TI-Lecture-28-4-2020

28 April, 2020 13:57

Reed - Solomon codes

$= \mathbb{F}$

$\alpha_1, \alpha_2, \dots \alpha_n \in GF_q \qquad q = 2^s$

$i \neq j \Rightarrow \alpha_i \neq \alpha_j \qquad k \to n$

$m \in \#^k$

$(m_0, \dots m_{k-1})$

$p_m(x) = \sum_{i=0}^{k-1} m_i x^i$

$C(m) = \langle p_m(\alpha_1), p_m(\alpha_2) \dots \quad p_m(\alpha_n) \rangle$

$[n, k, n-k+1]_q$

Berlekamp - Welch (1986)

$\langle r_1, r_2, r_3, \dots r_n \rangle$ received word

... error locating polynomial $E(x)$

if $r_i \neq p_m(\alpha_i) \Rightarrow E(\alpha_i) = 0$

d_e = degree $E(x)$ ideally $\frac{n-k+1-1}{2} = \frac{n-k}{2}$

$d_e \leq \frac{n-k-1}{2}$

$\forall i \quad (r_i - p(\alpha_i)) E(\alpha_i) = 0$

$(*) \Rightarrow \quad r_i E(\alpha_i) = p(\alpha_i) \cdot E(\alpha_i) \qquad \forall i = 1, \dots n$

$Q(x) = p(x) \cdot E(x) \qquad \sum_{i=0}^{\frac{n+k-3}{2}} c_i' x^i \qquad c_i', c_i$

$\deg p \leq k-1 \qquad \deg E \leq \frac{n-k-1}{2}$

$Q(x) = p(x) \cdot E(x)$ $\quad \sum_{i=0}^{n-1} c_i' x^i$ $\quad c_i', c_i$ unknowns

$E(x)$ $\quad \sum_{i=0}^{\frac{n-k-1}{2}} c_i x^i$

linear system of equations

n vars ... n eq's

#vars: $2 + \frac{n+k-3}{2} + \frac{n-k-1}{2} = n$

$\exists$ non-zero solution $E(x)$ assuming # errors $\leq \frac{n-k-1}{2}$

non-zero $\longrightarrow$ $Q(x), E(x) \not\equiv 0$

output: $\frac{Q(x)}{E(x)} = p(x)$

- $Q(x)$ is not divisible by $E(x) \rightarrow$ FAIL [too many errors]
- check $\Delta_{\text{Ham}}(\langle r_1, \ldots r_n \rangle, \langle p(\alpha_1), \ldots p(\alpha_n) \rangle) > \frac{n-k-1}{2}$ then FAIL

running time $O(n^3)$

[FFT $O(n \lg^c n)$]

Claim: Let $(Q(x), E(x)) \neq (Q'(x), E'(x))$ be two solutions to the lin. system where $E(x), E'(x) \not\equiv 0$.

then $\frac{Q(x)}{E(x)} = \frac{Q'(x)}{E'(x)}$.

R_1 $\qquad$ R_2

$E'(x)$

Pf: $R_1 = Q'(x) \cdot E(x)$ $\qquad$ $R_2 = Q(x) \cdot E'(x)$

$\frac{n-k-1}{2}$ $\qquad$ $\frac{n+k-3}{2}$ $\qquad \Rightarrow$ deg R_1, deg $R_2 \le n-1$

deg E $\qquad$ deg Q

$\alpha_1, \alpha_2, \dots \alpha_n$ $\qquad$ agree on n points $\Rightarrow$ must be the same polynomial

$\Rightarrow \forall i \in 1, \dots, n \qquad R_1(\alpha_i) = R_2(\alpha_i)$

$\forall i \quad r_i E(\alpha_i) = Q(\alpha_i)$
$r_i E'(\alpha_i) = Q'(\alpha_i)$
$\Rightarrow r_i \cdot E'(\alpha_i) Q(\alpha_i) = r_i E(\alpha_i) Q'(\alpha_i)$

($R_2(\alpha_i)$, $R_1(\alpha_i)$)

$r_i \neq 0 \Rightarrow R_1(\alpha_i) = R_2(\alpha_i)$

$r_i = 0 \Rightarrow Q(\alpha_i) = 0 \quad Q(\alpha_i)$
$R_1(\alpha_i) = R_2(\alpha_i)$

$\Rightarrow \overbrace{Q'(x) \cdot E(x)}^{P(x)} \equiv Q(x) \cdot E'(x)$

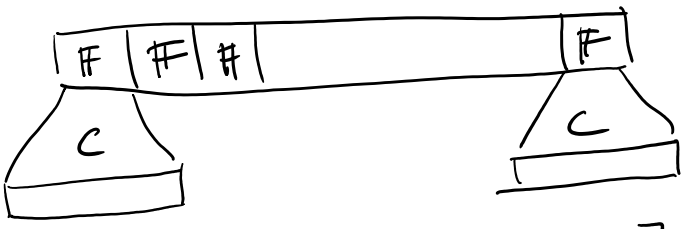
decompose R_1 and R_2 into irreducible polynomials, they must be the same (up to their permutation) $\Rightarrow \frac{Q(x)}{E(x)} = \frac{Q'(x)}{E'(x)}$

- Reed - Solomon codes $\qquad |\mathbb{F}| \ge n$
- Reed - Muller codes $\qquad$ smaller field $\mathbb{F}$, multivariate polynomials

