Reed Solomon Codes → Ron Roth

$$H_{GRS} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \cdots & \alpha_n^{n-k-1} \end{bmatrix} \begin{bmatrix} v_1 & & & \\ & v_2 & & 0 \\ & & \ddots & \\ & 0 & & v_n \end{bmatrix}$$

$\alpha_1\ \alpha_2 \ldots \alpha_n$ distinct

code locators

$v_1\ v_2 \ldots v_n$ nonzero.

column multipliers

$$G_{GRS} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{bmatrix} \begin{bmatrix} v_1' & & & 0 \\ & v_2' & & \\ & & \ddots & \\ 0 & & & v_n' \end{bmatrix}$$

ii. Encoding: $m(x) = m_0 + m_1 x + \cdots + m_k x^{k-1}$

$$\underline{c} = \left(m(\alpha_1) \quad m(\alpha_2) \quad \cdots \quad m(\alpha_n) \right)$$

Conventional RS code

$$\alpha_j = \alpha^{j-1}$$

$$v_j = \alpha^{b(j-1)}$$

$$\underbrace{\alpha^0, \alpha^1, \alpha^2, \ldots \alpha^{n-1}}_{\text{distinct}}$$

$$H_{RS} = \begin{bmatrix} 1 & 1 & 1 & 1 & & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \vdots & & \vdots \\ \vdots & \vdots & \vdots & & & \vdots \\ 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \alpha^{3(k-1)} & & \alpha^{n(k-1)} \end{bmatrix} \begin{bmatrix} 1 & & & \\ & \alpha^b & & \\ & & \alpha^{2b} & \\ & & & \ddots & \\ & & & & \alpha^{(n-1)b} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \alpha \\ 1 & \alpha^{b+1} \\ 1 & \alpha^{b+2} \\ \vdots & \vdots \\ 1 & \alpha^{b+n-k-1} \end{bmatrix}$$

$$\left(H_{RS}\right)_{i,j} = \alpha_j^{\,i-1} \times \alpha^{b(j-1)}$$

$$= \alpha^{(j-1)(i-1)} \, \alpha^{b(j-1)}$$

$$= \alpha^{(j-1)(b+i-1)} = \left(\alpha^{b+i-1}\right)^{j-1}$$

Every c/w $c_1 \sim c_n$

for all i,

$$\sum_{j=1}^{n} c_j \left(\alpha^{b+i-1}\right)^{j-1} = 0$$

If $c(x) = c_1 + c_2 x + c_3 x^2 + \sim + c_n x^{n-1}$,

$$c(\alpha^b) = 0$$

$$c(\alpha^{b+1}) = 0$$

$$\vdots$$

$$c(\alpha^{b+n-k-1}) = 0$$

$\Rightarrow \quad \alpha^b, \alpha^{b+1} \ldots \alpha^{b+n-k-1}$ are roots of $c(x)$

$\Updownarrow$

$c(x)$ is the polynomial corresp
to a codeword.

$\Updownarrow$

$$\underbrace{(x-\alpha^b)(x-\alpha^{b+1})\cdots(x-\alpha^{b+n-k-1})}_{\text{degree } n-k} \mid c(x)$$

$$\underbrace{(x-\alpha^{b})(x-\alpha^{b+1})\cdots(x-\alpha^{b+n-k-1})}_{p(x)}\; m'(x)$$

degree $\leq k-1$

gives all possible codewords!

