| Apr 13 | 1 min checkin

REMINDER

(•) HW 6 due by 11:59pm on Wed

RECAP

(•) (strongly) explicit asymptotically good code $(R>0, \delta>0)$?

	Hamming	Hadamard	RS over $\mathbb{F}_{2^s}$ + bin rep $s=\lceil \log n \rceil$
R	$1-O\left(\frac{\log n}{n}\right)$	$O\left(\frac{\log n}{n}\right)$	$\frac{1}{2}$
δ	$\Theta\left(\frac{1}{n}\right)$	$\frac{1}{2}$	$\Theta\left(\frac{1}{\log n}\right)$

Plan for today (•) Code concatenation (•) Zyablov bound (explicit) (•) Justesen codes (strongly explicit)

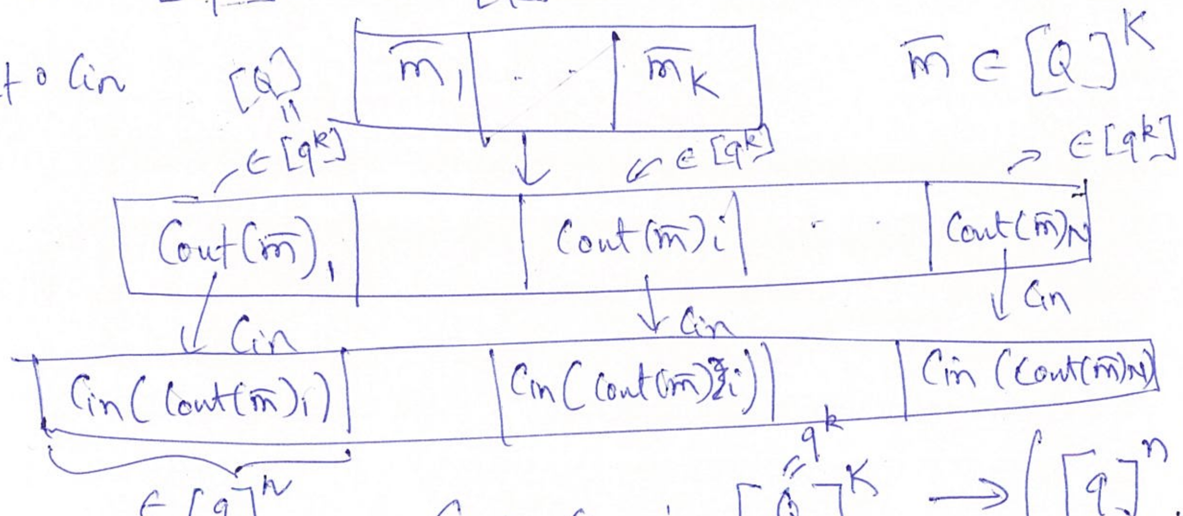
Code concatenation ← terrible name

(composition)

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

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

$C_{out} \circ C_{in}$



$C_{out} \circ C_{in}: [\underset{=q^k}{Q}]^K \longrightarrow \left([q]^n\right)^N$

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

THM: If C_{out} is $(N, K, D)_{q^k}$ code & C_{in} is $(n, k, d)_q$ code

$\Rightarrow C_{out} \circ C_{in}$ $(Nn, Kk, \geq Dd)_q$

Ex: linearity is preserved

$\Rightarrow C_{out}$: rate $\underset{K}{R}$, $\underset{D}{\delta_{out}}$, C_{in}: rate $\underset{\frac{k}{n}}{r}$, rel-dist $\underset{\frac{d}{n}}{\delta_{in}}$ $\Rightarrow C_{out} \circ C_{in}$ rate $R = Rr = \frac{Kk}{Nn}$