$p(x)$ vs. $p(x_1, x_2, \dots x_t)$

RS → binary

$[n, k, D]_q$



$2^s = q$

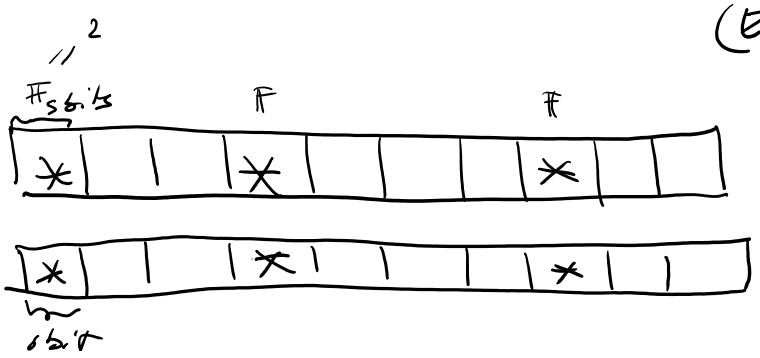
"concatenation of codes"

$C = [\ell, s, d]_2$ $\quad \ell = \Theta(s)$, $d = \Theta(s)$

$\rightarrow [n\ell, ks, dD]_2$ binary

(can choose C so that the resulting code is linear.) (Exc)

Decoding ?



D

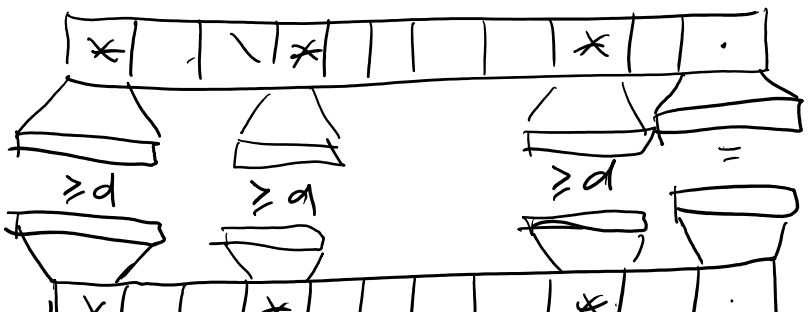
$D < \#\text{dist. far} < D_S$

$|F| \geq n$ $\quad s \geq \lg n \Rightarrow [n\lg n, k\lg n, n-k+1]_2$

$n = 2^s = q$ $\quad N$ $\quad K$ $\quad D$

$n = 2k$ rate $\frac{1}{2}$ $\quad n\lg n$ vs $\frac{n}{q}$

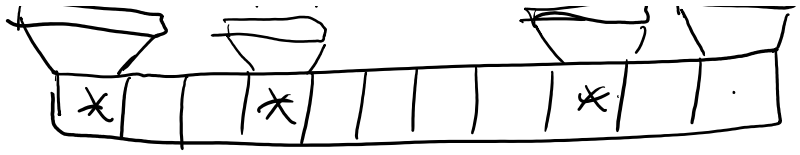
$\frac{D}{N} \to 0$ $\quad n \to 0$



D

$\downarrow$

D_1



$D \nearrow$

$C \quad [\ell, s, d]_2$

$\ell = \Theta(s) = \gamma s$
$d = \Theta(s) = \varepsilon s$
$n = 2k$
$D = k$

$[n\ell, ks, Dd]_2$

$[2\gamma ks, ks, \varepsilon ks]_2$

$2\gamma \qquad \varepsilon$

code with constant rate & constant relative min. distance

Decoding concatenated codes?

- decode each "symbol" from C
- decode RS code

Q: how many errors does this correct?

can decode $\simeq \frac{D \cdot d}{4}$ errors

$\frac{D'}{2} \quad \| \quad \frac{n-k}{2} \cdot \frac{d}{2} \quad \leq \frac{D}{2} \cdot \frac{d}{2}$

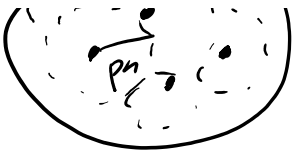
Could hope: $\frac{D \cdot d - 1}{2} \simeq \frac{D \cdot d}{2}$

Alg. Forney ($\simeq$ 60's) ... decodes $\simeq \frac{D \cdot d}{2}$ errors.

- $C = [\gamma s, s, \varepsilon s]_2$

$[n, \overbrace{[1 - H(p)]n}, pn]_2$

(Gilbert's) - code exists



- linear code $[n, \lceil (1-H(p))n \rceil, pn]_2$ ... C

  (Varshamov) ... pick a random generating matrix for C.

Claim: Let d & n, k satisfy

$$2^k \leq \frac{2^n}{Vol(n, d-1)}.$$ Then with high probability a random $k \times n$ matrix G generates $[n, k, d]_2$ code.

$Vol(n,d) \approx 2^{H(\frac{d}{n})n}$

$d = pn$

Pf: $\forall\ x \in \{0,1\}^k$, $x \neq 0$: $\Delta_{Ham}(xG) \geq d$

for fixed x

$$\Pr[\Delta_{Ham}(xG) \leq d] =$$

G picked at random

y ... uniform random over $\{0,1\}^n$

$$= \frac{Vol(n, d-1)}{2^n}$$

$$\Pr_G[\exists x \in \{0,1\}^k \setminus \{0^n\} \text{ s.t. } \Delta_{Ham}(xG) < d] \leq (2^k - 1) \cdot \frac{Vol(n, d-1)}{2^n} < 1.$$

$[\ ,\ 2^{10},\ \dots\ ]$