ANNOUNCEMENTS

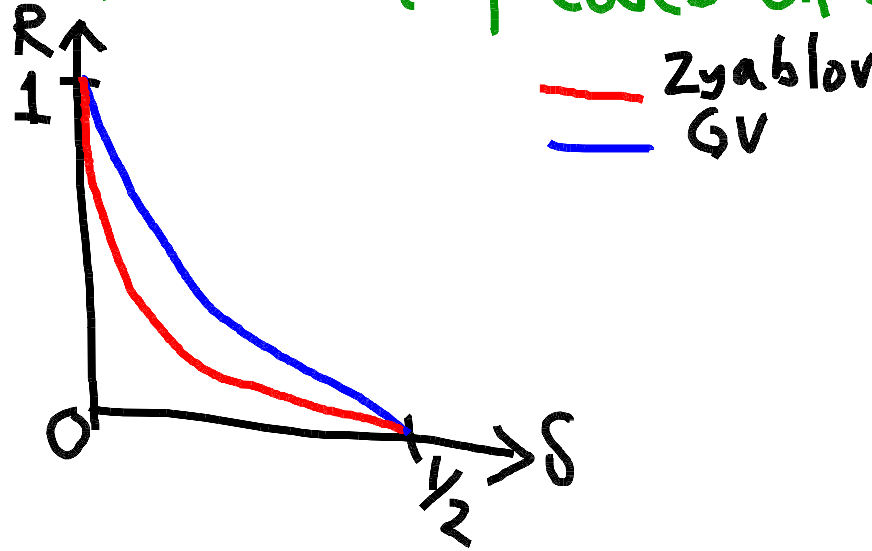
(I) Wikipedia report due by midnight

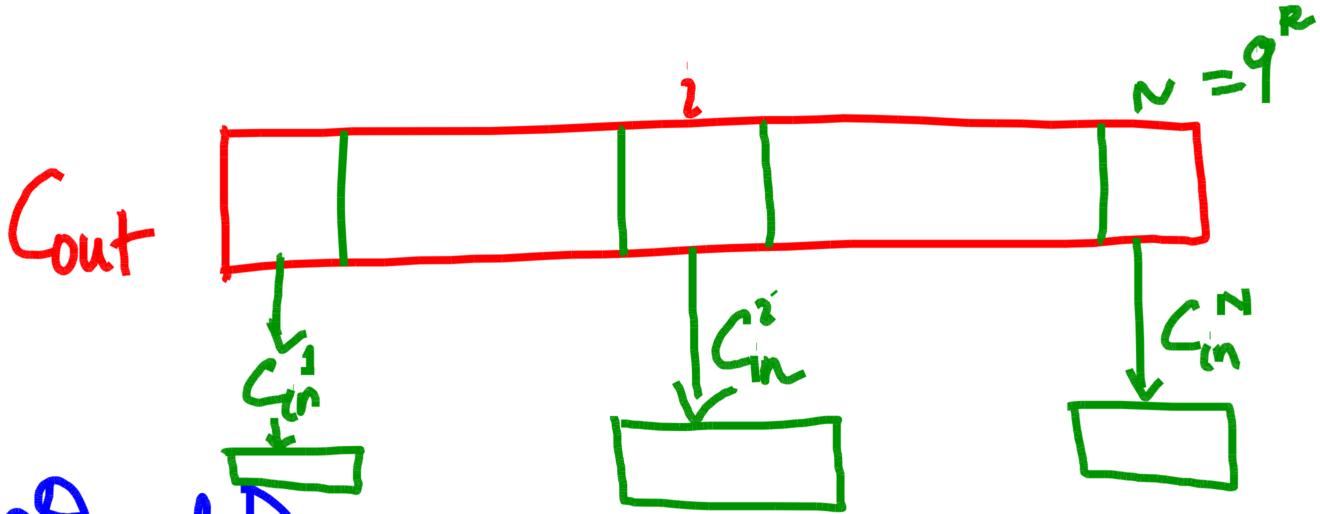
↳ I'll give back comments by end of the week

(II) Some 2nd versions of scribed notes are due.