$\delta = \delta_{out} \cdot \delta_{in} = Dd$

IF $\quad R>0,\ \delta_{out}>0 \qquad \Rightarrow \mathcal{R}>0,\ \delta>0$

$\quad r>0,\ \delta_{in}>0$

Goal: Get hold of asymptotically good C_{out} & C_{in}

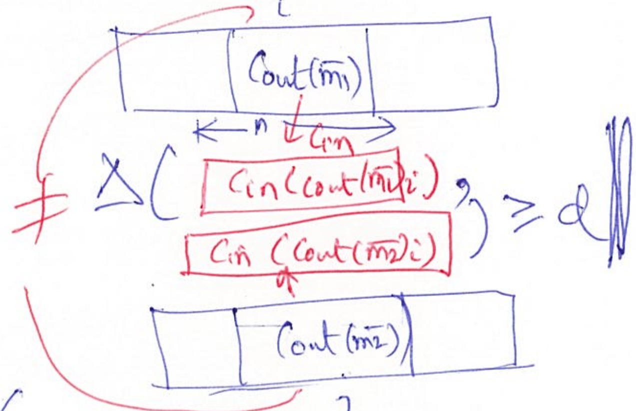
$\text{RS} \to C_{out}$ $\qquad C_{in} \leftarrow$ recursive?

Pf of THM: Claim on block length, dimension & alphabet size of $C_{out} \circ C_{in}$ is by defn ✓

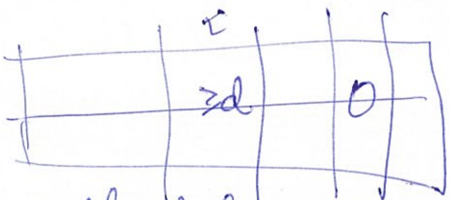
Fix $\overline{m_1} \neq \overline{m_2} \in [q]^{kK} \equiv [Q]^K$

$S = \{ i \in [N] \mid C_{out}(\overline{m_1})_i \neq C_{out}(\overline{m_2})_i \}$

$|S| \geq D$



If $i \in S \Rightarrow \Delta(C_{in}(C_{out}(m_1)_i), C_{in}(C_{out}(\overline{m_2})_i)) \overset{?}{\geq} d.$



$\Rightarrow$ overall dist $\geq |S| d = Dd$ ∎

$\mathcal{R} = Rr \quad , \quad \delta \geq \delta_{out} \cdot \delta_{in}$

Zyablov $\quad C_{out}$: Singleton bound (RS code of rate R, $\delta_{out} \geq 1 - R$)

C_{in}: (linear) code on GV bound, rate r, rel. dist δ_{in} $\quad \Rightarrow r \geq 1 - H_q(\delta_{in}) - \varepsilon$

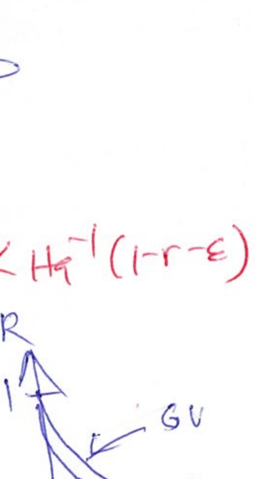
$\Rightarrow \delta_{in} \geq$ ~~$1 - H_q(r) - \varepsilon$~~ $H_q^{-1}(1 - r - \varepsilon)$

$C_{out} \circ C_{in}$: $\mathcal{R} = Rr$

$\delta \geq \delta_{out} \cdot \delta_{in} \geq (1-R)\, H_q^{-1}(1 - r - \varepsilon)$

δ is given. $\quad \Rightarrow R \geq 1 - \dfrac{\delta}{H_q^{-1}(1 - r - \varepsilon)}$ $\qquad \delta < H_q^{-1}(1 - r - \varepsilon)$

Overall rate $\mathcal{R} = Rr \geq \max_r r \left(1 - \dfrac{\delta}{H_q^{-1}(1 - r - \varepsilon)} \right)$



$R_{Zyablov} = \max_{0 < r < 1 - H_q(\varepsilon) - \varepsilon} r \left(1 - \dfrac{\delta}{H_q^{-1}(1 - r - \varepsilon)} \right)$

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

Q: How do we get an explicit code on the Zyablov bound?

(Ex:) If gen matrix of Cout & Cin can be constructed in poly (N) time ⇒ can compute gen matrix of Cout ∘ Cin in poly time

RS ✓ ?

Cout: RS : $N = q^k \Rightarrow k = \log_q N$

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

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

$a \cdot \log_b c = \log_b c^a$

Q: Can we get an $(n,k,d)_q$ code on the GV bound in $q^{O(n)}$ time?

A: By HW 4, yes! ⇒ can construct linear on the Zyablov bound in poly (N) time!

poly (N)

" Nn

$O(N \log_q N)$

Q: Strongly explicit asymptotically good linear codes.