59pm on Wed

(•) Video due by 11:59pm on Sun, May 14 (< 4 weeks)

RECAP

(•) Explicit codes on Zyablov bound

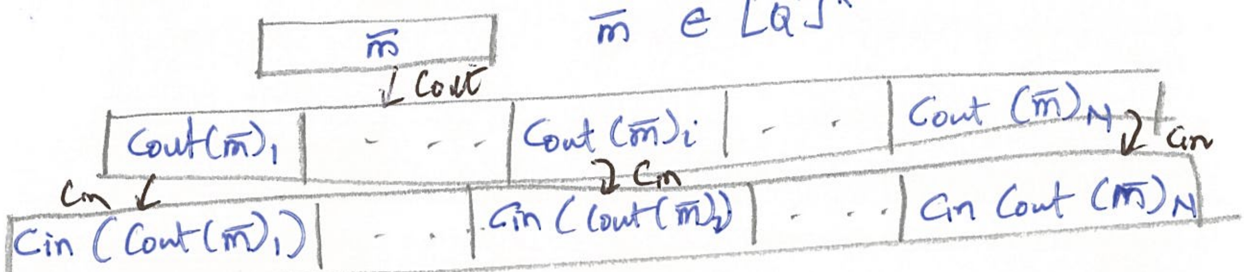


(•) Code concatenation:

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

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

$\bar{m} \in [Q]^K$



$C_{out} \circ C_{in} : [q]^{kK} \to [q]^{nN}$

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

Plan for today (•) Strongly explicit asymptotically good codes (•) Justesen codes

(•) (If there is time) Decoding of concatenated codes

Strongly explicit linear code: $G \in \mathbb{F}_q^{k \times n}$, $i \in [k]$, $j \in [n]$
Output $G[i,j]$ in poly-log(n) time

Justesen code: Use different linear codes

$C_{in}^1, \ldots, C_{in}^N : [q]^k \to [q]^n$

$C_{out} \circ (C_{in}^1, \ldots, C_{in}^N) = (C_{in}^1(C_{out}(\bar{m})_1), \ldots, C_{in}^i(C_{out}(\bar{m})_i), \ldots, C_{in}^N(C_{out}(\bar{m})_N))$

Note: If all C_{in}^i had rate r, C_{out} has $R \Rightarrow$ overall Rr

Wozencraft ~~Wozencraft~~ ensemble: Let $\varepsilon > 0$ be small enough. $\exists$ strongly explicit ensemble of linear code $C_{in}^1, \ldots, C_{in}^N$ s.t.

$r(C_{in}^i) = \frac{1}{2} \; \forall i \in [N]$, $\delta(C_{in}^i) \geq H_q^{-1}\left(\frac{1}{2} - \varepsilon\right)$
for at least $(1-\varepsilon)N$ values of $i \in [N]$

Justesen codes $\quad C_{out}$: (RS) of rate R. $\quad N = q^k - 1$

$\mathbb{F}_Q \quad Q = q^k$ $\quad$ eval pnt $\mathbb{F}_Q^* \overset{def}{=} \mathbb{F}_Q \setminus \{0\}$

$$C^* = C_{out} \circ \underbrace{(C_{in}^1, \ldots, C_{in}^N)}_{\text{Wozencraft ensemble}}$$

Claim1. Justesen codes are asymptotically good + strongly explicit

Pf: $R = R \cdot \frac{1}{2} = \frac{R}{2} > 0$ for $R > 0$

Pf: fix $\overline{m_1} \neq \overline{m_2} \in (\mathbb{F}_{q^k})^K$

$S = \{ j \mid C_{out}(\overline{m_1})_j \neq C_{out}(\overline{m_2})_j \} \Rightarrow |S| \geq (1-R)N$

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

Claim 2: $|S_g| \geq (1-R-\varepsilon)N$ $\quad \left\{ |S_b| \leq \right.$ $j \in [N]$ s.t. $\delta(C_{in}^j) < H_q^{-1}(\frac{1}{2} - \varepsilon)$