<u>One view</u>: $\underline{c}$ is obtained by evaluating $m_0 + m_1x + \cdots m_{k-1}x^{k-1}$

at $\alpha_1, \alpha_2 \cdots \alpha_n$

Another view of conventional RS codes:

$$c(x) = m'(x)\,p(x)$$

Alternant Codes: Subfield subcodes of GRS codes

Want a good code over $\mathbb{F}_p$. $p < n$

Choose m st $p^m > n$

$C = GRS(\mathbb{F}_{p^m})$ $\mathbb{F}_p \subseteq \mathbb{F}_{p^m}$

$C' = \{ \underline{c} \in C : c_i \in \mathbb{F}_p \text{ for all } \}$

a code in $\mathbb{F}_p$

$\boxed{\text{Claim: } C' \text{ is a linear code}}$

H_{GRS} is PC matrix for C

$H_{ij} \in \mathbb{F}_{p^m}$

$\mathbb{F}_{p^m} \supseteq \mathbb{F}_p$

Lemma: If $\mathbb{F}_p \subseteq \mathbb{F}_q$, then $\mathbb{F}_q$ forms a vector space over $\mathbb{F}_p$.

Closed under linear combination

$\mathbb{F}_{p^m}$ forms a vector space over $\mathbb{F}_p$

dim = m

$$\mathbb{F}_{p^m} = \{ [a_0 + a_1 x + \dots + a_{m-1} x^{m-1}] \bmod f(x) : a_1 \dots a_m \in \mathbb{F}_p \}$$

$\downarrow$

irreducible, degree m.

$$\{ a_0 + a_1 x : a_0, a_1 \in \mathbb{F} \}$$

$$(1, x) \qquad (1+x, x)$$

$$[\alpha_0, \alpha_1]$$

Every $\alpha \in \mathbb{F}_{p^m}$ can be written as a vector

$$\underline{\alpha} \in \mathbb{F}_p^m$$

$\underline{H}_{ij} = \Omega \, \underline{h}_{ij}$

representation of H_{ij} wrt basis Ω

$$a_0 + a_1 x = \begin{bmatrix} 1 & x \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$$

$\underline{c} \in C' \iff \underline{c} \in \mathbb{F}_p^n$ & $H_{GRS} \, \underline{c}^T = 0$

$$\forall i, \quad \sum_{j=1}^{n} H_{ij} c_j = 0$$

$$\Leftrightarrow \quad \forall i \qquad \sum_{j=1}^{n} \underline{h}_{ij}\, c_j = \underline{0} \in \mathbb{F}_p^m$$

$$\sum_{j=1}^{n} \underline{h}_{ij}\, c_j = \underline{0}$$

$$\Leftrightarrow \quad \sum_{j=1}^{n} \begin{bmatrix} h_{ij}(1) \\ h_{ij}(2) \\ \vdots \\ h_{ij}(m) \end{bmatrix} c_j = 0$$

$$\Leftrightarrow \quad 1 \le i \le n-k, \quad 1 \le l \le m \qquad \sum_{j=1}^{n} h_{ij}(l)\, c_j = 0$$

# of independent PC $\leq (n-k)m$

$$\mathrm{Dim}(C') = n - \#\text{ indp PC}$$
$$\geq n - (n-k)m$$

$$d_{min}(C') \geq d_{min}(C)$$
$$= n-k+1$$

If $D = n-k+1$,

$$k' = \dim(C') \geq n - (D-1)m = n - Dm + m$$

For p fixed $n \to \infty$

$$D = \delta n$$

$$k' \geq n - (\delta n - 1) m$$

$$k' \geq n - (\delta n - 1)(c \log n) \to 0$$

Reed - Muller Codes

→ Essential Coding Theory

$\mathbb{F}_q$ $\qquad RM(q, m, r)$

$$f(\underline{x}) = \sum_{i_1, i_2, \ldots, i_m} C_{i_1, i_2, i_3 \ldots i_m} \, x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m}$$

$$2x_1x_2 + x_2^3 + x_1^2 + x_1^2 x_2 + x_1^2 x_2^2$$

Degree of $f(x_1 \ldots x_m) = \max\{ i_1 + i_2 + \cdots + i_m : C_{i_1, i_2 \ldots i_m} \neq 0 \}$

$f(x) = x_1^2 x_2 + x_1^3 x_2^2 + 3 x_1 x_2^4$

Total degree v/s Individual degree

$\text{Ind. deg}(x_1) = 3$

$\text{Ind deg}(x_2) = 4$

$\text{Tot deg}(f(x)) = 5.$

$\deg(f) = 5$

$\deg_{x_1}(f) = 3$

$\deg_{x_2}(f) = 4$

Reed Muller codes $\qquad RM(q, m, r)$

field size $\qquad$ # of vars $\qquad$ max total deg.

