| Apr 19 |

1 min checkin

REMINDERS

(•) HW6 due by 11:59pm tonight
(•) Project video due in ~3.5 weeks (Sun, May 14)

RECAP

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

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

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

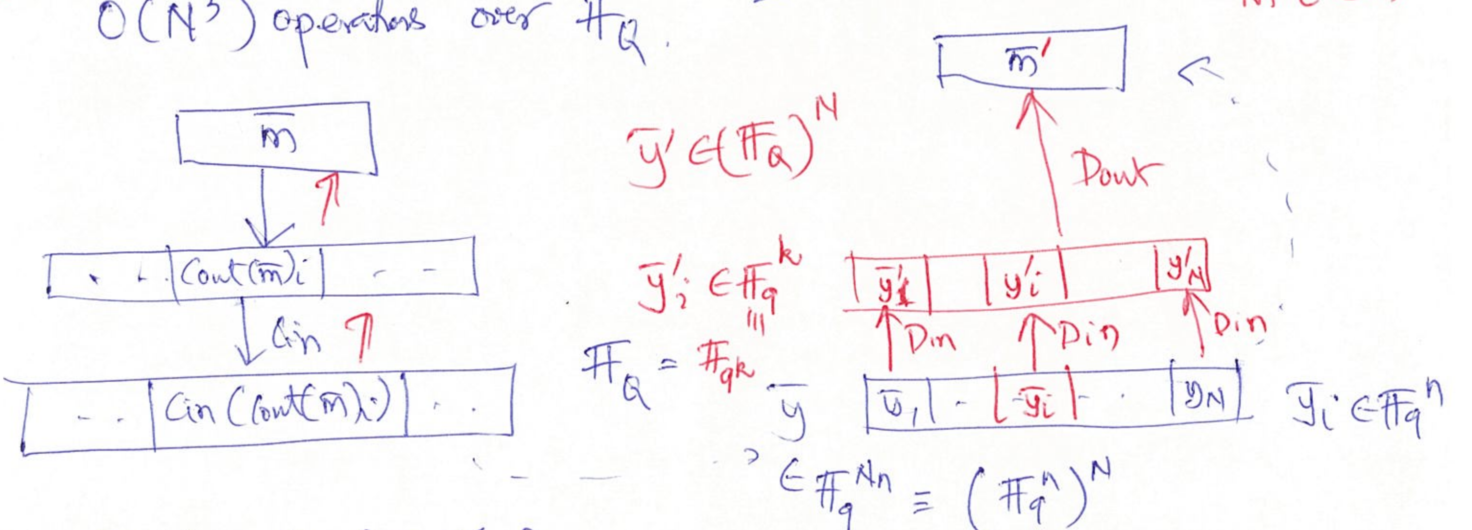
(•) Via concatenated codes:
(i) Explicit codes on Zyablov bound
(ii) Strongly explicit Justesen codes

Plan for today (•) Decoding concatenated codes
(•) Achieving BSC$_p$ capacity with explicit codes (+ efficient encoding + decoding)

Decoding concatenated codes

Assume: (i) C_{out} is $[N, K, N-K+1]_Q$ RS code $\quad \underline{N} = Q = \underline{q^k}$

(ii) $\exists$ a unique decoder for $< \frac{1-R}{2}$ frac of errors in $O(N^3)$ operations over $\mathbb{F}_Q$. D_{out}



(iii) $D_{in} \to$ unique decoder of C_{in}
$\hookrightarrow$ can correct upto $< \frac{d}{2}$ ← dist of C_{in}
$\hookrightarrow$ $MLD_{C_{in}} \to q^{O(k)} = poly(N) = poly(\mathcal{N})$
$\mathcal{N} = Nn$

Algo 1: input = $\bar{y} = (\bar{y}_1, \dots, \bar{y}_N) \in (\mathbb{F}_q^n)^N$

1. $\bar{y}' \leftarrow (\bar{y}'_1, \dots, \bar{y}'_N)$ where $\bar{y}'_i = \in D_{in}(\bar{y}_i)$

poly(N).