RECAP

→ Polytime construction of codes on Zyablov bound





$\forall i,$
$dist(C_{in}^i) \geq d$
$rate(C_{in}^i) = r$

$\mathcal{D} = dD$

$\mathcal{R} = rR$

Idea: Would be OK if <u>most</u> of C_{in}^i had good distance

Q: Have you seen an ensemble of codes most of which lie on the GV bound?

↳ # linear codes $= q^{kn}$ [$> q^k$ of them don't lie on GV]

THM: $\exists$ a strongly explicit ensemble of inner codes $C_{in}^1, \dots, C_{in}^N$ (each of rate $\frac{1}{2}$) s.t. $\geq (1-\varepsilon)N$ of them have rel distance $\geq H_q^{-1}(\frac{1}{2}-\varepsilon)$, $\varepsilon > 0$. (Wozencraft ensemble)

$N = q^k - 1$

→ Pick outer code to be RS, $N = q^{k}-1$, rate R

→ Inner codes as above

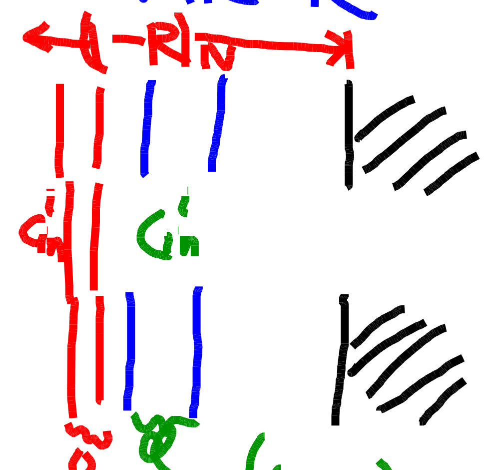
→ final code has rate $R/2$

→ rel dist $\geq (1-R-\varepsilon)\, H_q^{-1}(\frac{1}{2}-\varepsilon)$

$C_{in}^i \to$ good if it lies on the ov

$C_{in}^i \to$ bad otherwise (0 contrib to distance)

$d = H_q^{-1}(\frac{1}{2}-\varepsilon)\cdot n$



$\Delta \geq ((1-R)N - \varepsilon N)\, d$

$N = q^k - 1$ codes

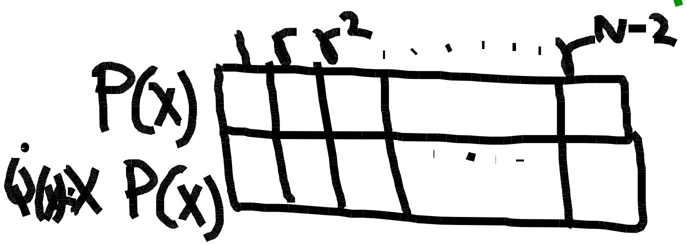
Wozencraft ensemble

$\forall \alpha \in \mathbb{F}_{q^k}^*$ $\quad C_{in}^{\alpha} : \mathbb{F}_q^k \to \mathbb{F}_q^{2k}$

$\forall x \in \mathbb{F}_q^k \cong \mathbb{F}_{q^k}$ $\quad$ Linear

$C_{in}^{\alpha}(x) = (x, \alpha x)$

→ Let $\varepsilon > 0$. For large enough k, for $\geq (1-\varepsilon)N$ values of α, C_{in}^{α} has rel dist $\geq H_q^{-1}(1/2 - \varepsilon)$



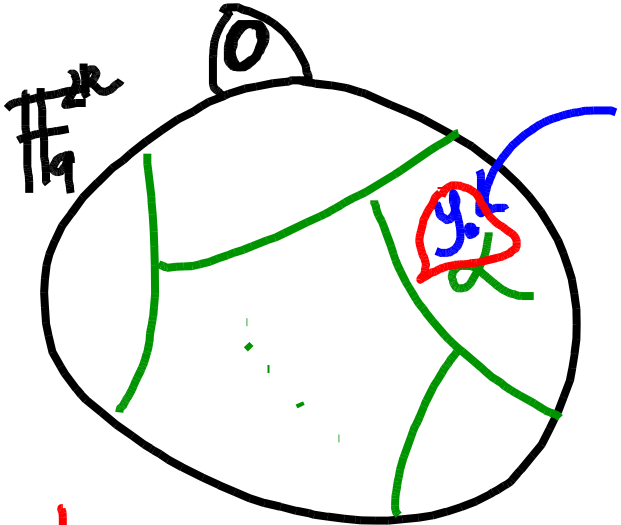
Code over $\mathbb{F}_{q^k}^2$ or over $\mathbb{F}_q$