Codewords are evaluations of all polynomials of max deg $\le r$, ind. deg $\le q-1$ at all points in $\mathbb{F}_q^m$

$n = q^m$ $\qquad$ # of codewords $\le$

Eg: $r=1$ $q=2$, $m=2$

0, 1, x_1, x_2, x_1+x_2, $1+x_1$, $1+x_2$, $1+x_1+x_2$

Evaluation pts: (00) $(0,1)$, (10), (11)

$$\underline{c}_1 = (0, 0, 0, 0) \qquad 0$$

$$\underline{c}_2 = (1, 1, 1, 1) \qquad 1$$

$$\underline{c}_3 = (0, 0, 1, 1) \qquad x_1$$

$$c_4 = (0\ 1\ 0\ 1) \qquad x_2$$

$$c_5 = (0\ 1\ 1\ 0) \qquad x_1+x_2$$

$c_6 = (1, 1, 0, 0) \quad 1 + x_1$

$c_7 = (1\ 0\ 1\ 0) \quad 1 + x_2$

$c_8 = (1\ 0\ 0\ 1) \quad 1 + x_1 + x_2$

<u>Claim</u>: If $r < q$, then

$$\dim\left(RM[q, m, r]\right) = \binom{r+m}{r}$$

In any $\mathbb{F}_q$, $x^q = 1$

$$\alpha^q = 1 \quad \forall \alpha \in \mathbb{F}_q.$$

<u>Claim</u> : If $r < q$ then

$$\dim(RM(q, m, r)) = \binom{r+m}{r}$$

<u>Proof</u> :

$1 + x_1 x_2 + 3x_1^2 + 4x_2^2$ $\qquad m = 2$

$r = 2$

$$m(x) = a_{00} x_1^0 x_2^0 + a_{01} x_1^0 x_2^1 + a_{10} x_1^1 x_2^0 + a_{20} x_1^2 x_2^0$$

RM(3, 2, 2)

dim = 6

$$+ a_{02} x_1^0 x_2^2 + a_{11} x_1^1 x_2^1$$

$$\underline{a} = (1, 0, 0, 0, 0, 2)$$

$$m(x) = 1 + 2x_1 x_2$$

$$\left(1, \; 1, \; 1, \; 1 \; 0 \; 2 \; 1 \; 2 \; 0\right)$$

$$\begin{matrix} 00 & 01 & 02 & 10 & 11 & 12 & 20 & 21 & 22 \end{matrix}$$

In general, $\dim(RM(q, m, r))$ = # of monomials in m vars & total degree $\leq r$

$(r < q)$

$$= \left| \left\{ (d_1, d_2 \ldots d_m) \in \mathbb{Z}^m : 0 \leq d_i \leq r \;\&\; \sum_{i=1}^{r} d_i \leq r \right\} \right|$$

(Stars & Bars problem)

n stars

① ③ ⓪ ②

$| \star | \star \; \star \; \star \, || \star \; \star$

$(d_1 \ldots d_m) \qquad 0 \leq d_i \leq n$

$$\sum_{i=1}^{m} d_i \leq n$$

$d_1 = 2, \quad d_2 = 1, \quad d_3 = 0, \quad d_4 = 1$

$\star \quad \star \, | \, \star \, || \, \star \, | \, \star \quad \ldots \quad \star$