2. $\bar{m}' \leftarrow D_{out}(\bar{y}')$
3. return $\bar{m}'$

$O(N^3)$ over $\tilde{O}(N^3) + N \cdot \mathrm{poly}(N) = \mathrm{poly}(N)$

$N \cdot \mathrm{poly}(N)$

C_{out} has dist $D > 1$

C_{in} ——— $d > 1$

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

Pf: $\bar{y}$ is s.t. $\exists\, \bar{m} \in (\mathbb{F}_{q^k})^K$ s.t. $\bar{m}$ is unique

$$\Delta(\bar{y}, C_{out} \circ C_{in}(\bar{m})) < \frac{Dd}{4} \qquad (*)$$

Goal: On input $\bar{y}$, Algo 1 outputs $\bar{m}$.

Def: A bad event occurs at $i \in [N]$ if $C_{in}(\bar{y}'_i) \neq C_{in}(C_{out}(\bar{m})_i) \equiv \bar{y}'_i \neq C_{out}(\bar{m})_i$

Claim 1: If # bad events $< \frac{D}{2} \Rightarrow$ Algo 1 is correct

Pf: $\Delta(\bar{y}', C_{out}(\bar{m})) < \frac{D}{2} \Rightarrow$ By assumption on D_{out} correcting $< \frac{D}{2}$ errors $\Rightarrow$ Algo 1 outputs $\bar{m}$.

Claim 2: # bad events $< \frac{D}{2}$

Claims 1+2 $\Rightarrow$ Lemma 1.

Pf: By contradiction $\rightarrow$ assume # bad events $\geq \frac{D}{2}$

Claim 3: Bad event at $i \in [N] \Rightarrow \Delta(\bar{y}_i, C_{in}(C_{out}(\bar{m})_i)) \geq \frac{d}{2}$

{ If not, $\Delta(\bar{y}_i, C_{in}(C_{out}(\bar{m})_i)) < \frac{d}{2}$ $\Rightarrow D_{in}$ should output $C_{out}(\bar{m})_i$ }

$\Rightarrow \Delta(\bar{y}, C_{out} \circ C_{in}(\bar{m})) \geq (\text{\# bad events}) \cdot \frac{d}{2} \geq \frac{D}{2} \cdot \frac{d}{2} = \frac{Dd}{4}$

$\Rightarrow$ contradicts (*) ∎

<u>Lemma 1:</u> $\Rightarrow$ decode codes on Zyablov bound (from Mon)
can decode in poly time $\frac{1}{4}$ · Zyablov bound

<u>Q:</u> Can we get $\frac{1}{2}$ · Zyablov bound? Ex Yes (Chap 13.2 + 13.3 in book)

Achieving BSC_p capacity w/ explicit codes + efficient decoding (+encoding)

$\rightarrow$ via code concatenation

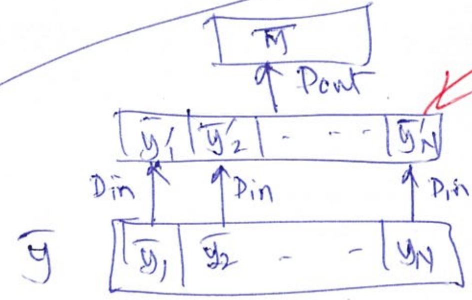
C_{out} ? RS codes (correct from some const. frac. of errors)

C_{in} ? BSC_p capacity achieving codes?

<u>Fact:</u> $\exists$ linear code of rate $1-H(p)-\varepsilon$ w/ dec. error prob $2^{-\Omega(\varepsilon^2 n)}$

$C^* = C_{out} \circ C_{in}$

Dec. ~~alg~~ algo: Algo 1



$\bar{y}'$ has $< \gamma$ frac of errors with high prob

$\uparrow$ Chernoff

each D_{in} has dec. error prob $\leq \frac{\gamma}{2}$

$\uparrow$ independent for each $i = 1..N$

$\rightarrow$ ~~If~~ D_{out} can handle $< \gamma$ frac of <u>worst case</u> errors. ✓