→ Fix $y \in \mathbb{F}_{q^k}^2 \setminus \{0\}$ $\quad$ Claim: $\exists \leq 1$ α s.t. $y \in C_{in}^{\alpha}$

→ Case 1: $y_1, y_2 \neq 0$, $\alpha = \frac{y_2}{y_1}$

→ Case 2: $y_1 = 0, y_2 \neq 0$, not possible (as $y_1 \alpha = 0$)

→ Case 3: $y_1 \neq 0, y_2 = 0$, not possible



$wt(y) < d \overset{def}{=} H_q^{-1}\left(\frac{1}{2}-\varepsilon\right)\cdot 2k$

$\Rightarrow C_{in}^{\alpha}$ is bad

bad codes =

$\left|\{\alpha \mid \exists y \in \mathbb{F}_q^{2k}\setminus\{0\},\ wt(y)<d\}\right|$

$\le \left|\{y \mid y \in \mathbb{F}_q^{2k}\setminus\{0\},\ wt(y)<d\}\right|$

$< Vol(q,d) \le q^{2k\left(H_q\left(H_q^{-1}\left(1/2-\varepsilon\right)\right)\right)}$

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

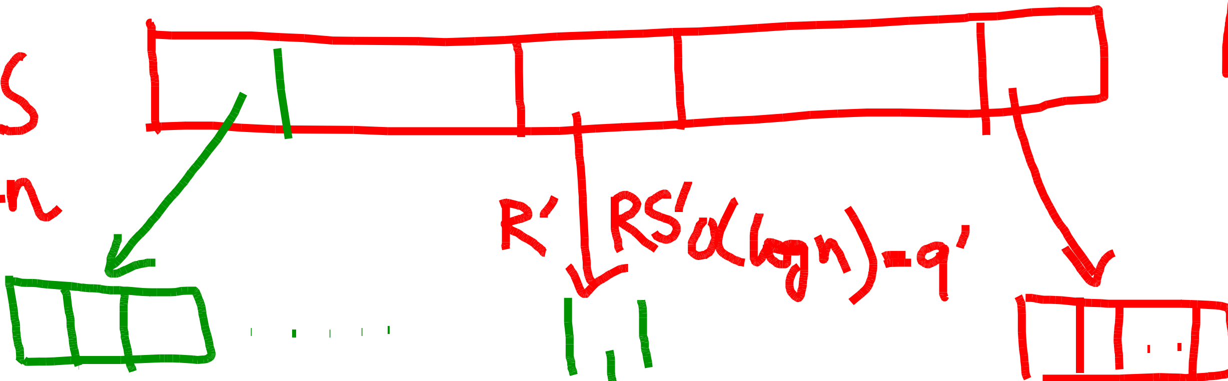
$\uparrow$ large enough k. ∎

[Justesen '72]