# of stars b/w $(i-1)$ th & i th bar $= d_i - d_{i-1}$

① ② 0+0

| ★ ★ | ★ ||| ★ ★ ★

$$(0,\ 3,\ 1,\ 0,\ 0)$$

$$(n+1) \qquad (n+1)^m$$

$$\binom{n+m}{m} = \binom{n+m}{n}$$

| ★ ★ | ★ ||| ★ ★ ★

① ① 0 0

| ★ | ★ | | | ★ ★

Minimum distance $\quad m < q$

$$wt_H(\underline{c}) = q^m - \#\text{ of roots of polynomial.}$$

If $m=1$, then $wt_H(\underline{c}) \geq q^m - r$

$$= q - r.$$

Claim: $\dfrac{\#\text{ of roots}}{q^m} \leq \dfrac{r}{q}$

$$wt(C) \geq q^m\left(1 - \frac{r}{q}\right) = q^m - r\,q^{m-1}$$

Proof: We know that for $m=1$,

$$\frac{\# \text{ of nodes}}{q^m} \le \frac{r}{q}$$

Suppose true for $(m-1)$-variate polynomial.

$$f(x_1 \dots x_m) = f_0(x_1 \dots x_{m-1})\, x_m^0 + f_1(x_1 \dots x_{m-1})\, x_m^1 + \dots + f_t(x_1 \dots x_{m-1})\, x_m^t$$

$$t \le r$$

$$\deg(f_i) \le r - i$$

What is $\Pr[f(x_1 - x_m) = 0]$?

$$\mathcal{E}_1 = \{ f_t(x_1 - x_{m-1}) = 0 \}$$

$$\mathcal{E}_2 = \{ f(x_1 - x_m) = 0 \mid f_t(x_1 -- x_{m-1}) \neq 0 \}$$

$$\Pr[f(x_1 -- x_m) = 0] \leq \Pr[\mathcal{E}_1] + \Pr[\mathcal{E}_2]$$

$$\left(\{ f(x_1 - x_m) = 0 \} \subsetneq \mathcal{E}_1 \cup \mathcal{E}_2 \right)$$

$f_t(x_1 - x_{m-1})$ is an $(m-1)$-variate poly of deg $\leq n-t$

$$\Pr[f_t(x_1 \ldots x_{m-1}) = 0] \leq \frac{r-t}{q}.$$

Conditioned on $f_t(x_1 \ldots x_{m-1}) \neq 0$, $f(\ldots, x_m)$ is a poly of degree $= t$.

$$\Pr[\mathcal{E}_2] \leq \frac{t}{q}$$

$$\Pr[f(x_1 \ldots x_m) = 0] \leq \frac{r-t}{q} + \frac{t}{q} = \frac{r}{q}$$

General Case (r could be greater than q)

<u>Theorem</u> : Let f be any nonzero poly in m variables

$$\deg_{x_i}(f) \le q-1$$

$$\deg(f) \le r$$

& let s, t be integers st $t \le q-2$ &

$$\underbrace{s(q-1) + t = r}$$

$s \to$ quotient $t \to$ remainder

$$|\{ \underline{a} \in \mathbb{F}_q^m : f(\underline{a}) \neq 0 \}| \ge (q-t)\, q^{m-s-1}$$

$$\ge q^{m - r/(q-1)}$$

If $r < q$, take $s = 0$, $t = r$

$$\text{RHS} = (q - r)\, q^{m-1} = q^m - r q^{m-1}$$

Take $m = 1$: $\Rightarrow$ $r \leq q - 1$

Case 1 : $r \leq q - 2$

$s = 0$, $t = r$

# of Non zeros $\Rightarrow$ $q - r$

$$= (q - t)\, q^{m-1}$$ $= 0$

Case 2: $r = q-1$

$s = 1, \quad t = 0 \qquad (s(q-1) + t = r)$

# of pts where $f \neq 0 \geq q - r$

$= q - s(q-1)$

$= 1$

RHS $= (q-t)\, q^{m-s-1} = (q-0)\, q^{1-1-1} = q\, q^{-1}$

$= 1$

$$f(x_1 \cdots x_m) = f_0(x_1 \cdots x_{m-1})\, x_m^0 + \cdots$$

$$+ f_b(x_1 \cdots x_{m-1})\, x_m^b$$

$b \leq n$ $\quad b \leq q-1$

Suppose theorem true for all polynomials in $m-1$ variables.

