Today

- Code Concatenation
- Zyablov's Bound
- Justesen Codes

CS5.318.1
Coding Theory
Lecture (2022-9-28)
Instructor: Prahladh Harsha.

Where we are:

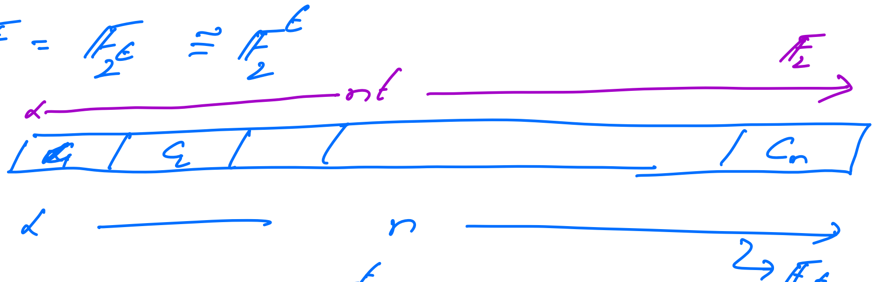
Reed-Solomon codes $[n, k, n-k+1]_q$ - code
& $q \geq n$
(drawback of RS codes)

$\mathbb{F} = \mathbb{F}_{2^t}$; $S = \mathbb{F}$, (ie, $n = q = 2^t$)

$k = n/2$

For this setting of parameters
RS-code $\left[n, \frac{n}{2}, \frac{n}{2}\right]_{2^t}$-code $n = 2^t$.

$\mathbb{F} = \mathbb{F}_{2^t} \cong \mathbb{F}_2^t$



$c_i \in \mathbb{F}_{2^t} \cong \mathbb{F}_2^t$

Just write out each elt of $\mathbb{F}_{2^t}$ in its row encoding (ie, a bit string of length t)

$[nt, \frac{nt}{2}, \frac{n}{2}]_2$-code for $t = \log n$

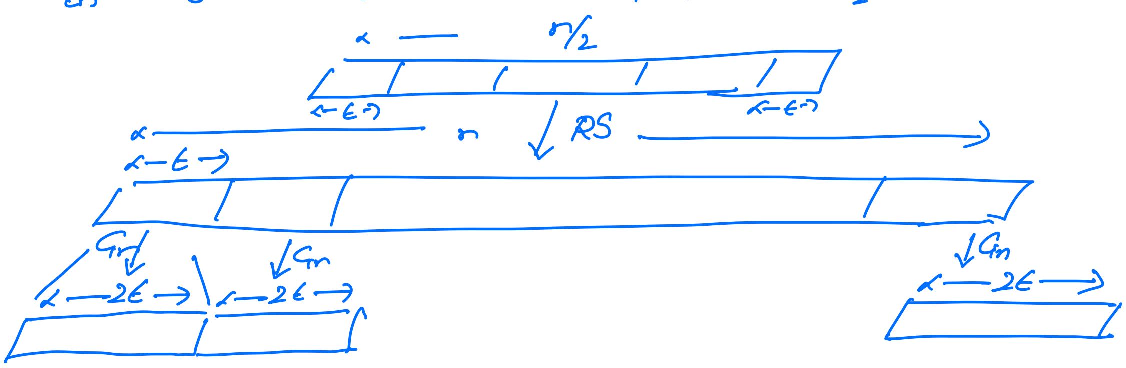
$[n\log n, \frac{n\log n}{2}, \frac{n}{2}]_2$-code

$[N, \frac{N}{2}, \frac{cN}{\log N}]_2$-code. $N = n\log n$

[Forney]

Idea: Use an inner code to encode the symbols of $\mathbb{F}_{2^t}$

$C_{in}: \{0,1\}^t \to \{0,1\}^{2t}$ $(2t, t, 0.001t)_2$-code



$[2nt, \frac{nt}{2}, \frac{n}{2} \times 0.001t]_2$-code.