$\leq \varepsilon N$ ← by defn of Wozencraft ensemble

$|S_g| = |S| - |S_b|$

$\geq (1-R)N - \varepsilon N = (1-R-\varepsilon)N.$

$$\Rightarrow \frac{\Delta(C^*(\overline{m_1}), C^*(\overline{m_2}))}{2N} \geq \frac{|S_g|}{N} \cdot \frac{H_q^{-1}(\frac{1}{2}-\varepsilon)\cancel{N}}{\cancel{N}}$$

$$\geq (1-R-\varepsilon) \cdot H_q^{-1}(\tfrac{1}{2} - \varepsilon) > 0 \quad \blacksquare$$

Wozencraft ensemble:

$N = q^k - 1 \quad C_{in}^1, \ldots, C_{in}^N \quad r(C_{in}^i) = \frac{1}{2} \quad \forall i \in [N]$

$\geq (1-\varepsilon)N$ values of $j \in [N]$, $\delta(C_{in}^j) \geq H_q^{-1}(\frac{1}{2} - \varepsilon)$

Re-index codes by $\alpha \in \mathbb{F}_{q^k}^*$ ($\overset{def}{=} \mathbb{F}_{q^k} \setminus \{0\}$) ← # of such $\alpha = q^k - 1 = N$

$C_{in}^\alpha : \mathbb{F}_q^k \to \mathbb{F}_q^{2k} \rightsquigarrow r(C_{in}^\alpha) = \frac{1}{2} \quad \forall i$

(assume $\alpha \geq 1$)

$$\underset{\in \mathbb{F}_q^k}{C_{in}^\alpha(\overline{X})} \to (\overline{X}, \alpha \cdot \overline{X})$$

$\alpha \in \mathbb{F}_{q^k}$, $\overline{X} \in \mathbb{F}_{q^k}$, $\alpha \cdot \overline{X} \in \mathbb{F}_{q^k}$

$\alpha \cdot X \in \mathbb{F}_q^k$

$\mathbb{F}_q^k \equiv \mathbb{F}_{q^k}$ ← linear

$\exists$ bijection $\Rightarrow C_{in}^\alpha$ linear

Pf: Show $\geq \underline{(1-\varepsilon)N}$ values $\alpha \in \mathbb{F}_{q^k}^*$, $\delta(C_{in}^{\alpha}) \geq H_q^{-1}(\frac{1}{2}-\varepsilon)$

Goal: for most values of α, C_{in}^{α} lies on the GV bound

~~Claim3~~: fix $\underbrace{\bar{y} = (\bar{y}_1, \bar{y}_2) \in (\mathbb{F}_q^k)^2 \setminus \{(\bar{0}, \bar{0})\}}$ $\Rightarrow \times$ $\bar{y}_1 = \bar{0} \wedge \bar{y}_2 = \bar{0}$

Claim3: Every is in at most one C_{in}^{α}

By case analysis

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

Case 1: $(\bar{y}_1 \neq \bar{0}, \bar{y}_2 \neq \bar{0})$ $\quad \hookrightarrow \alpha = \frac{\bar{y}_2}{\bar{y}_1} \Rightarrow \alpha \neq 0$ & unique.

Case 2: $(\bar{y}_1 \neq \bar{0}, \bar{y}_2 = \bar{0})$ $\quad \Rightarrow \alpha = \frac{\bar{y}_2}{\bar{y}_1} = 0$ (by $\alpha \neq 0$) $\times$

Case 3: $(\bar{y}_1 = \bar{0}, \bar{y}_2 \neq \bar{0})$ $\quad \Rightarrow \bar{y}_2 = \alpha \cdot \bar{y}_1 = \alpha \cdot 0 = \bar{0}$ (but $\bar{y}_2 \neq \bar{0}$) $\times$ $\blacksquare$

$$\left|\{\alpha \in \mathbb{F}_{q^k}^* \mid \delta(C_{in}^{\alpha}) < H_q^{-1}(\tfrac{1}{2}-\varepsilon)\}\right|$$

if $\exists\, \bar{y} \neq \bar{0}$ s.t. $wt(\bar{y}) < H_q^{-1}(\frac{1}{2}-\varepsilon) \cdot 2k$ & $\bar{y} \in C_{in}^{\alpha}$

by Claim3

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

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

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

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

for large enough k