$$A_1 = \{ f_b(X_1 - X_{m-1}) \neq 0 \}$$

$$A_2 = \{ f(X_1 - X_m) \neq 0 \mid f_b(X_1 - X_{m-1}) \neq 0 \}$$

$$\Pr[f(X_1 \dots X_m) \neq 0] \geq \Pr[A_1] \Pr[A_2]$$

$$\shortparallel$$

$$\Pr[f(X_1 \dots X_m) \neq 0 \mid f_b(X_1 \dots X_{m-1}) \neq 0] \Pr[f_b(X_1 \dots X_{m-1}) \neq 0]$$

$$+ \Pr[f(X_1 \dots X_m) \neq 0 \mid f_b(X_1 \dots X_{m-1}) = 0] \Pr[f_b(X_1 \dots X_{m-1}) = 0]$$

$$\Pr[A_1] \geq \frac{q-b}{q}$$

Given $f_b \neq 0$,
$f(\dots, X_m)$ is a poly
(in x_m) of deg b

$$\Pr[A_2] \geq \underbrace{(q-t')\, q^{m-d'-1}}$$

(induction step)

$f_b(x_1 \ldots x_{m-1})$ has tot deg $\leq r - b$

$s'(q-1) + t' = r - b.$

$$\Pr[\, f(x_1 \ldots x_m) \neq 0 \,] \geq \left(\frac{q-b}{q}\right)(q-t')\, q^{m-s'-1}$$

$$\geq (q-t)\, q^{m-s-1}$$

(See Essentials of Coding theory)

Claim : Let $K_{qmn} = \dim(RM(q,m,n))$

$$= \left| \left\{ (d_1, d_2, \dots, d_m) : d_i \in \mathbb{Z},\ 0 \le d_i \le q-1,\ \sum_{i=1}^{m} d_i \le n \right\} \right|$$

Then, $K^-_{qmn} \le K_{q,m,n} \le K^+_{qmn}$

$$K^-_{qmn} = \begin{cases} \max\left\{ \frac{q^m}{2},\ q^m - K^+_{q,m,(q-1)m-n} \right\} & \text{if } n \ge \frac{(q-1)m}{2} \\ \max\left\{ \binom{m}{n},\ \frac{1}{2} \left\lfloor \frac{2n+m}{m} \right\rfloor^m \right\} & \text{ow} \end{cases}$$

$$K^{+}_{qmr} = \min\left\{ q^m, \binom{m+r}{r} \right\}$$

What about $q=2$?

Minimum distance:

$$d_{min} = |\{ \underline{a} : f(\underline{a}) \neq 0 \}| \geq q^{m-r} = q^m q^{-r}$$

$$= n 2^{-r}$$

Suppose we want $d_{min} = n\delta$

$$\Rightarrow 2^{-r} = \delta$$

$$r = \log_2 \frac{1}{\delta}$$

$$n = 2^m \qquad m = \log_2 n$$

$$m >> r$$

$$K_{q,m,r} \geq \max\left\{ \binom{m}{r}, \frac{1}{2}\left\lfloor \frac{2r+m}{m} \right\rfloor^m \right\}$$

$$\downarrow \qquad \downarrow$$

$$\binom{m}{r} = \frac{m(m-1)\cdots(m-r+1)}{r(r-1)\cdots 1} \qquad \left(1 + \frac{2r}{m}\right)^m = \left(\left(1 + \frac{2r}{m}\right)^{\frac{m}{2r}}\right)^{2r}$$

