Apr 8

REMINDERS

(•) HW 5 due by 11:59 pm Wed

(•) Video due in ~ 5 weeks (last Wed of sem)

↳ Y'all will get atleast 4 weeks b/w feedback on report + video due date

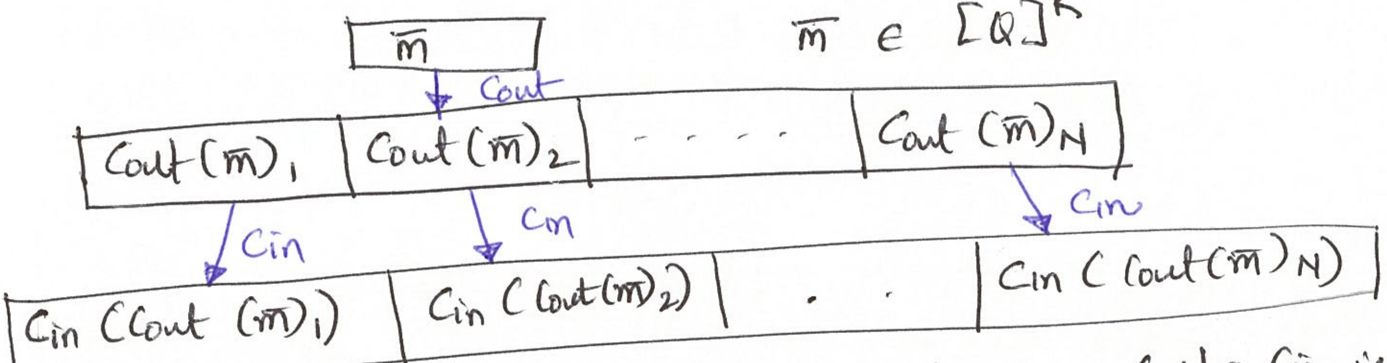
RECAP

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

(→) Code concatenation

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

$C_{in}: \underbrace{[q]^k}_{\equiv [Q]} \to [q]^n \qquad C_{out} \circ C_{in}(\bar{m}) = (C_{in}(C_{out}(\bar{m})_1), \ldots C_{in}(C_{out}(\bar{m})_N))$



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

THM: If C_{out} is an $(N, K, D)_{Q=q^k}$ code $\Rightarrow$ $C_{out} \circ C_{in}$ is $(Nn, Kk, Dd)_q$ code

+ C_{in} ——— $(n, k, d)_q$ ———

Ex: Linearity is preserved

TODAY

(•) Proof readers: Madhukar, Rick

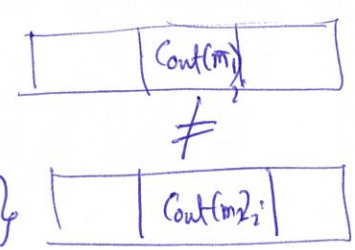
(•) Pf of THM above

(•) Zyablov bound ($\Rightarrow \exists$ explicit asymp. good codes)

(•) Justesen codes ($\Rightarrow \exists$ strongly explicit ———)

↳ Pf: By defn: $C_{out} \circ C_{in} \quad [q^k]^K \to [q^n]^N$

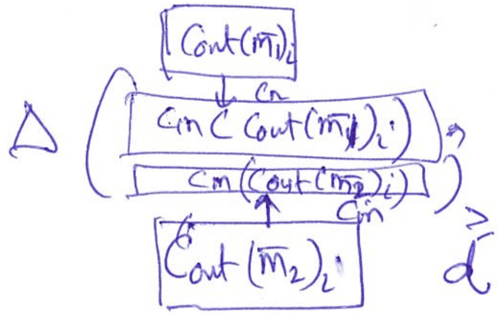
$= [q]^{kK} \to [q]^{nN}$



Fix $\bar{m}_1 \neq \bar{m}_2 \in [q]^{kK} \equiv [Q]^K$

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

Pf $i \in S$, $\Delta\big(C_{in}(C_{out}(\overline{m}_1)_i),$
$C_{in}(C_{out}(\overline{m}_2)_i)\big) \geq d$