Zuckerman's construction

RS

$2^{\log n} = q = n$



$N = n \log n$

$\frac{\log\log n}{R' \cdot r}$

Use all possible linear codes

$C_{in}^{?}$

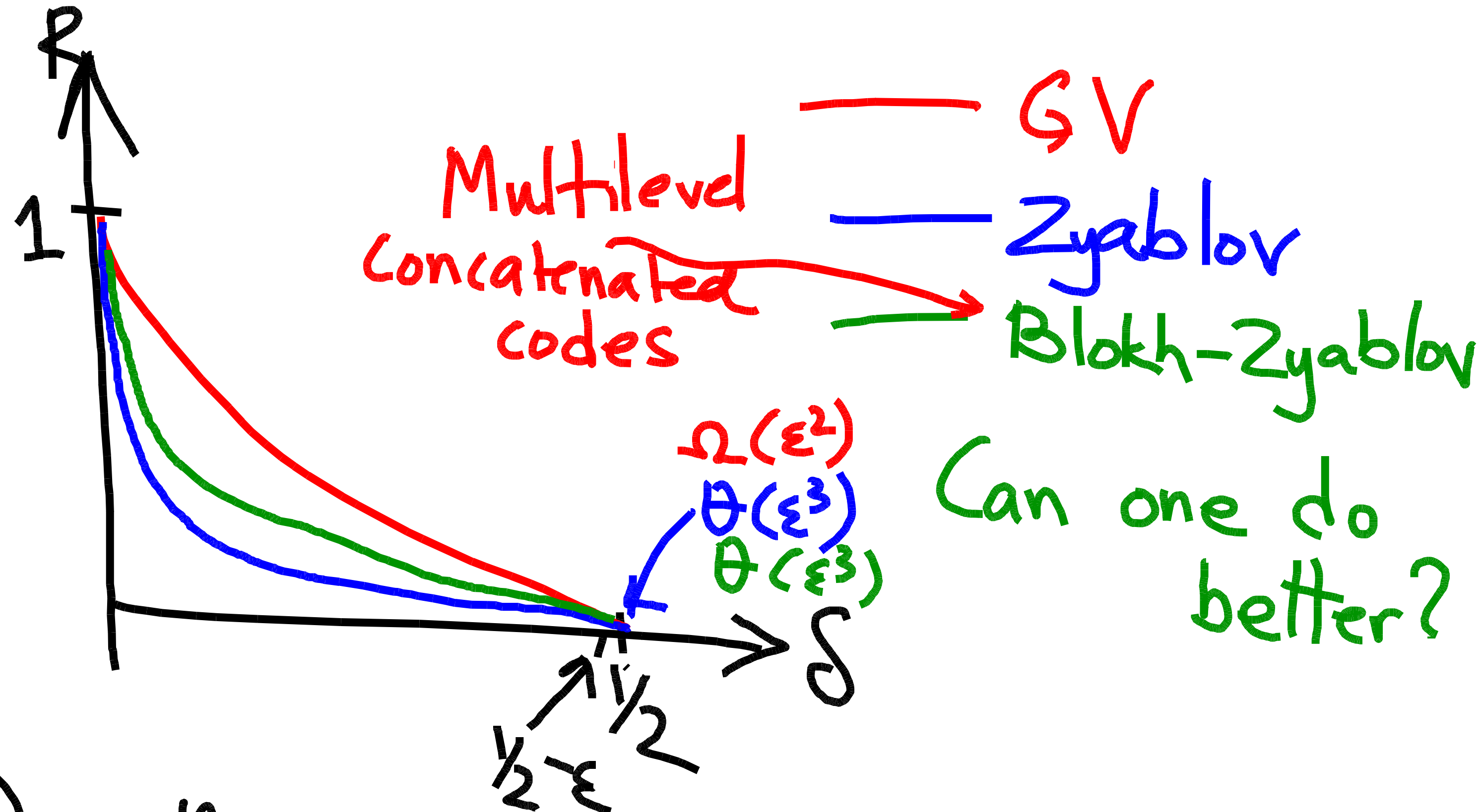
$C_{in}^{?} : \{0,1\}^{k = O(\log\log n)} \longrightarrow \{0,1\}^{\frac{k}{r}}$

$\#$ linear codes $= 2^{\frac{O(\log \log^2 n)}{r}} << n$

most of inner codes lie on the GV bound.

Ex: Figure out rel. dist.

Q: Best R vs δ (w/ explicit codes)



Can one do better?

Q: Does there ∃ a concatenated that lies on the GV bound?

A: Yes [Thommesen]

Outer → RS, inner → independent random

→ Concatenated codes have distance $\geq \underline{dD}$

design distance

→ Design distance $\leq$ Zyablov bound

→ Explicit constructions

↳ Poly time encoding ✓

Q: Decoding? (Poly time) (unique) Can we decode up to $\frac{dD}{2}$ errors?