$$= e^{2r}$$

Suppose we want $K_{qmr} \gtrsim nR$

$$K_{qmr} \gtrsim \binom{m}{r} \approx 2^{m} R$$

$$\binom{m}{r} \leq \left(\frac{me}{r}\right)^{r}$$

$$\binom{m}{r} \approx 2^{m H_2\left(\frac{r}{m}\right)} \approx 2^{m} R \rightarrow \text{rate}$$

$$m H_2(r/m) = m + \log_2 R$$

$$H_2\left(\frac{r}{m}\right) = 1 + \frac{\log_2 R}{m}$$

$$\frac{n}{m} = \frac{1}{2} - \delta$$

$$d_{min} \geq 2^{m-n} = 2^{m(1-n/m)}$$

$$= 2^{m\left(\frac{1}{2}+\delta\right)}$$

$$= 2^{m\delta}\, 2^{m/2}$$

$$\approx 2^{m/2} = \sqrt{2^m} = \sqrt{n}$$

Reed Solomon Codes

<u>Fact</u>: $\exists$ a decoder for GRS codes that has $O(n^2)$ complexity & can correct $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors

Consider any DMC. (BSC): Shannon says $\exists$ codes of blocklength n, rate $\approx C$ & $P_e = \Pr[\hat{m}^i \neq m^i] \leq 2^{-\alpha n}$

decoding complexity $= O(2^{nC})$

Concatenated Codes

n

n'

Let us pick a "good" (capacity achieving) code of blocklength n', rate $\approx C$

- Decoding complexity of each sub-block $= O(2^{cn'})$

If $n' = O(\log n)$ $= n^2$

Total decoding complexity $= \frac{n}{n'} n^2 = \text{poly}(n)$

$$\Pr[\text{i'th block is decoded incorrectly}] \leq 2^{-\alpha n'} \leq \frac{1}{n^{\beta}}$$

$$= \text{poly}\left(\frac{1}{n}\right)$$

$$\Pr[\text{all blocks decoded correctly}] = 1 - \Pr[\text{any block dec incorrectly}]$$

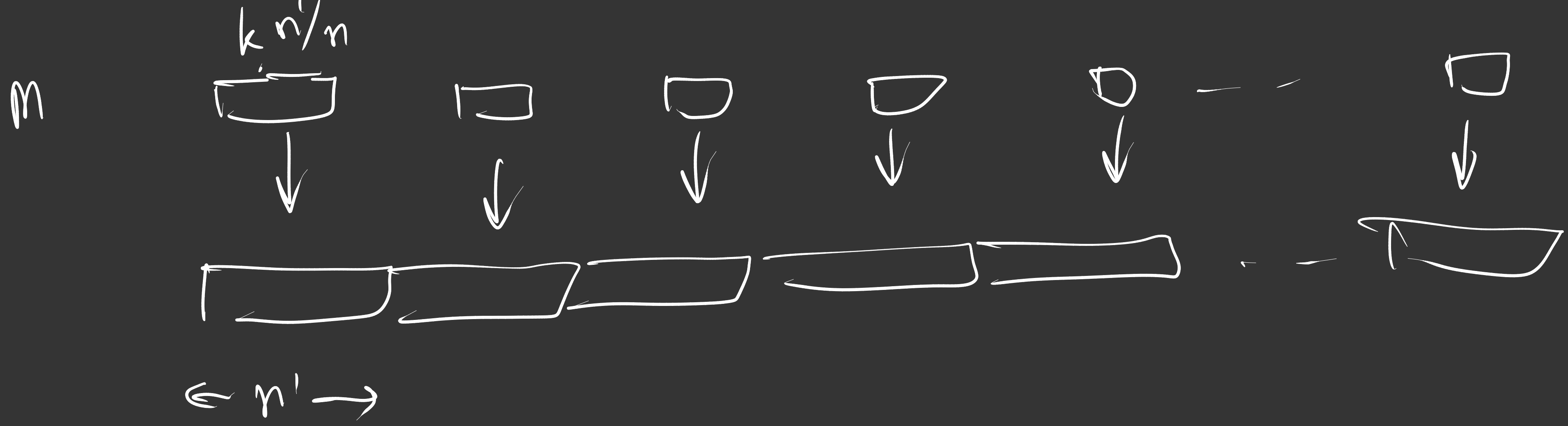
$$\geq 1 - \frac{n}{n'} \frac{1}{n^{\beta}}$$

$$\mathbb{E}[\#\text{ of erroneous chunks}] = \frac{n}{n'} \cdot \frac{1}{n^{\beta}}$$