$\Rightarrow$ overall dist $\geq |S| \cdot d$
$\geq D \cdot d$ ∎

Zyablov bound

C_{out}: Singleton bound CRS codes of rate R, $\delta_{out} \geq 1-R$)

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

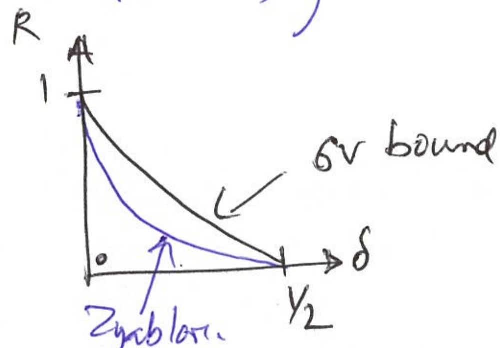
$C_{out} \circ C_{in}$: $\mathcal{R} = R \cdot r$, rel dist $\geq \delta_{out} \cdot \delta_{in}$

s.t. $H_q^{-1}(1-r-\varepsilon) > \delta$ $\qquad \delta \geq (1-R)\, H_q^{-1}(1-r-\varepsilon)$

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

$\Rightarrow$ overall rate $\displaystyle \mathcal{R} \geq \max_{0 < r < 1 - H_q(\delta) - \varepsilon} r\left(1 - \frac{\delta}{H_q^{-1}(1-r-\varepsilon)}\right)$

Comparison pt: $\delta = \frac{1}{2} - \varepsilon$, $R_{GV} \geq \Omega(\varepsilon^2)$
$R_Z \geq \Omega(\varepsilon^3)$



Q: How do we get explicit codes on Zyablov bound.

Ex: C_{out} & C_{in} can be constructed in poly(N) time $\Rightarrow$ $C_{out} \circ C_{in}$ is explicit.

$Q = q^k$

$\mathcal{N} = Nn$

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

Assume $r > 0$, $n = O(k) \Rightarrow n = O(\log_q N)$

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

$\Rightarrow$ By HW 4, can construct C_{in} in time $q^{O(n)} = \text{poly}(N)$

$\Rightarrow$ Can construct codes on Zyablov bound in poly$(\mathcal{N})$ time.
$\Rightarrow$ explicit asymptotically good codes!

Q: Strongly explicit asymptotically good ~~code~~ linear code?
$\underbrace{\text{Strongly explicit}}$ each entry of G can be computed in poly(log n) time.

Justesen codes

Idea: Use different inner codes: $C_{in}^1, C_{in}^2, \ldots, C_{in}^N$

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

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

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

$N = q^k - 1$

Wozencraft ensemble: Let $\varepsilon > 0$ be small enough. $\exists$ strongly explicit linear $C_{in}^1, \ldots, C_{in}^N$ s.t. $r(C_{in}^i) = \frac{1}{2}$ $\forall i \in [N]$
for at least $(1-\varepsilon)N$ values of $j \in [N]$ $\delta(C_{in}^j) \geq H_q^{-1}(\frac{1}{2} - \varepsilon)$

Justesen code: C_{out} (RS) rate R $\quad N = q^k - 1$ eval pts
$\delta_{out} = 1 - R$

$\mathbb{F}_q^* \overset{def}{=} \mathbb{F}_q \setminus \{0\}$

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

$R(C^*) = R \cdot \frac{1}{2} = \frac{R}{2}$

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

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

$S = \{ j \mid C_{out}(\bar{m}_1)_j \neq C_{out}(\bar{m}_2)_j \}$

Note: $|S| \geq (1-R)N$

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

Claim: $|S_g| \geq (1 - R - \varepsilon)N$

$\dfrac{\Delta(C^*(\bar{m}_1), C^*(\bar{m}_2))}{Nn} \geq \dfrac{|S_g|}{N} \cdot H_q^{-1}(\frac{1}{2} - \varepsilon) \geq (1 - R - \varepsilon) \cdot H_q^{-1}(\frac{1}{2} - \varepsilon)$.