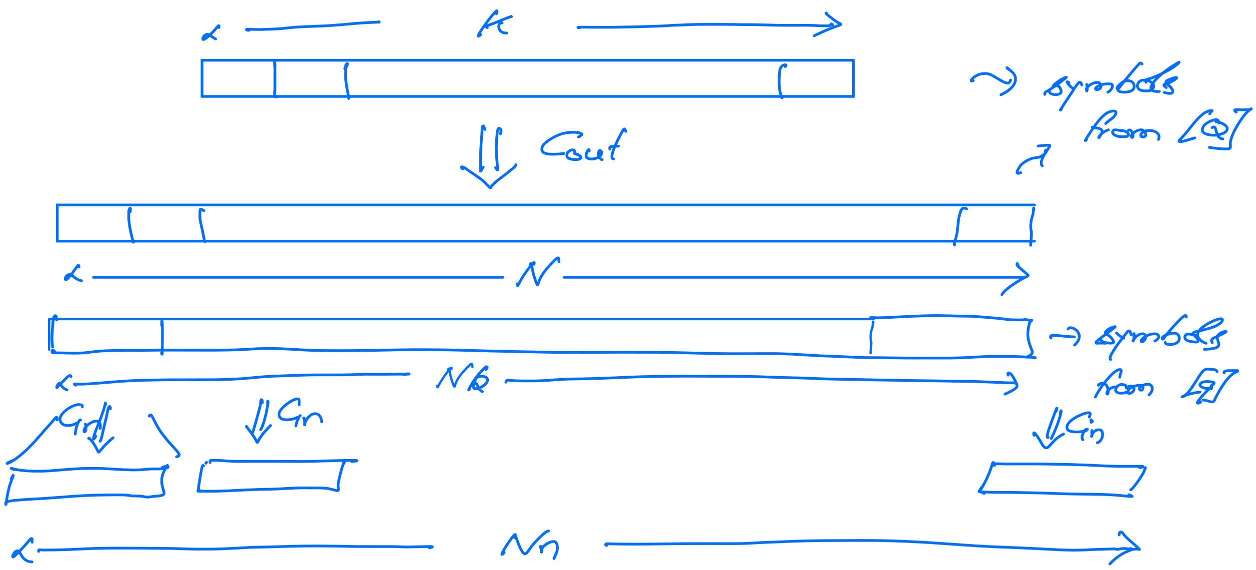
$[2nt, \frac{nt}{2}, 0.0005nt]_2$-code.

Code Concatenation [Forney]

C_{out} : $(N, K, D)_Q$ - code $Q \le q^k$

C_{in} : $(n, k, d)_q$ - code

Concatenated Code



$C = (Nn, Kk, Dd)_q$ $\qquad C = C_{out} \odot C_{in}$

Furthermore, if $[q] = \mathbb{F}_q$ & $[Q] = \mathbb{F}_{q^k}$ – a field extension of $\mathbb{F}_q$.

& C_{out} & C_{in} are linear

so is C.

How to construct good codes using code concatenation.

– Find C_{inner} – a good code in time poly(Nn)

To find a good linear code, using Varshamov's technique $q^{O(kn)}$

(for C_{out} – RS.

C_{in} – as above

$n = \Theta(\log N)$

$k = \Theta(\log N)$

Time $= 2^{\Theta(\log^2 n)} = N^{\Theta(\log N)}$

carefully w/ bookkeeping

Gilbert's greedy construction – $q^{\Theta(n)} = poly(N)$.

—

Above construction is "*explicit*"

(but still involves brute-force search).

Strongly Explicit Codes: (linear)

$$G = \begin{bmatrix} & & \\ & & \\ & & \end{bmatrix}$$

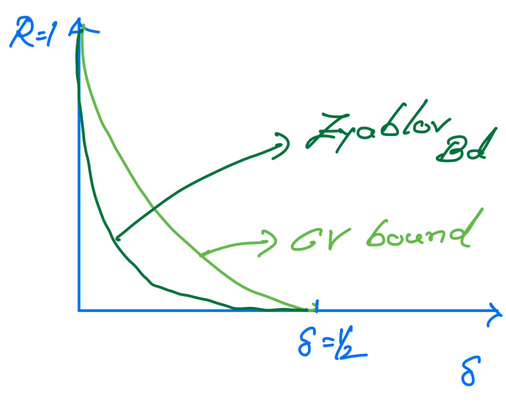
$\xleftrightarrow{k}$, n

Given $i \in [n]$, & $j \in [k]$ can output $G[i,j]$ in time $\mathrm{poly}(|i|, |j|)$

(i.e., poly log n)

(The algebraic codes (RS, RM) are strongly explicit.

However, above construction is not strongly explicit.



Qn: What is the R-vs-δ trade off achieved by the above explicit construction?