Chernoff

$$\Pr[\#\text{ of erroneous chunks} \geq \delta\, n/n'] \leq 2^{-\gamma n/n'}$$

$$\delta \to 0 \quad \text{as } n \longrightarrow \infty$$



message → k $\quad k = nC$ $\quad k$ bits

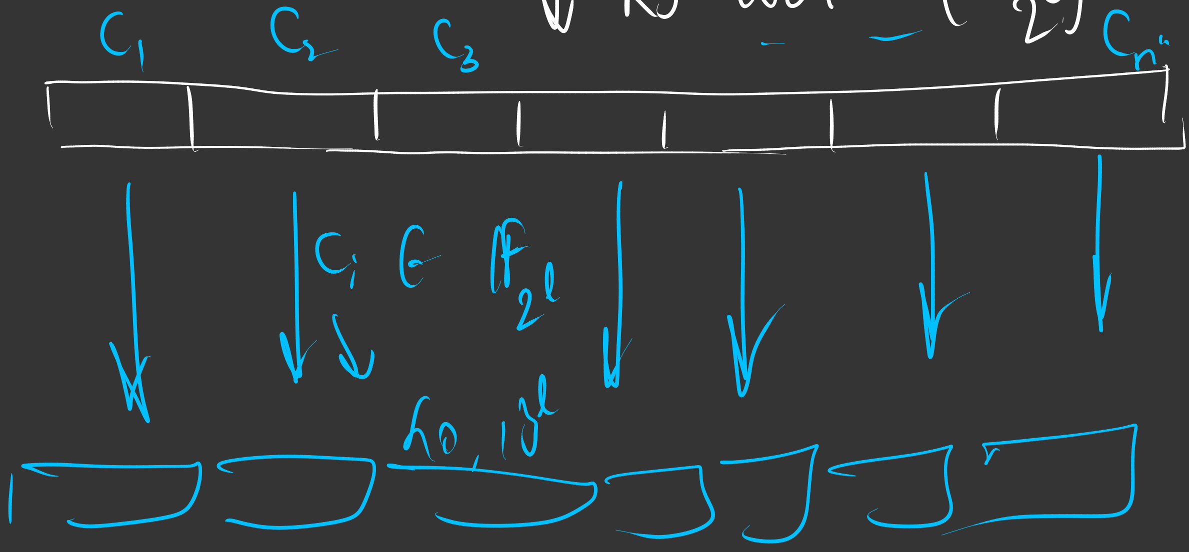
Rate $\to 1$ as $n \to \infty$

$\downarrow$ RS code $(\mathbb{F}_{2^\ell})$

min dist $> 2\delta \frac{n}{n'}$ $\to 0$ as $n \to \infty$

Blocklength $\approx \frac{nC}{\ell}$

k'



n'

Capacity achieving code

n

Overall prob of error $\leq \Pr[\, > \delta \frac{n}{n'}$ chunks are in error$]$

$\leq 2^{-\delta n/n'}$

$$\text{Rate} = \frac{k}{n} = \frac{k}{k'}\,\frac{k'}{n} = \left(\frac{k'-d+1}{k'}\right)\frac{k'}{n}$$

$$\approx (1-\delta)\,C$$

Overall:

$$P_e \approx 2^{-\alpha' n}$$

$$\text{Complexity} \approx O(\text{poly}(n))$$

$$R \approx C$$