C_{out} - RS code. $\delta_{out} \gtrsim 1 - R_{out}$

C_{inner} - Gilbert construction $\delta_{in} \geq H_2^{-1}(1-r) - \varepsilon$

Concatenated Code: $R = R_{out} \cdot r$

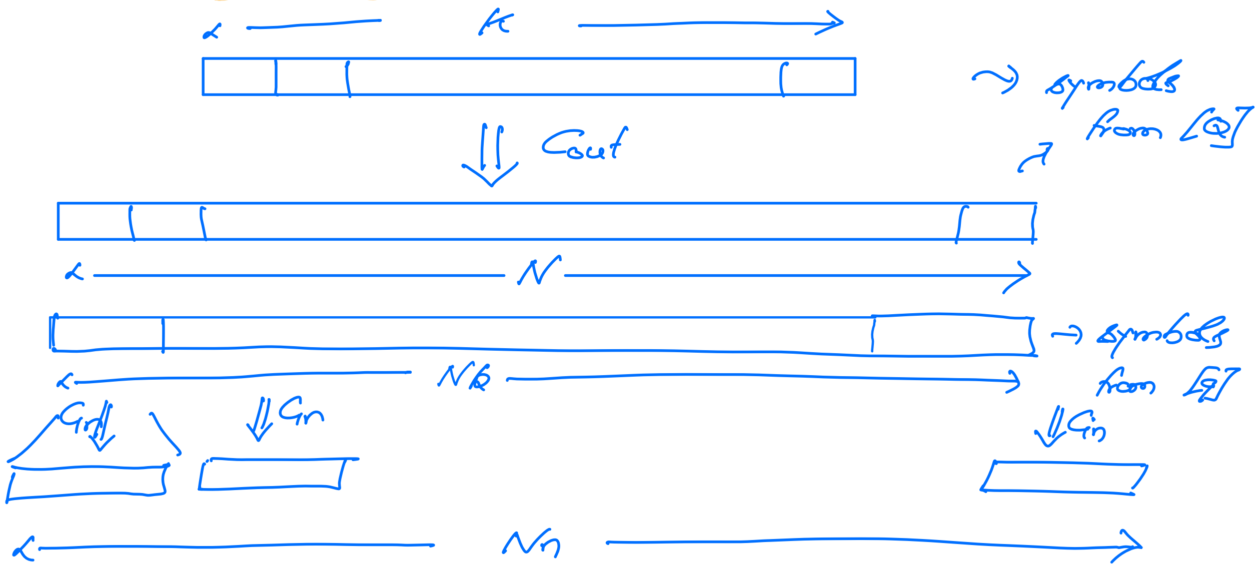
$\delta \geq \delta_{out} \cdot \delta_{in}$

Zyablov's Bound:

$$\delta \geq \max_{r \in (0,1)} \left(1 - \frac{R}{r}\right) \cdot \left(H_2^{-1}(1-r) - \varepsilon\right)$$

What about strongly explicit codes that meet the Zyablov Bound?

Justesen's Codes:



Justesen's Idea:

- Ok if inner codes are different
  - sufficient if most inner codes are "good"
- Construct an ensemble of inner codes such that most of them are good.

Proposition: Let C_{out} be a $(N, K, D)_Q$-code & $\{C_{in}^1, C_{in}^2, \dots C_{in}^N\}$ are an ensemble of $(n, k)_q$-codes (where $Q = q^k$) such that at least $(1-\varepsilon)N$ of inner codes have distance d, then

$$\mathcal{C} = C_{out} \circledcirc \{C_{in}^1, C_{in}^2, \dots C_{in}^N\}$$

is a $(Nn, Kk, (D-\varepsilon N)d)_q$-code.

Pf: $m, m' \in [q]^{kK}$ st $m \neq m'$
$[Q]^K$

By distance of C_{out}. $\Delta(C_{out}(m)\ C_{out}(m')) \geq D$

Since all but εN of inner codes have distance $\geq d$.

$$\Delta(\mathcal{C}(m)\ \mathcal{C}(m')) \geq (D - \varepsilon N) d$$

Qn: What is a good ensemble of inner codes?

Wozencraft's Ensemble:

Outer code: RS $\quad \mathbb{F} = \mathbb{F}_{2^k}$

$S = \mathbb{F}^*$ (ie, $N = 2^k - 1$)

$K = R_{out} N$

Inner Ensemble:

For each $\alpha \in \mathbb{F}^*$, $C_\alpha : \{0,1\}^k \to \{0,1\}^{2k}$

$$\mathbb{F}_{2^k} \to \mathbb{F}_{2^k}^2$$

$$x \mapsto (x, \alpha x)$$

$\left.\right\}$ C_α is $[2k, k]_2$-code

Lemma: $\forall \varepsilon$, sufficiently large N at least $(1-\varepsilon)N$ of the inner codes $\{C_\alpha \mid \alpha \in \mathbb{F}^*\}$ have distance $H_2^{-1}(\frac{1}{2}-\varepsilon)$.

Final Justesen code

(obtained by concatenating RS w/ Wozencraft's ensemble)

Encoding map:

$$m = (m_0, \ldots m_{k-1}) \sim \sum m_i X^i$$

$$m \xmapsto{RS} (m(\alpha))_{\alpha \in \mathbb{F}^*} \xmapsto{Wozen} (m(\alpha), \alpha m(\alpha))_{\alpha \in \mathbb{F}^*}$$

Pf of Lemma:

Let $(x,y) \neq (0,0)$

Obs: (x,y) is in the image of at most one of the C_α's.

$$\#\{\alpha \in \mathbb{F}^* \mid d(C_\alpha) \leq H_2^{-1}(\tfrac{1}{2}-\varepsilon)\}$$

$$\leq \#\{(x,y) \in \{0,1\}^{2t} \setminus \bar{0} \mid wt(x,y) \leq h^{-1}(\tfrac{1}{2}-\varepsilon)\cdot 2t\}$$

$$\leq Vol_2(2t, h^{-1}(\tfrac{1}{2}-\varepsilon)2t)$$

$$\leq 2^{2t(\frac{1}{2}-\varepsilon)} = 2^{t(1-2\varepsilon)}$$

$$\Pr_{\alpha \in \mathbb{F}^*}[d(C_\alpha) \leq h_2^{-1}(\tfrac{1}{2}-\varepsilon)] \leq \frac{2^{t(1-2\varepsilon)}}{2^t-1} \leq \varepsilon$$

(for large enough t)

$\square$